Cisco Systems

User Guide for Cisco Secure ACS for Windows

Version 4.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7816992=
Text Part Number: 78-16992-02

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.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0501R)

User Guide for Cisco Secure Access Control Server for Windows
© 2002-2006 Cisco Systems, Inc. All rights reserved.

Preface 25

Audience 25

Organization 25

Conventions 26

Product Documentation 27

Related Documentation 28

Obtaining Documentation 28

Cisco.com 28

Product Documentation DVD 29

Ordering Documentation 29

Documentation Feedback 29

Cisco Product Security Overview 29

Reporting Security Problems in Cisco Products 30

Obtaining Technical Assistance 30

Cisco Technical Support & Documentation Website 31

Submitting a Service Request 31

Definitions of Service Request Severity 31

Obtaining Additional Publications and Information 32

CHAPTER 1

Overview 1

Introduction to ACS 1

ACS Features, Functions and Concepts 2

ACS as the AAA Server 3

AAA Protocols—TACACS+ and RADIUS 3

TACACS+ 3

RADIUS 3

Additional Features in ACS Version 4.0 4

Authentication 6

Authentication Considerations 6

Authentication and User Databases 7

Authentication Protocol-Database Compatibility 7

Passwords 8

Other Authentication-Related Features 11

Authorization 12

Max Sessions 12
Dynamic Usage Quotas 13
Shared Profile Components 13
Support for Cisco Device-Management Applications 13
Other Authorization-Related Features 14
Accounting 14
Other Accounting-Related Features 15
Managing and Administrating ACS 15
Web Interface Security 15
HTTP Port Allocation for Administrative Sessions 16
Web Interface Layout 16
Uniform Resource Locator for the Web Interface 18
Online Help and Online Documentation 18
Using Online Help 18
Using the Online User Guide 19
ACS Specifications 19
System Performance Specifications 19
ACS Windows Services 20

CHAPTER 2 **Deployment Considerations** 1
Basic Deployment Factors for ACS 1
Network Topology 2
Dial-Up Topology 2
Wireless Network 4
Remote Access using VPN 6
Remote Access Policy 7
Security Policy 8
Administrative Access Policy 8
Separation of Administrative and General Users 9
Database 10
Number of Users 10
Type of Database 10
Network Latency and Reliability 10
Suggested Deployment Sequence 11

CHAPTER 3 **Using the Web Interface** 1
Administrative Sessions 1
Administrative Sessions and HTTP Proxy 2
Administrative Sessions Through Firewalls 2

Administrative Sessions Through a NAT Gateway 2
Accessing the Web Interface 3
Logging Off the Web Interface 3
Interface Design Concepts 4
Introduction of Network Access Profiles 4
User-to-Group Relationship 4
Per-User or Per-Group Features 4
User Data Configuration Options 4
Configuring New User Data Fields 5
Advanced Options 5
Setting Advanced Options for the ACS User Interface 7
Protocol Configuration Options for TACACS+ 7
Setting Options for TACACS+ 9
Protocol Configuration Options for RADIUS 9
Setting Protocol Configuration Options for IETF RADIUS Attributes 12
Setting Protocol Configuration Options for Non-IETF RADIUS Attributes 13

CHAPTER 4 **Network Configuration** 1
About Network Configuration 1
About Distributed Systems 2
AAA Servers in Distributed Systems 2
Default Distributed System Settings 3
Proxy in Distributed Systems 3
Fallback on Failed Connection 4
Character String 4
Stripping 4
Proxy in an Enterprise 5
Remote Use of Accounting Packets 5
Other Features Enabled by System Distribution 5
Network Device Searches 6
Network Device Search Criteria 6
Searching for Network Devices 6
AAA Client Configuration 7
AAA Client Configuration Options 8
Adding AAA Clients 11
Editing AAA Clients 13
Configuring a Default AAA Client 14
Deleting AAA Clients 14

AAA Server Configuration 15
AAA Server Configuration Options 15
Adding AAA Servers 16
Editing AAA Servers 18
Deleting AAA Servers 19
Network Device Group Configuration 19
Adding a Network Device Group 20
Assigning an Unassigned AAA Client or AAA Server to an NDG 21
Reassigning AAA Clients or AAA Servers to an NDG 21
Renaming a Network Device Group 22
Deleting a Network Device Group 22
Proxy Distribution Table Configuration 23
About the Proxy Distribution Table 23
Adding a New Proxy Distribution Table Entry 24
Sorting the Character String Match Order of Distribution Entries 25
Editing a Proxy Distribution Table Entry 25
Deleting a Proxy Distribution Table Entry 26

CHAPTER 5 **Shared Profile Components** 1
About Shared Profile Components 1
802.1X Example Setup 2
Network Access Filters 2
About Network Access Filters 3
Adding a Network Access Filter 3
Editing a Network Access Filter 5
Deleting a Network Access Filter 6
RADIUS Authorization Components 6
About RADIUS Authorization Components 7
Understanding RACs and Groups 7
Migrating Away from Groups to RACs 7
Vendors 7
Attribute Types 8
Before You Begin Using RADIUS Authorization Components 8
Enabling Use of RAC 9
Adding RADIUS Authorization Components 9
Cloning a RADIUS Authorization Component 10
Editing a RADIUS Authorization Component 10
Deleting a RADIUS Authorization Component 11
Downloadable IP ACLs 13

About Downloadable IP ACLs 13
Adding a Downloadable IP ACL 15
Editing a Downloadable IP ACL 16
Deleting a Downloadable IP ACL 17
Network Access Restrictions 17
About Network Access Restrictions 18
About IP-based NAR Filters 19
About Non-IP-based NAR Filters 19
Adding a Shared NAR 20
Editing a Shared NAR 22
Deleting a Shared NAR 23
Command Authorization Sets 24
About Command Authorization Sets 24
Command Authorization Sets Description 24
Command Authorization Sets Assignment 26
Case Sensitivity and Command Authorization 26
Arguments and Command Authorization 27
About Pattern Matching 27
Adding a Command Authorization Set 28
Editing a Command Authorization Set 29
Deleting a Command Authorization Set 30

CHAPTER 6 **User Group Management** 1
About User Group Setup Features and Functions 2
Default Group 2
Group TACACS+ Settings 2
Group RADIUS Settings 3
Basic User Group Settings 3
Group Disablement 3
Enabling VoIP Support for a User Group 4
Setting Default Time-of-Day Access for a User Group 5
Setting Callback Options for a User Group 5
Setting Network Access Restrictions for a User Group 6
Setting Max Sessions for a User Group 9
Setting Usage Quotas for a User Group 10
Configuration-Specific User Group Settings 12
Setting Enable Privilege Options for a User Group 13
Setting Token Card Settings for a User Group 14
Enabling Password Aging for the ACS Internal Database 15

Varieties of Password Aging Supported by ACS 15
Password Aging Feature Settings 16
Enabling Password Aging for Users in Windows Databases 19
Setting IP Address Assignment Method for a User Group 21
Assigning a Downloadable IP ACL to a Group 22
Configuring TACACS+ Settings for a User Group 22
Configuring a Shell Command Authorization Set for a User Group 24
Configuring a PIX Command Authorization Set for a User Group 25
Configuring Device Management Command Authorization for a User Group 26
Configuring IETF RADIUS Settings for a User Group 27
Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group 28
Advanced Configuration Options 29
Configuring Cisco Airespace RADIUS Settings for a User Group 29
Configuring Cisco Aironet RADIUS Settings for a User Group 30
Configuring Ascend RADIUS Settings for a User Group 32
Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group 33
Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group 34
Configuring Microsoft RADIUS Settings for a User Group 35
Configuring Nortel RADIUS Settings for a User Group 36
Configuring Juniper RADIUS Settings for a User Group 37
Configuring BBSM RADIUS Settings for a User Group 38
Configuring Custom RADIUS VSA Settings for a User Group 39
Group Setting Management 39
Listing Users in a User Group 40
Resetting Usage Quota Counters for a User Group 40
Renaming a User Group 40
Saving Changes to User Group Settings 41

CHAPTER 7 **User Management** 1
About User Setup Features and Functions 1
About User Databases 2
Basic User Setup Options 2
Adding a Basic User Account 3
Setting Supplementary User Information 4
Setting a Separate CHAP/MS-CHAP/ARAP Password 5
Assigning a User to a Group 5
Setting the User Callback Option 6
Assigning a User to a Client IP Address 7
Setting Network Access Restrictions for a User 8

Setting Max Sessions Options for a User 11
Options for Setting User Usage Quotas 12
Setting Options for User Account Disablement 13
Assigning a Downloadable IP ACL to a User 14
Advanced User Authentication Settings 15
TACACS+ Settings (User) 16
Configuring TACACS+ Settings for a User 16
Configuring a Shell Command Authorization Set for a User 17
Configuring a PIX Command Authorization Set for a User 19
Configuring Device-Management Command Authorization for a User 20
Configuring the Unknown Service Setting for a User 21
Advanced TACACS+ Settings for a User 22
Setting Enable Privilege Options for a User 22
Setting TACACS+ Enable Password Options for a User 23
Setting TACACS+ Outbound Password for a User 24
RADIUS Attributes 24
Setting IETF RADIUS Parameters for a User 25
Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User 26
Setting Cisco Airespace RADIUS Parameters for a User 27
Setting Cisco Aironet RADIUS Parameters for a User 28
Setting Ascend RADIUS Parameters for a User 29
Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User 30
Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User 31
Setting Microsoft RADIUS Parameters for a User 32
Setting Nortel RADIUS Parameters for a User 33
Setting Juniper RADIUS Parameters for a User 34
Setting BBSM RADIUS Parameters for a User 35
Setting Custom RADIUS Attributes for a User 35
User Management 36
Listing All Users 37
Finding a User 37
Disabling a User Account 38
Deleting a User Account 38
Resetting User Session Quota Counters 39
Resetting a User Account after Login Failure 39
Removing Dynamic Users 40
Saving User Settings 41

CHAPTER 8 **System Configuration: Basic** 1

Service Control 1
Determining the Status of ACS Services 2
Stopping, Starting, or Restarting Services 2
Setting Service Log File Parameters 3
Logging 3
Date Format Control 3
Setting the Date Format 4
Local Password Management 4
Configuring Local Password Management 6
ACS Backup 7
About ACS Backup 7
Backup File Locations 8
Directory Management 8
Components Backed Up 8
Reports of ACS Backups 8
Backup Options 9
Performing a Manual ACS Backup 9
Scheduling ACS Backups 9
Disabling Scheduled ACS Backups 10
ACS System Restore 11
About ACS System Restore 11
Backup Filenames and Locations 11
Components Restored 12
Reports of ACS Restorations 12
Restoring ACS from a Backup File 12
ACS Active Service Management 13
System Monitoring 13
System Monitoring Options 13
Setting Up System Monitoring 14
Event Logging 15
Setting Up Event Logging 15
VoIP Accounting Configuration 15
Configuring VoIP Accounting 16

CHAPTER 9 **System Configuration: Advanced** 1

ACS Internal Database Replication 1
About ACS Internal Database Replication 2

Replication Process 3
Replication Frequency 5
Important Implementation Considerations 5
Database Replication Versus Database Backup 6
Database Replication Logging 7
Replication Options 7
Replication Components Options 7
Outbound Replication Options 9
Inbound Replication Options 10
Implementing Primary and Secondary Replication Setups on ACSs 10
Configuring a Secondary ACS 11
Replicating Immediately 12
Scheduling Replication 14
Disabling ACS Database Replication 15
Configuring Automatic Change Password Replication 16
Database Replication Event Errors 16
RDBMS Synchronization 17
About RDBMS Synchronization 17
Users 18
User Groups 18
Network Configuration 19
Custom RADIUS Vendors and VSAs 19
RDBMS Synchronization Components 19
About CSDBSync 20
About the accountActions Table 20
ACS Database Recovery Using the accountActions Table 21
Reports and Event (Error) Handling 22
Preparing to Use RDBMS Synchronization 22
Configuring a System Data Source Name for RDBMS Synchronization 23
RDBMS Synchronization Options 24
RDBMS Setup Options 24
Synchronization Scheduling Options 25
Synchronization Partners Options 25
Performing RDBMS Synchronization Immediately 25
Scheduling RDBMS Synchronization 26
Disabling Scheduled RDBMS Synchronizations 28
IP Pools Server 28
About IP Pools Server 28
Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges 29
Refreshing the AAA Server IP Pools Table 30

Adding a New IP Pool 30
Editing an IP Pool Definition 31
Resetting an IP Pool 32
Deleting an IP Pool 32
IP Pools Address Recovery 33
Enabling IP Pool Address Recovery 33

CHAPTER 10 System Configuration: Authentication and Certificates 1
About Certification and EAP Protocols 1
Digital Certificates 1
EAP-TLS Authentication 2
About the EAP-TLS Protocol 2
EAP-TLS and ACS 3
EAP-TLS Limitations 4
Enabling EAP-TLS Authentication 4
PEAP Authentication 5
About the PEAP Protocol 5
PEAP and ACS 6
PEAP and the Unknown User Policy 7
Enabling PEAP Authentication 7
EAP-FAST Authentication 8
About EAP-FAST 8
About Master Keys 10
About PACs 11
Provisioning Modes 12
Types of PACs 12
Master Key and PAC TTLs 15
Replication and EAP-FAST 15
Enabling EAP-FAST 17
Stateless Session Server Resume 18
Global Authentication Setup 19
Configuring Authentication Options 19
ACS Certificate Setup 25
Installing an ACS Server Certificate 25
Adding a Certificate Authority Certificate 27
Editing the Certificate Trust List 27
Managing Certificate Revocation Lists 28
About Certificate Revocation Lists 29
Certificate Revocation List Configuration Options 29

Editing a Certificate Revocation List Issuer 31
Generating a Certificate Signing Request 31
Using Self-Signed Certificates 32
About Self-Signed Certificates 33
Self-Signed Certificate Configuration Options 33
Generating a Self-Signed Certificate 34
Updating or Replacing an ACS Certificate 35

CHAPTER 11 **Logs and Reports** 1
Logging Formats 1
Special Logging Attributes 2
Posture-Validation Attributes in Logs 3
Reporting HCAP Errors 3
Update Packets in Accounting Logs 3
About ACS Logs and Reports 4
Accounting Logs 4
Dynamic Administration Reports 6
Viewing the Logged-in Users Report 7
Deleting Logged-in Users 7
Viewing the Disabled Accounts Report 8
ACS System Logs 8
Configuring the Administration Audit Log 9
Working with CSV Logs 10
CSV Log File Names 10
CSV Log File Locations 10
Enabling or Disabling a CSV Log 11
Viewing a CSV Report 12
Log Filtering 13
Regular Expression Basic Syntax Reference 14
Configuring a CSV Log 14
Working with ODBC Logs 16
Preparing for ODBC Logging 16
Configuring a System Data Source Name for ODBC Logging 17
Configuring an ODBC Log 17
Remote Logging 19
About Remote Logging 19
Implementing Centralized Remote Logging 20
Remote Logging Options 21
Enabling and Configuring Remote Logging 21

Disabling Remote Logging 22
Service Logs 23
Services Logged 23
Configuring Service Logs 24
Helping Customer Support Gather Data 25

CHAPTER 12 **Administrators and Administrative Policy** 1
Administrator Accounts 1
About Administrator Accounts 1
Administrator Privileges 2
Adding an Administrator Account 4
Editing an Administrator Account 5
Unlocking a Locked Out Administrator Account 7
Deleting an Administrator Account 7
Access Policy 8
Access Policy Options 8
Setting Up Access Policy 9
Session Policy 11
Session Policy Options 11
Setting Up Session Policy 11
Audit Policy 12

CHAPTER 13 **User Databases** 1
ACS Internal Database 1
About the ACS Internal Database 2
User Import and Creation 2
About External User Databases 3
Authenticating with External User Databases 4
External User Database Authentication Process 4
Windows User Database 5
Windows User Database Support 6
Authentication with Windows User Databases 6
Trust Relationships 7
Windows Dial-Up Networking Clients 7
Windows Dial-Up Networking Clients with a Domain Field 7
Windows Dial-Up Networking Clients without a Domain Field 7
Usernames and Windows Authentication 8
Username Formats and Windows Authentication 8
Nondomain-Qualified Usernames 9

Domain-Qualified Usernames 9
UPN Usernames 10
EAP and Windows Authentication 10
EAP-TLS Domain Stripping 10
Machine Authentication 11
Machine Access Restrictions 13
Microsoft Windows and Machine Authentication 14
Enabling Machine Authentication 16
User-Changeable Passwords with Windows User Databases 17
Preparing Users for Authenticating with Windows 18
Windows User Database Configuration Options 18
Configuring a Windows External User Database 21
Generic LDAP 22
ACS Authentication Process with a Generic LDAP User Database 23
Multiple LDAP Instances 23
LDAP Organizational Units and Groups 23
Domain Filtering 24
LDAP Failover 25
Successful Previous Authentication with the Primary LDAP Server 25
Unsuccessful Previous Authentication with the Primary LDAP Server 25
LDAP Admin Logon Connection Management 26
Distinguished Name Caching 26
LDAP Configuration Options 26
Configuring a Generic LDAP External User Database 30
ODBC Database 34
What is Supported with ODBC User Databases 35
ACS Authentication Process with an ODBC External User Database 35
Preparing to Authenticate Users with an ODBC-Compliant Relational Database 36
Implementation of Stored Procedures for ODBC Authentication 37
Type Definitions 38
Microsoft SQL Server and Case-Sensitive Passwords 38
Sample Routine for Generating a PAP Authentication SQL Procedure 38
Sample Routine for Generating an SQL CHAP Authentication Procedure 39
Sample Routine for Generating an EAP-TLS Authentication Procedure 39
PAP Authentication Procedure Input 40
PAP Procedure Output 40
CHAP/MS-CHAP/ARAP Authentication Procedure Input 41
CHAP/MS-CHAP/ARAP Procedure Output 41
EAP-TLS Authentication Procedure Input 42
EAP-TLS Procedure Output 42

Result Codes 43
Configuring a System Data Source Name for an ODBC External User Database 43
Configuring an ODBC External User Database 44
LEAP Proxy RADIUS Server Database 46
Configuring a LEAP Proxy RADIUS Server External User Database 47
Token Server User Databases 48
About Token Servers and ACS 49
Token Servers and ISDN 49
RADIUS-Enabled Token Servers 49
About RADIUS-Enabled Token Servers 50
Token Server RADIUS Authentication Request and Response Contents 50
Configuring a RADIUS Token Server External User Database 50
RSA SecurID Token Servers 53
Configuring an RSA SecurID Token Server External User Database 53
Deleting an External User Database Configuration 54

CHAPTER 14 **Posture Validation** 1
What is Posture Validation? 1
Network Access Control Overview 1
Benefits of NAC 2
NAC Architecture Overview 2
Posture Tokens 3
Posture Validation in ACS 4
Configuring NAC in ACS 4
Posture Validation Process 6
Policy Overview 7
About Posture Credentials and Attributes 7
Extended Attributes 8
Internal Policies 9
About Internal Policies 9
About Rules, Rule Elements, and Attributes 10
Internal Policy Configuration Options 10
External Policies 11
About External Policies 11
External Policy Configuration Options 12
NAH Policies 14
About External Audit Servers 14
External Audit Server Configuration Options 16
Configuring Policies 17

Setting Up Posture Validation Policies 18
Creating an Internal Policy 18
Editing a Policy 20
Cloning a Policy or Policy Rule 21
Renaming a Policy 22
Deleting a Policy or Rule 23
Deleting a Condition Component or Condition Set 23
Setting Up an External Policy Server 24
Editing an External Posture Validation Server 25
Deleting an External Posture Validation Server 25
Setting Up an External Audit Posture Validation Server 25
Editing an External Posture Validation Audit Server 26
Deleting an External Posture Validation Server 27
How Posture Validation Fits into Profile-Based Policies 27

CHAPTER 15 **Network Access Profiles** 1
Overview of NAPs 1
Profile-based Policies 2
Configuring Profile-Based Policies 3
Setting Up a Profile 3
Defining User Access Requests 4
NAFs 4
Protocol Types 5
Advanced Filtering 5
About Rules, Rule Elements, and Attributes 6
Configuring Advanced Filtering 7
NAP Administrative Tasks 7
Adding a Profile 7
Ordering Profiles 9
Editing a Profile 9
Cloning a Profile 9
Deleting a Profile 10
Processing Unmatched User Requests 10
NAP Administration Pages 11
Using Profile Templates 13
Shared-profile Components 13
Prerequisites for Using Profile Templates 14
Selecting a Profile Template 14
NAC L3 IP 15

Downloadable ACLs 15
NAC L2 IP 17
ACS and AV Pairs 19
Default ACLs 20
NAC Layer 2 802.1x 20
Microsoft IEEE 802.1x 23
Wireless (NAC L2 802.1x) 24
Authentication Bypass 24
NAC Agentless Host 25
Configuring Policies for Profiles 27
Configuring Authentication Policies 27
Populate from Global 28
Authentication Protocols 28
MAC-Authentication Bypass 29
EAP Configuration 29
EAP-FAST 30
Posture Validation Settings 30
Credential Validation Databases 30
Setting Authentication Policies 30
Configuring MAC Authentication Bypass 31
Configuring Posture-Validation Policies 35
URL Redirect Policy 36
Import Vendor Attribute-Value Pairs (AVPs) 36
Setting a Posture-Validation Policy 37
Deleting a Posture Validation Rule 40
Audit Server Functionality 40
System Posture Token Configuration 40
Mapping an Audit Server to a Profile 40
Posture Validation for Agentless Hosts 41
Configuring Fail Open 41
Runtime Behavior 43
Configuring Authorization Policies 43
Authorization Rules 43
Configuring an Authorization Rule 44
Configuring a Default Authorization Rule 45
Ordering the Authorization Rules 46
Deleting an Authorization Rule 46
Shared RACs 46
RAC and Groups 47
Merging Attributes 47

Troubleshooting Profiles 47
Migrating from Groups to RACs 47
Policy Replication and Backup 48

CHAPTER 16 **Unknown User Policy** 1
Known, Unknown, and Discovered Users 2
Authentication and Unknown Users 3
About Unknown User Authentication 3
General Authentication of Unknown Users 3
Windows Authentication of Unknown Users 4
Domain-Qualified Unknown Windows Users 4
Windows Authentication with Domain Qualification 5
Multiple User Account Creation 5
Performance of Unknown User Authentication 6
Added Authentication Latency 6
Authentication Timeout Value on AAA clients 6
Authorization of Unknown Users 6
Unknown User Policy Options 7
Database Search Order 7
Configuring the Unknown User Policy 8
Disabling Unknown User Authentication 9

CHAPTER 17 **User Group Mapping and Specification** 1
About User Group Mapping and Specification 1
Group Mapping by External User Database 1
Creating an ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database 2
Group Mapping by Group Set Membership 3
Group Mapping Order 3
No Access Group for Group Set Mappings 4
Default Group Mapping for Windows 4
Windows Group Mapping Limitations 4
Creating an ACS Group Mapping for Windows or Generic LDAP Groups 4
Editing a Windows or Generic LDAP Group Set Mapping 6
Deleting a Windows or Generic LDAP Group Set Mapping 7
Deleting a Windows Domain Group Mapping Configuration 7
Changing Group Set Mapping Order 8
RADIUS-Based Group Specification 8

APPENDIX A **Troubleshooting** 1

Administration Issues 2
Browser Issues 3
Cisco NAC Issues 3
Database Issues 6
Dial-in Connection Issues 8
Proxy Issues 11
Installation and Upgrade Issues 11
MaxSessions Issues 11
Report Issues 12
Third-Party Server Issues 14
User Authentication Issues 14
TACACS+ and RADIUS Attribute Issues 15

APPENDIX B **TACACS+ Attribute-Value Pairs** 1

Cisco IOS AV Pair Dictionary 1
TACACS+ AV Pairs 1
TACACS+ Accounting AV Pairs 3

APPENDIX C **RADIUS Attributes** 1

Before Using RADIUS Attributes 1
Cisco IOS Dictionary of RADIUS IETF 2
Cisco IOS/PIX 6.0 Dictionary of RADIUS VSAs 4
About the cisco-av-pair RADIUS Attribute 5
Cisco VPN 3000 Concentrator/ASA/PIX 7.x+ Dictionary of RADIUS VSAs 6
Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs 10
Cisco Building Broadband Service Manager Dictionary of RADIUS VSA 10
Cisco Airespace Dictionary of RADIUS VSA 10
IETF Dictionary of RADIUS IETF (AV Pairs) 11
Microsoft MPPE Dictionary of RADIUS VSAs 19
Ascend Dictionary of RADIUS AV Pairs 21
Nortel Dictionary of RADIUS VSAs 28
Juniper Dictionary of RADIUS VSAs 28

APPENDIX D **CSUtil Database Utility** 1

Location of CSUtil.exe and Related Files 2

CSUtil Command Syntax 2
Backing Up ACS with CSUtil.exe 3
Restoring ACS with CSUtil.exe 4
Creating an ACS Internal Database 5
Creating an ACS Internal Database Dump File 6
Loading the ACS Internal Database from a Dump File 7
Compacting the ACS Internal Database 8
User and AAA Client Import Option 9
Importing User and AAA Client Information 9
User and AAA Client Import File Format 10
About User and AAA Client Import File Format 11
ONLINE or OFFLINE Statement 11
ADD Statements 12
UPDATE Statements 13
DELETE Statements 13
ADD_NAS Statements 14
DEL_NAS Statements 15
Import File Example 15
Exporting User List to a Text File 15
Exporting Group Information to a Text File 16
Decoding Error Numbers 17
User-Defined RADIUS Vendors and VSA Sets 18
About User-Defined RADIUS Vendors and VSA Sets 18
Adding a Custom RADIUS Vendor and VSA Set 18
Deleting a Custom RADIUS Vendor and VSA Set 19
Listing Custom RADIUS Vendors 20
Exporting Custom RADIUS Vendor and VSA Sets 21
RADIUS Vendor/VSA Import File 21
About the RADIUS Vendor/VSA Import File 22
Vendor and VSA Set Definition 22
Attribute Definition 23
Enumeration Definition 24
Example RADIUS Vendor/VSA Import File 24
PAC File Generation 25
PAC File Options and Examples 25
Generating PAC Files 27
Posture-Validation Attributes 28
Posture-Validation Attribute Definition File 28

Exporting Posture-Validation Attribute Definitions 31
Importing Posture-Validation Attribute Definitions 31
Importing External Audit Posture-Validation Servers 33
Deleting a Posture-Validation Attribute Definition 33
Deleting an Extended Posture-Validation Attribute Definition 34
Default Posture-Validation Attribute Definition File 35

APPENDIX E **VPDN Processing** 1
VPDN Process 1

APPENDIX F **RDBMS Synchronization Import Definitions** 1
accountActions Specification 1
accountActions Format 1
accountActions Mandatory Fields 2
accountActions Processing Order 3
Supported Versions for ODBC Datasources 3
Action Codes 3
Action Codes for Setting and Deleting Values 4
Action Codes for Creating and Modifying User Accounts 4
Action Codes for Initializing and Modifying Access Filters 9
Action Codes for Modifying TACACS+ and RADIUS Group and User Settings 12
Action Codes for Modifying Network Configuration 17
ACS Attributes and Action Codes 22
User-Specific Attributes 22
User-Defined Attributes 24
Group-Specific Attributes 24
An Example of accountActions 25

APPENDIX G **Internal Architecture** 1
Windows Services 1
Windows and SQL Registries 2
Windows Registry 2
SQL Registry 2
CSAdmin 3
CSAuth 3
CSDBSync 3
CSLog 4
CSMon 4

Monitoring 4
Recording 5
Notification 5
Response 5
CSTacacs and CSRadius 6

INDEX

Preface

This guide describes Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

Audience

This guide is for system administrators who use ACS, and who set up and maintain accounts and dial-in network security.

Organization

This document contains the following chapters and appendixes:

- **Chapter 1, "Overview"**—An overview of ACS and its features, network diagrams, and system requirements.
- **Chapter 2, "Deployment Considerations"**—A guide to deploying ACS that includes requirements, options, trade-offs, and suggested sequences.
- **Chapter 3, "Using the Web Interface"**—Concepts and procedures regarding how to use the Interface Configuration section of ACS to configure the HTML interface.
- **Chapter 4, "Network Configuration"**—Concepts and procedures for establishing ACS network configuration and building a distributed system.
- **Chapter 5, "Shared Profile Components"**—Concepts and procedures regarding ACS shared profile components: downloadable IP acls, network access filters, network access restrictions, and device command sets.
- **Chapter 6, "User Group Management"**—Concepts and procedures for establishing and maintaining ACS user groups.
- **Chapter 7, "User Management"**—Concepts and procedures for establishing and maintaining ACS user accounts.
- **Chapter 8, "System Configuration: Basic"**—Concepts and procedures regarding the basic features found in the System Configuration section of ACS.
- **Chapter 9, "System Configuration: Advanced"**—Concepts and procedures regarding RDBMS Synchronization, CiscoSecure Database Replication, and IP pools, found in the System Configuration section of ACS.

- **Chapter 10, "System Configuration: Authentication and Certificates"**—Concepts and procedures regarding the Global Authentication and ACS Certificate Setup pages, found in the System Configuration section of ACS.
- **Chapter 11, "Logs and Reports"**—Concepts and procedures regarding ACS logging and reports.
- **Chapter 12, "Administrators and Administrative Policy"**—Concepts and procedures for establishing and maintaining ACS administrators.
- **Chapter 13, "User Databases"**—Concepts about user databases and procedures for configuring ACS to perform user authentication with external user databases.
- **Chapter 14, "Posture Validation"**—Concepts and procedures for implementing Posture Validation (also known as Network Admission Control or NAC) and configuring posture validation policies.
- **Chapter 15, "Network Access Profiles"**—Concepts and procedures for creating Network Access Profiles and implementing profile-based policies in ACS.
- **Chapter 16, "Unknown User Policy"**—Concepts and procedures about using the Unknown User Policy with posture validation and unknown user authentication.
- **Chapter 17, "User Group Mapping and Specification"**—Concepts and procedures regarding the assignment of groups for users authenticated by an external user database.
- **Appendix A, "Troubleshooting"**—How to identify and solve certain problems you might have with ACS.
- **Appendix B, "TACACS+ Attribute-Value Pairs"**—A list of supported TACACS+ AV pairs and accounting AV pairs.
- **Appendix C, "RADIUS Attributes"**—A list of supported RADIUS AV pairs and accounting AV pairs.
- **Appendix D, "CSUtil Database Utility"**—Instructions for using CSUtil.exe, a command line utility you can use to work with the CiscoSecure user database, to import AAA clients and users, to define RADIUS vendors and attributes, and to generate PAC files for EAP-FAST clients.
- **Appendix E, "VPDN Processing"**—An introduction to Virtual Private Dial-up Networks (VPDN), including stripping and tunneling, with instructions for enabling VPDN on ACS.
- **Appendix F, "RDBMS Synchronization Import Definitions"**—A list of import definitions, for use with the RDBMS Synchronization feature.
- **Appendix G, "Internal Architecture"**—A description of ACS architectural components.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	**boldface** font
Variables for which you supply values and new or important terminology	*italic* font
Displayed session and system information, paths and file names	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*italic screen* font

Item	Convention
Menu items and button names	**boldface** font
Indicates menu items to select, in the order you select them.	**Option > Network Preferences**

Tip Identifies information to help you get the most benefit from your product.

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.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

Warning **Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.**

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
Finding Documentation for Cisco Secure ACS for Windows	• Shipped with product. • PDF on the product CD-ROM. • On Cisco.com.
Release Notes for Cisco Secure ACS for Windows	• On Cisco.com.
Installation Guide for Cisco Secure ACS for Windows	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816991=).[1]

Table 1 Product Documentation (continued)

Document Title	Available Formats
User Guide for Cisco Secure ACS for Windows	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816992=).[1]
Installation and User Guide for Cisco Secure ACS User-Changeable Passwords	• PDF on the product CD-ROM. • On Cisco.com.
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows	• On Cisco.com.
Online Documentation	In the ACS HTML interface, click Online Documentation.
Online Help	In the ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature.

1. See Obtaining Documentation, page 28.

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

A set of white papers about ACS are available on Cisco.com at:

http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml

For information on Network Admission Control, various NAC components, and ACS see:

http://www.cisco.com/go/nac

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview

This chapter contains an overview of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

The following topics are presented:

- Introduction to ACS, page 1-1
- ACS Features, Functions and Concepts, page 1-2
- Managing and Administrating ACS, page 1-15
- ACS Specifications, page 1-19

Introduction to ACS

ACS is a scalable, high-performance Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+) security server. As the centralized control point for managing enterprise network users, network administrators, and network infrastructure resources, ACS provides a comprehensive identity-based network-access control solution for Cisco intelligent information networks.

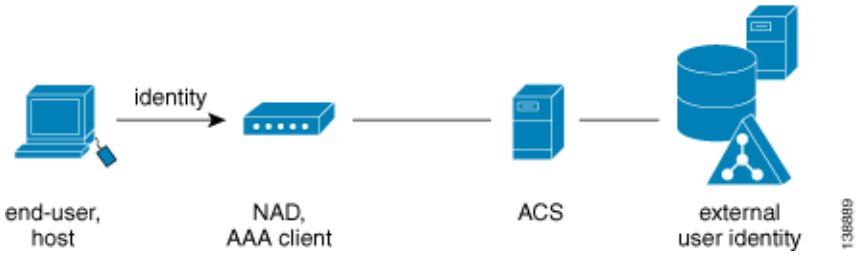
ACS extends network-access security by combining traditional authentication, authorization, and accounting (AAA - pronounced “triple A”) with policy control. ACS enforces a uniform network-access security policy for network administrators and other network users.

ACS supports a broad variety of Cisco and other network-access devices (NADs), also known as AAA clients, including:

- Wired and wireless LAN switches and access points
- Edge and core routers
- Dialup and broadband terminators
- Content and storage devices
- Voice over IP
- Firewalls
- Virtual private networks (VPNs)

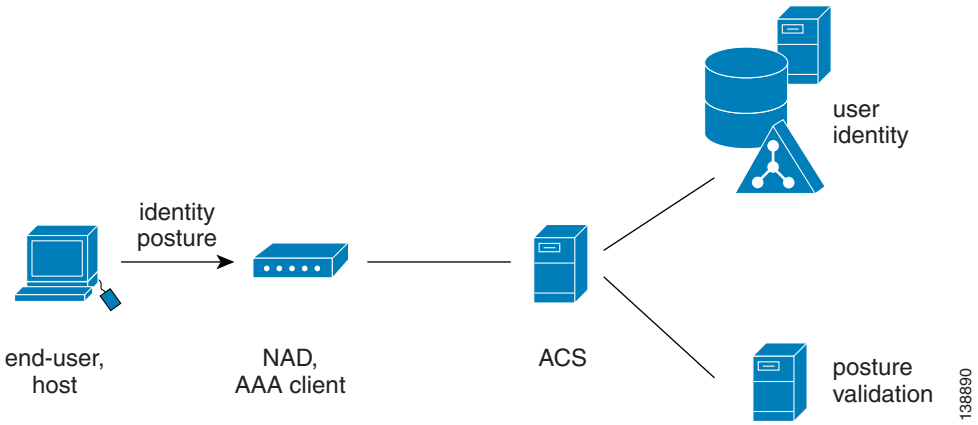
Figure 1-1 on page 1-2 illustrates the role of ACS as a traditional network access control/AAA server.

Figure 1-1 A Simple AAA Scenario



ACS is a critical component of the Cisco Network Admission Control (NAC) framework. Cisco NAC is a Cisco Systems-sponsored industry initiative that uses the network infrastructure to enforce security-policy compliance on all machines seeking to access network computing resources, thereby limiting damage from viruses and worms. With NAC, network access to compliant and trusted PCs can be permitted, while the access of noncompliant devices can be restricted. See Figure 1-2.

Figure 1-2 ACS Extended to NAC



ACS is also an important component of the Cisco Identity-Based Networking Services (IBNS) architecture. Cisco IBNS is based on Extensible Authentication Protocol (EAP) and on port-security standards such as IEEE 802.1x (a standard for port-based network-access control) to extend security authentication, authorization, and accounting from the perimeter of the network to every connection point inside the LAN. New policy controls such as per-user quotas, virtual LAN (VLAN) assignments, and access-control lists (ACLs) can be deployed, due to the extended capabilities of Cisco switches and wireless access points to query ACS over the RADIUS protocol.

ACS Features, Functions and Concepts

ACS incorporates many technologies to render AAA services to network-access devices, and provides a central access-control function.

This section contains the following topics:

- ACS as the AAA Server, page 1-3
- AAA Protocols—TACACS+ and RADIUS, page 1-3
- Additional Features in ACS Version 4.0, page 1-4

ACS as the AAA Server

From the perspective of the NAD, ACS functions as the AAA server. You must configure the device, which functions as a AAA client from the ACS perspective, to direct all end-user host access requests to ACS, via the TACACS+ or RADIUS protocols.

TACACS+ is traditionally used to provide authorization for network administrative operations on the network infrastructure itself; RADIUS is universally used to secure the access of end-users to network resources.

Basically, 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 its internal database or one of the configured external identity directories. ACS ultimately responds to the NAD with an access denied or an access-accept message with a set of authorization attributes. When ACS is used in the context of the NAC architecture, additional machine data, known as *posture*, is validated as well, before the user is granted access to the network.

AAA Protocols—TACACS+ and RADIUS

ACS can use the TACACS+ and RADIUS AAA protocols.

Table 1-1 compares the two protocols.

Table 1-1 TACACS+ and RADIUS Protocol Comparison

Point of Comparison	TACACS+	RADIUS
Transmission Protocol	TCP—Connection-oriented transport-layer protocol, reliable full-duplex data transmission	UDP—Connectionless transport-layer protocol, datagram exchange without acknowledgments or guaranteed delivery
Ports Used	49	Authentication and Authorization: 1645 and 1812 Accounting: 1646 and 1813
Encryption	Full packet encryption	Encrypts only passwords up to 16 bytes
AAA Architecture	Separate control of each service: authentication, authorization, and accounting	Authentication and authorization combined as one service
Intended Purpose	Device management	User access control

TACACS+

ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.78. For more information, refer to the Cisco IOS software documentation at http://www.cisco.com.

RADIUS

ACS conforms to the RADIUS protocol as defined in the draft of April 1997 and in the following Requests for Comments (RFCs):

- RFC 2138, Remote Authentication Dial In User Service
- RFC 2139, RADIUS Accounting
- RFC 2284

- RFC 2865
- RFC 2866
- RFC 2867
- RFC 2868
- RFC 2869

The ports used for authentication and accounting have changed in RADIUS RFC documents. To support the older and newer RFCs, ACS accepts authentication requests on port 1645 and port 1812. For accounting, ACS accepts accounting packets on port 1646 and 1813.

In addition to support for standard Internet Engineering Task Force (IETF) RADIUS attributes, ACS includes support for RADIUS vendor-specific attributes (VSAs). We have predefined the following RADIUS VSAs in ACS:

- Cisco Building Broadband Service Manager (BBSM)
- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+
- Cisco VPN 5000
- Cisco Airespace
- Ascend
- Juniper
- Microsoft
- Nortel

ACS also supports up to 10 RADIUS VSAs that you define. After you define a new RADIUS VSA, you can use it as you would one of the RADIUS VSAs that come predefined in ACS. In the Network Configuration section of the ACS web interface, you can configure AAA clients to use a user-defined RADIUS VSA as the AAA protocol. In Interface Configuration, you can enable user-level and group-level attributes for user-defined RADIUS VSAs. In User Setup and Group Setup, you can configure the values for enabled attributes of a user-defined RADIUS VSA.

For more information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-19.

Additional Features in ACS Version 4.0

ACS version 4.0 provides the following features that help fortify and protect networked business systems:

- **Cisco NAC support**—ACS 4.0 acts as a policy decision point in NAC deployments. Using configurable policies, it evaluates and validates the credentials received from the Cisco Trust Agent (CTA, posture), determines the state of the host, and sends a per-user authorization to the network-access device: ACLs, a policy based access control list, or a private VLAN assignment. Evaluation of the host credentials can enforce many specific policies, such as OS patch level and antivirus DAT file version. ACS records the policy evaluation result for use with monitoring systems. ACS 4.0 also allows hosts without the appropriate agent technology to be audited by third party Audit Vendors, before granting network access. ACS policies can be extended with external policy servers to which ACS forwards posture credentials. For example, credentials specific to an

antivirus vendor can be forwarded to the vendor's antivirus policy server, and audit policy requests can be forwarded to third-party audit products. For more information, see Chapter 14, "Posture Validation."

- **Scalability improvements**—ACS 4.0 has been upgraded to use an industry standard relational database management system (RDBMS), improving the number of devices (AAA clients) by tenfold and the number of users by threefold. There have also been significant improvements in performance (transactions per second) across the protocol portfolio that ACS supports.
- **Network Access Profiles**—ACS 4.0 supports a new feature called Network Access Profiles (NAPs). Profiles allow administrators to classify access requests according to network location, membership in a network device group (NDG), protocol type, or other specific RADIUS attribute values sent by the network-access device through which the user connects. You can map AAA policies to specific profiles. For example, you can apply a different access policy for wireless access and remote (VPN) access. For more information, see Chapter 15, "Network Access Profiles."
- **Extended replication components**—ACS 4.0 has improved and enhanced replication. Administrators now can replicate NAPs, and all related configurations, including:
  - Posture Validation settings
  - AAA clients and hosts
  - external database configuration
  - global authentication configuration
  - Network Device Groups
  - dictionaries
  - shared-profile components
  - additional logging attributes
- **EAP-Flexible Authentication via Secure Tunneling (FAST) enhanced support** — EAP-FAST is a new, publicly accessible IEEE 802.1x EAP type that Cisco developed to support customers who cannot enforce a strong password policy; or, who want to deploy an 802.1x EAP type that:
  - does not require digital certificates
  - supports a variety of user and password database types
  - supports password expiration and change
  - is flexible
  - is easy to deploy
  - is easy to manage

  For example, a customer who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks. ACS 4.0 adds support for EAP-FAST supplicants available on a wide variety of wireless client adapters.
- **Downloadable IP ACLs** — ACS 4.0 extends per-user ACL support to any Layer 3 network device that supports this feature, such as Cisco PIX® firewalls, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that can be applied per user or per group. This feature complements NAC support by enforcing the correct ACL policy. When used in conjunction with network-access filters (NAFs), you can apply downloadable ACLs differently per device. You can, therefore, tailor ACLs uniquely per user, per access device.
- **Certification Revocation List (CRL) Comparison**—ACS 4.0 supports certificate revocation by using the X.509 CRL profile. A CRL is a time-stamped list identifying revoked certificates; the list is signed by a certificate authority or CRL issuer, and made freely available in a public repository.

ACS 4.0 periodically retrieves the CRLs from provisioned CRL Distribution Points by using Lightweight Directory Access Protocol (LDAP) or HyperText Transfer Protocol (HTTP), and stores them for use during EAP-Transport Layer Security (EAP-TLS) authentication. If the retrieved CRL contains the certificate that the user presents during an EAP-TLS authentication, ACS fails the authentication and denies access to the user. This capability is crucial due to frequent organizational changes and protects valuable company assets in case of fraudulent network use.

- **Machine Access Restrictions (MAR)**—ACS 4.0 includes MARs as an enhancement of Windows machine authentication. When Windows machine authentication is enabled, you can use MARs to control authorization of EAP-TLS, EAP-FASTv1a, and Microsoft Protected Extensible Authentication Protocol (PEAP) users who authenticate with a Windows external user database. Users who access the network with a computer that has not passed machine authentication within a configurable length of time are given the authorizations of a user group that you specify and which you can configure to limit authorization as needed. Alternatively, you can deny network access altogether.
- **Network Access Filter (NAF)**—ACS 4.0 includes NAFs as a new type of Shared Profile Component. NAFs provide a flexible way to apply network-access restrictions and downloadable ACLs on network device names, network device groups, or their IP address. NAFs applied by IP addresses can use IP address ranges and wildcards. This feature introduces granular application of network-access restrictions and downloadable ACLs, which previously supported only the use of the same access restrictions or ACLs to all devices. You can use NAFs to define flexible network device restriction policies to be defined, a requirement that is common in large environments.

Authentication

Authentication determines user identity and verifies the information. Traditional authentication uses a name and a fixed password. More secure methods use technologies such as Challenge Authentication Handshake Protocol (CHAP) and One-time Passwords (OTPs). 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.

This section contains the following topics:

- Authentication Considerations, page 1-6
- Authentication and User Databases, page 1-7
- Authentication Protocol-Database Compatibility, page 1-7
- Passwords, page 1-8
- Other Authentication-Related Features, page 1-11

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 capturing 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, such as:

- 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 User Database
- Generic LDAP
- Open Database Connectivity (ODBC)-compliant relational databases
- Rivest, Shamir, and Adelman (RSA) SecurID Token Server
- RADIUS-compliant token servers

Note For more information about token server support, see Token Server User Databases, page 13-48.

Authentication Protocol-Database Compatibility

The various password protocols that ACS supports for authentication are supported unevenly by the various databases that ACS supports. For more information about the password protocols that ACS supports, see Passwords, page 1-8.

Note This release does not support Windows NT.

Table 1-2 specifies non-EAP authentication protocol support.

Table 1-2 Non-EAP Authentication Protocol and User Database Compatibility

Database	ASCII/PAP	CHAP	ARAP	MS-CHAP v.1	MS-CHAP v.2
ACS	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes
Windows AD	Yes	No	No	Yes	Yes
LDAP	Yes	No	No	No	No
ODBC	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes
All Token Servers	Yes	No	No	No	No

Table 1-3 specifies EAP authentication protocol support.

Table 1-3 EAP Authentication Protocol and User Database Compatibility

Database	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MS CHAPv2)	EAP-FAST Phase Zero	EAP-FAST Phase Two
ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes	Yes	Yes
Windows AD	Yes	No	Yes	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	Yes	No	No	Yes
ODBC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes	Yes	Yes
All Token Servers	No	No	No	Yes	No	No	No

Passwords

ACS supports many common password protocols:

- ASCII/Password Authentication Protocol (ASCII/PAP)
- CHAP
- MS-CHAP
- Lightweight and Efficient Application Protocol (LEAP)
- EAP-MD5
- EAP-TLS
- PEAP(EAP-GTC)
- PEAP(EAP-MSCHAPv2)
- EAP-FAST
- AppleTalk Remote Access Protocol (ARAP)

Passwords can be processed by using these password-authentication protocols based on the version and type of security-control protocol used (for example, RADIUS or TACACS+), and the configuration of the AAA client and end-user client. The following sections outline the different conditions and functions of password handling.

In the case of token servers, ACS acts as a client to the token server by using its proprietary API or its RADIUS interface, depending on the token server. For more information, see About Token Servers and ACS, page 13-49.

Different levels of security can be concurrently used with ACS for different requirements. The basic user-to-network security level is PAP. Although it represents the unencrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows database. With this configuration, users need to log in only once. CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client. You can use CHAP with the ACS internal database. ARAP support is included to support Apple clients.

Comparing PAP, CHAP, and ARAP

PAP, CHAP, and ARAP are authentication protocols that encrypt passwords. However, each protocol provides a different level of security.

- **PAP**—Uses clear-text passwords (that is, unencrypted passwords) and is the least sophisticated authentication protocol. If you are using the Windows user database to authenticate users, you must use PAP password encryption or Microsoft-Challenge Authentication Handshake Protocol (MS-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.
- **ARAP**—Uses a two-way challenge-response mechanism. The AAA client challenges the end-user client to authenticate itself, and the end-user client challenges the AAA client to authenticate itself.

MS-CHAP

ACS supports MS-CHAP for user authentication. Differences between MS-CHAP and standard CHAP are:

- The MS-CHAP Response packet is in a format compatible with Microsoft Windows and LAN Manager 2.x. The MS-CHAP format does not require the authenticator to store a clear-text or reversibly encrypted password.
- MS-CHAP provides an authentication-retry mechanism that the authenticator controls.
- MS-CHAP provides additional failure codes in the Failure packet Message field.

For more information on MS-CHAP, refer to RFC 2433 Microsoft PPP CHAP Extensions for RADIUS Attributes for MS-CHAP Support.

EAP Support

The EAP, based on IETF 802.1x, is an end-to-end framework that allows the creation of authentication types without changing AAA client configurations. For more information about EAP, see RFC 2284, PPP Extensible Authentication Protocol (EAP).

ACS supports the following varieties of EAP:

- **EAP-MD5**—An EAP protocol that does not support mutual authentication.
- **EAP-TLS**—EAP incorporating Transport Layer Security. For more information, see EAP-TLS Deployment Guide for Wireless LAN Networks and EAP-TLS Authentication, page 10-2.
- **LEAP**—An EAP protocol used by Cisco Aironet wireless equipment; it supports mutual authentication.
- **PEAP**—Protected EAP, which is implemented with EAP-Generic Token Card (GTC) and EAP-MS-CHAPv2 protocols. For more information, see PEAP Authentication, page 10-5.
- **EAP-FAST**—A faster means of encrypting EAP authentication, supports EAP-GTC authentication. For more information, see EAP-FAST Authentication, page 10-8.

The architecture of ACS is extensible with regard to EAP; additional varieties of EAP will be supported as those protocols mature.

Basic Password Configurations

Several basic password configurations are available:

Note These configurations are all classed as inbound authentication.

- **Single password for ASCII/PAP/CHAP/MS-CHAP/ARAP**—The most convenient method for the administrator when setting up accounts and the user when obtaining authentication. However, because the CHAP password is the same as the PAP password, and the PAP password is transmitted in clear text during an ASCII/PAP login, the CHAP password could be compromised.
- **Separate passwords for ASCII/PAP and CHAP/MS-CHAP/ARAP**—For a higher level of security, users can have two separate passwords. If the ASCII/PAP password is compromised, the CHAP/ARAP password can remain secure.
- **External user database authentication**—For authentication by an external user database, the user does not need a password stored in the ACS internal database. Instead, ACS records which external user database it should query to authenticate the user.

Advanced Password Configurations

ACS supports the following advanced password configurations:

- **Inbound passwords**—Passwords used by most ACS users. The TACACS+ and RADIUS protocols support these passwords. The passwords held in the ACS internal database and are not usually provided to an external source if an outbound password has been configured.
- **Outbound passwords**—The TACACS+ protocol supports outbound passwords that can be used, for example, when another AAA client and end-user client authenticate a AAA client. Passwords from the ACS internal database are then sent to the second AAA client and end-user client.
- **Token caching**—When token caching is enabled, ISDN users can connect (for a limited time) a second B Channel by using the same OTP that was entered during original authentication. For greater security, the B-Channel authentication request from the AAA client should include the OTP in the username value (for example, Fred*password*) while the password value contains an ASCII/PAP/ARAP password. The TACACS+ and RADIUS servers then verify that the token is still cached and validate the incoming password against the single ASCII/PAP/ARAP or separate CHAP/ARAP password, depending on the configuration that the user employs.

  The TACACS+ SENDAUTH feature enables AAA clients to authenticate themselves to other AAA clients or an end-user clients via outbound authentication. The outbound authentication can be PAP, CHAP, or ARAP. With outbound authentication, the ACS password is given out. By default, ASCII/PAP or CHAP/ARAP password is used, depending on how this has been configured; however, we recommend that you configure the separate SENDAUTH password for the user so that ACS inbound passwords are never compromised.

If you want to use outbound passwords and maintain the highest level of security, we recommend that you configure users in the ACS internal user database with an outbound password that is different from the inbound password.

Password Aging

With ACS you can choose whether and how to employ password aging. Control for password aging may reside in the ACS internal database, or in an external Windows user database. Each password-aging mechanism differs as to requirements and setting configurations.

You use the password aging feature the ACS internal database controls to force users to change their passwords under any of the following conditions:

- Date exceeds: value (a date).
- After a specified number of logins.
- The first time a new user logs in.

For information on the requirements and configuration of the password aging feature that the ACS internal database controls, see Enabling Password Aging for the ACS Internal Database, page 6-15.

You use the Windows-based password aging feature to control the following password aging parameters:

- Maximum password age in days.
- Minimum password age in days.

The methods and functionality of Windows password aging differ according to the Windows operating system release. For information on the requirements and configuration of the Windows-based password aging feature, see Enabling Password Aging for Users in Windows Databases, page 6-19, and refer to your Windows system documentation.

User-Changeable Passwords

With ACS, you can install a separate program so that users can change their passwords by using a web-based utility. For more information about installing user-changeable passwords, see the *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords*.

Other Authentication-Related Features

In addition to the authentication-related features discussed in this section, ACS provides additional features:

- Authentication of unknown users with external user databases. (See About Unknown User Authentication, page 16-3.)
- Authentication of computers running Microsoft Windows. (See Machine Authentication, page 13-11.)
- Support for the Microsoft Windows Callback feature. (See Setting the User Callback Option, page 7-6.)
- Ability to configure user accounts, including passwords, by using an external data source. (See About RDBMS Synchronization, page 9-17.)
- Ability for external users to authenticate via an enable password. (See Setting TACACS+ Enable Password Options for a User, page 7-23.)
- Proxy of authentication requests to other AAA servers. (See Proxy in Distributed Systems, page 4-3.)
- Configurable character string stripping from proxied authentication requests. (See Stripping, page 4-4.)

- Self-signed server certificates. (See Using Self-Signed Certificates, page 10-32.)
- Certificate revocation list checking during EAP-TLS authentication. (See Managing Certificate Revocation Lists, page 10-28.)

Authorization

Authorization determines what a user is allowed to do. ACS can send user profile policies to AAA clients to determine which network services the user can access. You can configure authorization to give different users and groups different levels of service. For example, standard dial-up users might not have the same access privileges as premium customers and users. You can also differentiate by levels of security, access times, and services.

You can use the ACS access restrictions feature to permit or deny logins based on time-of-day and day-of-week. For example, you could create a group for temporary accounts that you can disable on specified dates. A service provider could then offer a 30-day free trial. You could use the same authorization to create a temporary account for a consultant with login permission that is limited to Monday through Friday, 9 A.M. to 5 P.M.

You can restrict users to a service or combination of services such as PPP, ARAP, Serial Line Internet Protocol (SLIP), or EXEC. After a user selects a service, you can restrict Layer 2 and Layer 3 protocols, such as IP and IPX, and you can apply individual access lists. Access lists on a per-user or per-group basis can restrict users from reaching parts of the network where critical information is stored or prevent them from using certain services, such as File Transfer Protocol (FTP) or Simple Network Management Protocol (SNMP).

One fast-growing service that providers offer and corporations adopt is a service authorization for Virtual Private Dial-Up Networks (VPDNs). ACS can provide information to the network device for a specific user to configure a secure tunnel through a public network, such as the Internet. The information can be for the access server (such as the home gateway for that user) or for the home gateway router to validate the user at the customer premises. In either case, ACS can be used for each end of the VPDN.

This section contains the following topics:

- Max Sessions, page 1-12
- Dynamic Usage Quotas, page 1-13
- Shared Profile Components, page 1-13
- Support for Cisco Device-Management Applications, page 1-13
- Other Authorization-Related Features, page 1-14

Max Sessions

Max Sessions is a useful feature for organizations that need to limit the number of concurrent sessions that are available to a user or a group:

- **User Max Sessions**—For example, an Internet service provider can limit each account holder to a single session.
- **Group Max Sessions**—For example, an enterprise administrator can allow the remote access infrastructure to be shared equally among several departments and limit the maximum number of concurrent sessions for all users in any one department.

In addition to enabling simple User and Group Max Sessions control, as an administrator you can use ACS to specify a Group Max Sessions value and a group-based User Max Sessions value; that is, a User Max Sessions value based on the group membership of the user. For example, an administrator can

allocate a Group Max Sessions value of 50 to the group *Sales* and also limit each member of the *Sales* group to five sessions each. Therefore, no single member of a group account would be able to use more than five sessions at any one time, but the group could still have up to 50 active sessions.

For more information about the Max Sessions feature, see Setting Max Sessions for a User Group, page 6-9 and Setting Max Sessions Options for a User, page 7-11.

Dynamic Usage Quotas

You can use ACS to define network usage quotas for users. Using quotas, you can limit the network access of each user in a group or of individual users. You define quotas by duration of sessions or the total number of sessions. Quotas can be absolute; or based on daily, weekly, or monthly periods. To grant access to users who have exceeded their quotas, you can reset session quota counters as needed.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off and the accounting stop packet is received from the AAA client. If the AAA client through which the user is accessing your network fails, the session information is not updated. In the case of multiple sessions, such as with ISDN, the quota would not be updated until all sessions terminate, which means that a second channel will be accepted; even if the first channel has exhausted the quota that is allocated to the user.

For more information about usage quotas, see Setting Usage Quotas for a User Group, page 6-10 and Options for Setting User Usage Quotas, page 7-12.

Shared Profile Components

ACS provides a means for specifying authorization profile components that you can apply to multiple user groups and users. For example, you may have multiple user groups that have identical network-access restrictions. Rather than configuring the network-access restrictions several times, once per group, you can configure a network-access restriction set in the Shared Profile Components section of the web interface, and then configure each group to use the network-access restriction set that you created.

For information about the types of shared-profile components that ACS supports, see About Shared Profile Components, page 5-1.

Support for Cisco Device-Management Applications

ACS supports Cisco device-management applications, such as 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-authorization set types for each management application that is configured to use ACS for authorization.

ACS uses TACACS+ to communicate with management applications. For a management application to communicate with ACS, you must configure the management application in ACS as a AAA client that uses TACACS+. Also, you must 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.

Additionally, the administrator that the management application uses must have the Create New Device Command Set Type privilege enabled. When a management application initially communicates with ACS, it dictates to ACS the creation of a device command set type, which appears in the Shared Profile Components section of the web interface. It also dictates a custom service for TACACS+ to authorize. The custom service appears on the TACACS+ (Cisco IOS) page in the Interface Configuration section

of the web interface. For information about enabling TACACS+ services, see Protocol Configuration Options for TACACS+, page 3-7. For information about device command-authorization sets for management applications, see Command Authorization Sets, page 5-24.

After the management application has dictated the custom TACACS+ service and device command-authorization set type to ACS, you can configure command-authorization sets for each role that the management application supports and apply those sets to user groups that contain network administrators or to individual users who are network administrators.

Other Authorization-Related Features

In addition to the authorization-related features discussed in this section, ACS provides these additional features:

- Group administration of users. (See Chapter 6, "User Group Management.")
- Ability to map a user from an external user database to a specific ACS group. (See Chapter 17, "User Group Mapping and Specification.")
- Ability to disable an account after a number of failed attempts, specified by the administrator. (See Setting Options for User Account Disablement, page 7-13.)
- Ability to disable an account on a specific date. (See Setting Options for User Account Disablement, page 7-13.)
- Ability to disable groups of users. (See Group Disablement, page 6-3.)
- Ability to restrict time-of-day and day-of-week access. (See Setting Default Time-of-Day Access for a User Group, page 6-5.)
- Network access restrictions (NARs) based on remote address caller line identification (CLID) and dialed number identification service (DNIS.) (See Setting Network Access Restrictions for a User Group, page 6-6.)
- Downloadable ACLs for users or groups, enabling centralized, modular ACL management. (See Downloadable IP ACLs, page 5-13.)
- Network access filters, which apply different downloadable ACLs and NARs based on a user's point of entry into your network. (See Network Access Filters, page 5-2.)
- Ability to enable or disable users based on the Network Access Profile configuration. (See Configuring Authorization Policies, page 15-43.)
- IP pools for IP address assignment of end-user client hosts. (See Setting IP Address Assignment Method for a User Group, page 6-21.)
- Per-user and per-group TACACS+ or RADIUS attributes. (See Advanced Options, page 3-5.)
- Support for Voice-over-IP (VoIP), including configurable logging of accounting data. (See Enabling VoIP Support for a User Group, page 6-4.)

Accounting

AAA clients use the accounting functions that the RADIUS and TACACS+ protocols provide to communicate relevant data for each user session to the AAA server for recording. ACS writes accounting records to a comma-separated value (CSV) log file or ODBC database, depending on your configuration. You can easily import these logs into popular database and spreadsheet applications for billing, security audits, and report generation. You can also use a third-party reporting tool to manage accounting data.

The types of accounting logs that you can generate include:

- **TACACS+ Accounting**—Lists when sessions start and stop; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **RADIUS Accounting**—Lists when sessions stop and start; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **Administrative Accounting**—Lists commands entered on a network device with TACACS+ command authorization enabled.

For more information about ACS logging capabilities, see Chapter 11, "Logs and Reports."

Other Accounting-Related Features

In addition to the accounting-related features in this section, ACS provides these additional features:

- Centralized logging, allowing several ACS installations to forward their accounting data to a remote ACS. (See Remote Logging, page 11-19.)
- Configurable supplementary user ID fields for capturing additional information in logs. (See User Data Configuration Options, page 3-4.)
- Configurable logs, allowing you to capture as much information as needed. (See Accounting Logs, page 11-4.)

Managing and Administrating ACS

ACS provides a flexible administration scheme to configure, maintain, and protect its AAA functionality. You can perform nearly all ACS administration tasks through the ACS web interface. You use the web interface to easily modify the ACS configuration from any connection on your LAN or WAN, and view it by using a web browser. For a list of supported browsers, see the latest version of the Release Notes for ACS Windows on http://www.cisco.com.

The web interface not only makes viewing and editing user and group information possible, you use it to restart services, add remote administrators, change AAA client information, back up the system, view reports from anywhere on the network, and more.

This section describes the ACS web interface and provides information about the following topics:

- Web Interface Security, page 1-15
- HTTP Port Allocation for Administrative Sessions, page 1-16
- Web Interface Layout, page 1-16
- Uniform Resource Locator for the Web Interface, page 1-18
- Online Help and Online Documentation, page 1-18

Web Interface Security

Accessing the web interface requires a valid administrator name and password. The ACS Login page encrypts the administrator credentials before sending them to ACS.

Administrative sessions time out after a configurable length of idle time. Regardless, we recommend that you log out of the web interface after each session. For information about configuring the idle timeout feature, see Access Policy, page 12-8.

You can enable a secure socket layer (SSL) for administrative sessions. This method ensures that all communication between the web browser and ACS is encrypted. Your browser must support SSL. You can enable this feature on the Access Policy Setup page in the Administration Control section. For more information about enabling the SSL for web interface security, see Access Policy, page 12-8.

HTTP Port Allocation for Administrative Sessions

You use the HTTP port allocation feature to configure the range of TCP ports that ACS uses for administrative HTTP sessions. Narrowing this range with the HTTP port allocation feature reduces the risk of unauthorized access to your network through a port that is open for administrative sessions.

We do not recommend that you administer ACS through a firewall. Doing so requires that you configure the firewall to permit HTTP traffic over the range of HTTP administrative session ports that ACS uses. While narrowing this range reduces the risk of unauthorized access, a greater risk of attack remains if you allow administration of ACS from outside a firewall. A firewall that is configured to permit HTTP traffic over the ACS administrative port range must also permit HTTP traffic through port 2002, because a web browser must address this port to initiate an administrative session.

Note A broad HTTP port range could create a security risk. To prevent accidental discovery of an active administrative port by unauthorized users, keep the HTTP port range as narrow as possible. ACS tracks the IP address that is associated with each administrative session. An unauthorized user would have to impersonate, or "spoof," the IP address of the legitimate remote host to make use of the active administrative session HTTP port.

For information about configuring the HTTP port allocation feature, see Access Policy, page 12-8.

Web Interface Layout

The web interface has three vertical partitions, known as frames:

- **Navigation Bar**—The gray frame on the left side of the browser window, the navigation bar contains the task buttons. Each button changes the configuration area to a unique section of the ACS application, such as the User Setup section or the Interface Configuration section. This frame does not change; it always contains the following buttons:
  - **User Setup**—Add and edit user profiles. For more information about the User Setup section, see Chapter 7, "User Management."
  - **Group Setup**—Configure network services and protocols for groups of users. For more information about the Group Setup section, see Chapter 6, "User Group Management."
  - **Shared Profile Components**—Add and edit network-access restriction and command-authorization sets, to be applied to users and groups. For more information about the Shared Profile Components section, see Chapter 5, "Shared Profile Components."
  - **Network Configuration**—Add and edit network-access devices and configure distributed systems. For more information about the Network Configuration section, see Chapter 4, "Network Configuration."
  - **System Configuration**—Configure system-level features. Four chapters address this large section of the web interface. For information about fundamental features such as backup scheduling and service controls, see Chapter 8, "System Configuration: Basic." For information about advanced features such as database replication, see Chapter 9, "System Configuration:

Advanced." For information about configuring authentication protocols and certificate-related features, see Chapter 10, "System Configuration: Authentication and Certificates." For information about configuring logs and reports, see Chapter 11, "Logs and Reports."

- **Interface Configuration**—Display or hide product features and options to configure. For more information about the Interface Configuration section, Chapter 3, "Using the Web Interface."
- **Administration Control**—Define and configure access policies. For more information about the Administration Control section, Chapter 12, "Administrators and Administrative Policy."
- **External User Databases**—Configure databases, the Unknown User Policy, and user group mapping. For information about configuring databases, see Chapter 13, "User Databases." For information about the Unknown User Policy, see Chapter 16, "Unknown User Policy." For information about user group mapping, see Chapter 17, "User Group Mapping and Specification."
- **Posture Validation**—Control the degree of access that is permitted from computers that access your network through AAA clients that are configured to enforce NAC. For more information on posture validation, see Chapter 14, "Posture Validation."
- **Network Access Profiles**—Set up the conditions that allow a user to connect to the network and identify the way requests to access the network are applied. For more information on setting up Network Access Profiles and Profile-based Policies, see Chapter 15, "Network Access Profiles."
- **Reports and Activity**—Display accounting and logging information. For information about viewing reports, see Chapter 11, "Logs and Reports."
- **Online Documentation**—View the user guide. For information about using the online documentation, see Online Help and Online Documentation, page 1-18.

- **Configuration Area**—The frame in the middle of the browser window, the configuration area displays web pages that belong to one of the sections represented by the buttons in the navigation bar. The configuration area is where you add, edit, or delete information. For example, you configure user information in this frame on the User Setup Edit page.

Note Most pages have a Submit button at the bottom. Click Submit to confirm your changes. If you do not click Submit, the changes are not saved.

- **Display Area**—The frame on the right side of the browser window, the display area shows one of the following options:
  - **Online Help**—Displays basic help about the page that currently appears in the configuration area. This help does not offer in-depth information, rather it gives some basic information about what can be accomplished in the middle frame. For more information about online help, see Using Online Help, page 1-18.
  - **Reports or Lists**—Displays lists or reports, including accounting reports. For example, in User Setup you can show all usernames that start with a specific letter. The list of usernames beginning with a specified letter appears in this section. The usernames are hyperlinks to the specific user configuration, so you click the name to edit that user.
  - **System Messages**—Displays messages after you click Submit if you have typed in incorrect or incomplete data. For example, if the information that you entered in the Password box does not match the information in the Confirm Password box in the User Setup section, ACS displays an error message here. The incorrect information remains in the configuration area so that you can retype the information correctly and resubmit it.

Uniform Resource Locator for the Web Interface

You can access the ACS web interface by using one of the following uniform resource locators (URLs):

- http://*IP address*:2002
- http://*hostname*:2002

where *IP address* is the dotted decimal IP address and *hostname* is the hostname of the server that is running ACS. If you use the hostname, DNS must be functioning properly on your network or the hostname must be listed in the local hosts file of the computer that is running the browser.

If ACS is configured to use SSL to protect administrative sessions, you must specify the HTTPS protocol in the URLs:

- https://*IP address*:2002
- https://*hostname*:2002

If SSL is enabled and you do not specify HTTPS, ACS redirects the initial request to HTTPS for you. Using SSL to access the login page protects administrator credentials. For more information about enabling SSL to protect administrative sessions, see Access Policy, page 12-8.

From the computer that is running ACS, you can also use the following URLs:

- http://127.0.0.1:2002
- http://localhost:2002

If SSL is enabled, you can specify the HTTP protocol in the URLs:

- https://127.0.0.1:2002
- https://localhost:2002

Online Help and Online Documentation

We provide two sources of information in the web interface:

- **Online Help**—Contains basic information about the page shown in the configuration area.
- **Online Documentation**—Contains the entire user guide.

Using Online Help

Online help is the default content in the display area. For every page that appears in the configuration area, there is a corresponding online help page. Each online help page contains a list of topics covered on that page.

The two help icons that appear on pages in ACS are:

- **Question Mark**—Many subsections of the pages in the configuration area contain an icon with a question mark (?). To jump to the applicable topic in an online help page, click the question mark (?) icon.
- **Back to Help**—Wherever you find a online help page with a Section Information icon, the corresponding page in the configuration area contains a Back to Help icon. If you have accessed the online documentation by clicking a Section Information icon and want to view the online help page again, click the Back to Help icon.

Using the Online User Guide

The user guide provides information about the configuration, operation, and concepts of ACS. The information in the online documentation is as current as the release date of the ACS version that you are using. For the latest documentation about ACS, click http://www.cisco.com.

To access online documentation:

Step 1 In the ACS web interface, click **Online Documentation**.

Step 2 If you want to select a topic from the table of contents, scroll through the table of contents and click the applicable topic.

The online documentation for the topic selected appears in the display area.

Step 3 If you want to select a topic from the index, click **Index** and scroll through the index to find an entry for the topic that you want.

Tip Use the lettered shortcut links to jump to a particular section of the index.

Step 4 If you want to search for a specific string or topic in the online documentation, click **Search**, and then enter the string that you want.

Step 5 If you want to access the entire user guide in PDF format, click, **View PDF**.

ACS Specifications

Note For the hardware, operating system, third-party software, and network requirements, see the *Installation Guide for Cisco Secure ACS for Windows* at: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/install/index.htm.

This section contains the following topics:

- System Performance Specifications, page 1-19
- ACS Windows Services, page 1-20

System Performance Specifications

The performance capabilities of ACS are depend mostly on the Windows server it is installed on, your network topology and network management, the selection of user databases, and other factors. For example, ACS can perform many more authentications per second if it is using its internal user database and running on a computer that is using the fastest processor and network interface card available than if it is using external user databases and running on a computer that complies with the minimum system requirements. (See *Installation Guide for Cisco Secure ACS for Windows*.)

The following items are general answers to common system-performance questions. The performance of ACS in your network depends on your specific environment and AAA requirements.

- **Maximum users supported by the ACS internal database**—There is no theoretical limit to the number of users the ACS internal database can support. We have successfully tested ACS with databases in excess of 100,000 users. The practical limit for a single ACS authenticating against all its databases, internal and external, is 300,000 to 500,000 users. This number increases significantly if the authentication load is spread across a number of replicated ACS instances.
- **Transactions per second**—Authentication and authorization transactions per second depend on many factors, most of which are external to ACS. For example, high network latency in communication with an external user database lowers the number of transactions per second that ACS can achieve.
- **Maximum number of AAA clients supported**— ACS has been tested to support AAA services for approximately 50,000 AAA client configurations. This limitation is primarily a limitation of the ACS memory.

  If your network comprises tens of thousands of AAA clients, we recommend using multiple ACSs and assigning a manageable number of AAA clients to each ACS. For example, if you have 80,000 AAA clients, you could use four ACS servers and divide the AAA client load among them so that no single ACS manages more than 40,000 AAA client configurations. Then you can have overlapping AAA client support for backup AAA servers and not exceed the 50,000 AAA client limit. If you use replication to propagate configuration data among ACSs, limit replication of AAA client data to ACSs that serve the same set of AAA clients.

ACS Windows Services

ACS operates as a set of Microsoft Windows services. When you install ACS, the installation adds these Windows services to the server. These services provide the core of ACS functionality.

The ACS services on the computer running ACS include:

- **CSAdmin**—Provides the web interface for administration of ACS.
- **CSAuth**—Provides authentication services.
- **CSDBSync**—Provides synchronization of the ACS internal database with an external RDBMS application.
- **CSLog**—Provides logging services, for accounting and system activity.
- **CSMon**—Provides monitoring, recording, and notification of ACS performance, and behavior.
- **CSTacacs**—Provides communication between TACACS+ AAA clients and the CSAuth service.
- **CSRadius**—Provides communication between RADIUS AAA clients and the CSAuth service.

For a full description of each service, see Appendix G, “Internal Architecture”.

You can start and stop each module individually from within the Microsoft Windows Service Control Panel or as a group from within the ACS web interface. For information about stopping and starting ACS services, see Service Control, page 8-1. For information on service logs and gathering data for troubleshooting, see Service Logs, page 11-23.

Network administrators who offer increased levels of security services, and corporations that want to lessen the chance of intruder access resulting from password capturing, can use an OTP. ACS supports several types of OTP solutions, including PAP for Point-to-Point Protocol (PPP) remote-node login. Token cards are considered one of the strongest OTP authentication mechanisms.

Deployment Considerations

Deployment of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, can be complex and iterative, depending on the specific implementation required. This chapter describes the deployment process and presents the factors that you should consider before deploying ACS.

The complexity of deploying ACS reflects the evolution of AAA servers in general, and the advanced capabilities, flexibility, and features of ACS in particular. AAA was conceived originally to provide a centralized point of control for user access via dial-up services. As user databases grew and the locations of AAA clients became more dispersed, more capability was required of the AAA server. Regional, and then global, requirements became common. Today, ACS is required to provide AAA services for dial-up access, dial-out access, wireless, VLAN access, firewalls, VPN concentrators, administrative controls, and more. The list of external databases that are supported has also continued to grow and the use of multiple databases, as well as multiple ACSs, has become more common. Regardless of the scope of your ACS deployment, the information in this chapter should prove valuable. If you have deployment questions that are not addressed in this guide, contact your Cisco technical representative for assistance.

This chapter contains the following topics:

- Basic Deployment Factors for ACS, page 2-1
- Suggested Deployment Sequence, page 2-11

For more documentation on deployment for NAC support, see the Go NAC site on Cisco.com. For minimum ACS system and client requirements refer to your installation guide or the Release Notes at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm.

Basic Deployment Factors for ACS

Generally, the ease in deploying ACS is directly related to the complexity of the implementation that is planned, and the degree to which you have defined your policies and requirements. This section presents some basic factors that you should consider before you begin implementing ACS.

This section contains the following topics:

- Network Topology, page 2-2
- Remote Access Policy, page 2-7
- Security Policy, page 2-8
- Administrative Access Policy, page 2-8
- Database, page 2-10
- Network Latency and Reliability, page 2-10

Network Topology

How your enterprise network is configured is likely to be the most important factor in deploying ACS. While an exhaustive treatment of this topic is beyond the scope of this guide, this section details how the growth of network topology options has made ACS deployment decisions more complex.

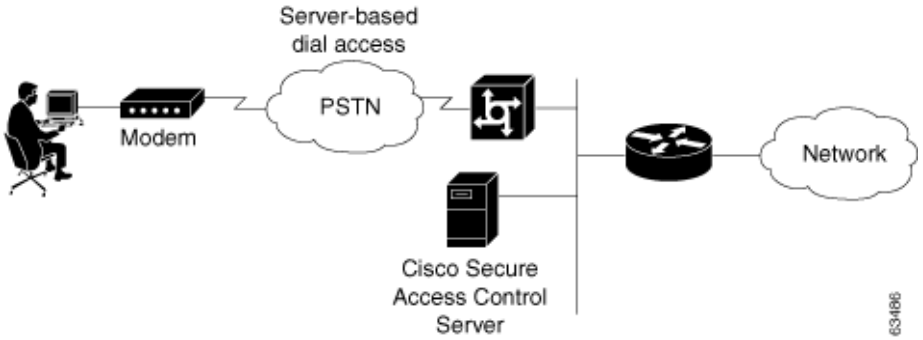
When AAA was created, network access was restricted to devices that were directly connected to the LAN or remote devices that gained access via a modem. Today, enterprise networks can be complex and, because of tunneling technologies, can be widely geographically dispersed.

Dial-Up Topology

In the traditional model of dial-up access (a PPP connection), a user employing a modem or ISDN connection is granted access to an intranet via a network access server (NAS) functioning as a AAA client. Users may be able to connect via only a single AAA client as in a small business, or have the option of numerous geographically dispersed AAA clients.

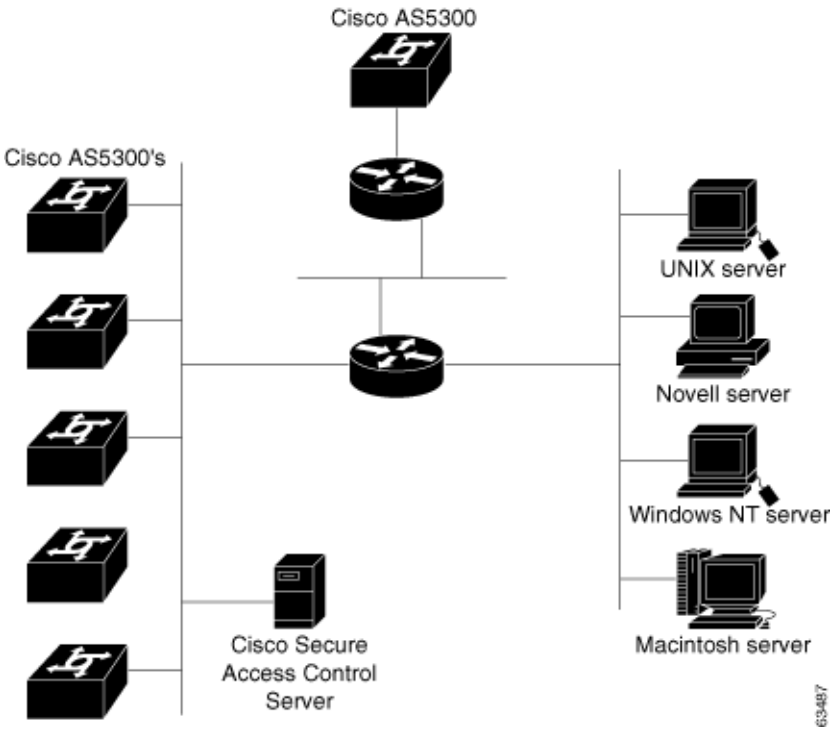
In the small LAN environment, see Figure 2-1, network architects typically place a single ACS internal to the AAA client, which is protected from outside access by a firewall and the AAA client. In this environment, the user database is usually small, few devices require access to the ACS for AAA, and any database replication is limited to a secondary ACS as a backup.

Figure 2-1 Small Dial-up Network



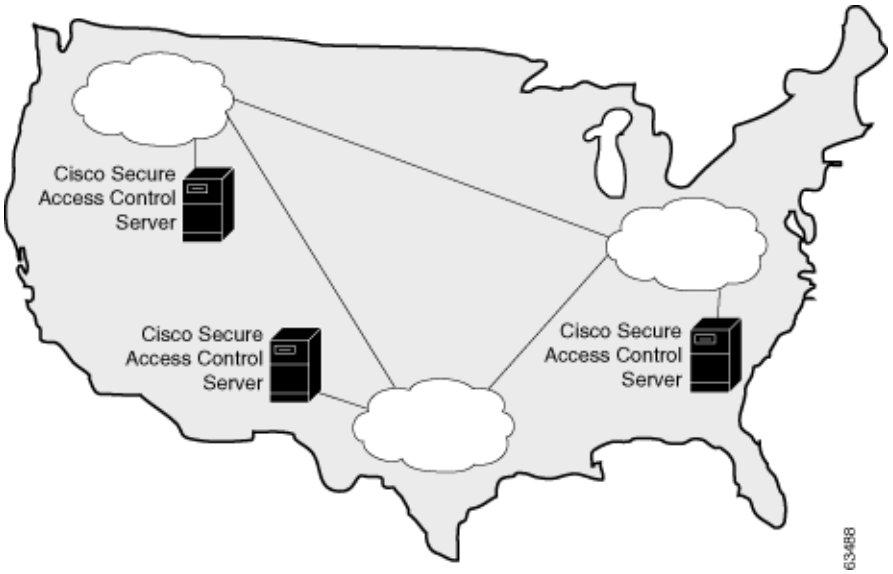
In a larger dial-in environment, a single ACS with a backup may be suitable, too. The suitability of this configuration depends on network and server access latency. Figure 2-2 shows an example of a large dial-in arrangement. In this scenario the addition of a backup ACS is a recommended addition.

Figure 2-2 Large Dial-up Network



In a very large, geographically dispersed network (Figure 2-3), access servers might be located in different parts of a city, in different cities, or on different continents. If network latency is not an issue, a central ACS may work; but connection reliability over long distances may cause problems. In this case, local ACSs may be preferable to a central ACS. If the need for a globally coherent user database is most important, database replication or synchronization from a central ACS may be necessary. Authentication by using external databases, such as a Windows user database or the Lightweight Directory Access Protocol (LDAP), can further complicate the deployment of distributed, localized ACSs. While ACS uses encryption for all replication and database-synchronization traffic, additional security measures may be required to protect the network and user information that ACS sends across the WAN.

Figure 2-3 Geographically Dispersed Network



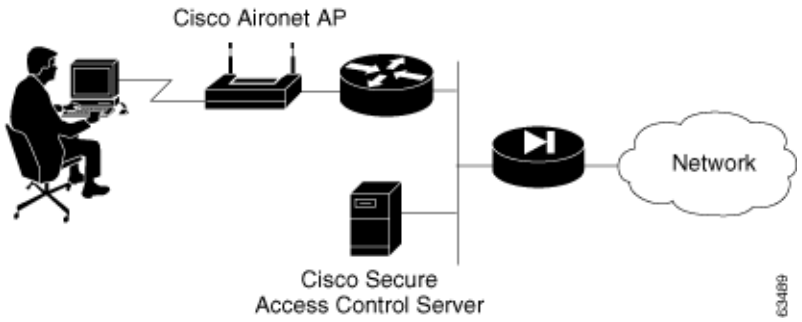
Wireless Network

The wireless network access point is a relatively new client for AAA services. The wireless access point (AP), such as the Cisco Aironet series, provides a bridged connection for mobile end-user clients into the LAN. Authentication is absolutely necessary due to the ease of access to the AP. Encryption is also necessary because of the ease of eavesdropping on communications. As such, security plays an even bigger role than in the dial-up scenario and is discussed in more detail later in this section.

Scaling can be a serious issue in the wireless network. The mobility factor of the wireless LAN (WLAN) requires considerations similar to those given to the dial-up network. Unlike the wired LAN, however, the WLAN can be more readily expanded. Though WLAN technology does have physical limits as to the number of users that can be connected via an AP, the number of APs can grow quickly. As with the dial-up network, you can structure your WLAN to allow full access for all users, or to provide restricted access to different subnets between sites, buildings, floors, or rooms. This raises a unique issue with the WLAN: the ability of a user to roam between APs.

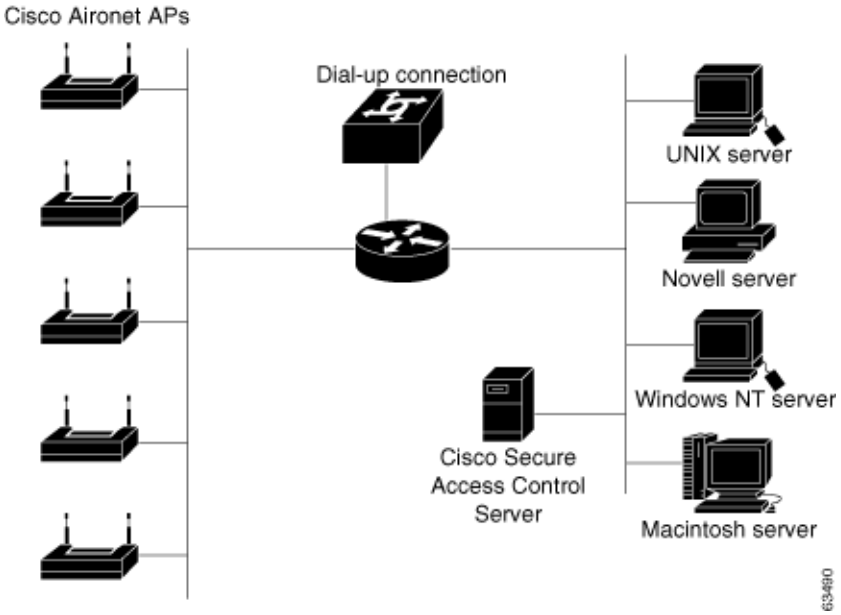
In the simple WLAN, there may be a single AP installed (Figure 2-4). Because there is only one AP, the primary issue is security. In this environment, there is generally a small user base and few network devices to worry about. Providing AAA services to the other devices on the network does not cause any significant additional load on the ACS.

Figure 2-4 Simple WLAN



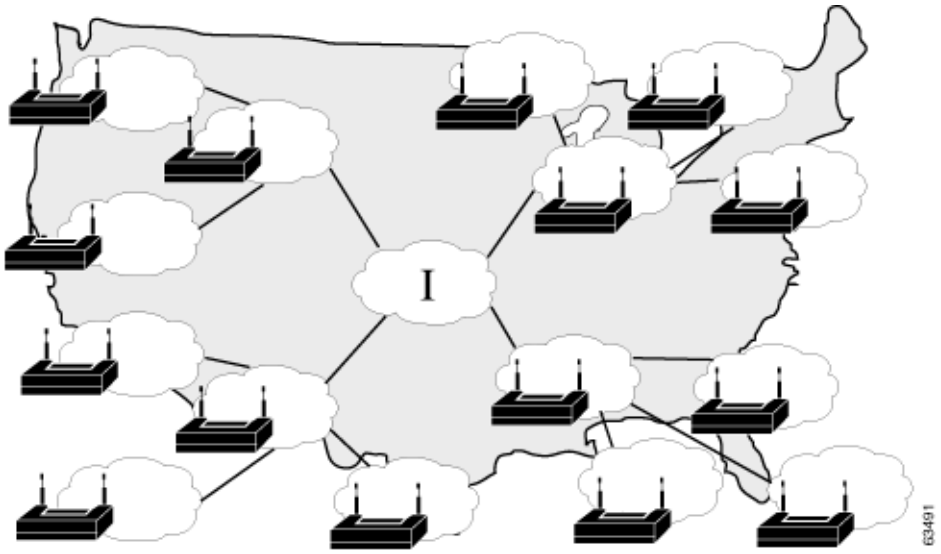
In the LAN where a number of APs are deployed, as in a large building or a campus environment, your decisions on how to deploy ACS become more complex. Figure 2-5 shows all APs on the same LAN; however, they may be distributed throughout the LAN, and connected via routers, switches, and so on. In the larger, geographical distribution of WLANs, deployment of ACS is similar to that of large regional distribution of dial-up LANs (Figure 2-3).

Figure 2-5 Campus WLAN



This is particularly true when the regional topology is the campus WLAN. This model starts to change when you deploy WLANs in many small sites that more resemble the simple WLAN shown in Figure 2-4. This model may apply to a chain of small stores that are distributed throughout a city or state, nationally, or globally (Figure 2-6).

Figure 2-6 Large Deployment of Small Sites



For the model in Figure 2-6, the location of ACS depends on whether all users need access on any AP, or require only regional or local network access. Along with database type, these factors control whether local or regional ACSs are required, and how database continuity is maintained. In this very large deployment model, security becomes a more complicated issue, too.

Remote Access using VPN

Virtual Private Networks (VPNs) use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets (Figure 2-7). The benefits of a VPN include the following:

- **Cost Savings**—By leveraging third-party networks with VPN, organizations no longer have to use expensive leased or frame relay lines, and can connect remote users to their corporate networks via a local Internet service provider (ISP); instead of using expensive toll-free or long-distance calls to resource-consuming modem banks.
- **Security**—VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.
- **Scalability**—VPNs allow corporations to use remote-access infrastructure within ISPs; therefore, corporations can add a large amount of capacity without adding significant infrastructure.
- **Compatibility with Broadband Technology**—VPNs allow mobile workers and telecommuters to take advantage of high-speed, broadband connectivity, such as DSL and cable, when gaining access to their corporate networks thereby, providing workers significant flexibility and efficiency.

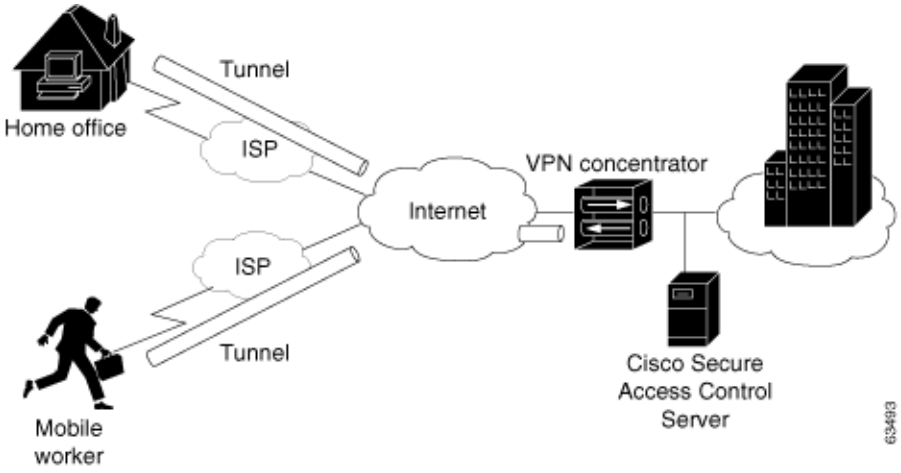
Figure 2-7 Simple VPN Configuration

The two types of VPN access into a network are:

- **Site-to-Site VPNs**—Extend the classic WAN by providing large-scale encryption between multiple fixed sites, such as remote offices and central offices, over a public network, such as the Internet.
- **Remote-Access VPNs**—Permit secure, encrypted connections between mobile or remote users and their corporate networks via a third-party network, such as an ISP, via VPN client software.

Generally speaking, site-to-site VPNs can be viewed as a typical WAN connection and are not usually configured to use AAA to secure the initial connection and are likely to use the device-oriented IPSec tunneling protocol. Remote-access VPNs, however, are similar to classic remote connection technology (modem/ISDN) and lend themselves to using the AAA model very effectively (Figure 2-8).

Figure 2-8 Enterprise VPN Solution



For more information about implementing VPN solutions, see the reference guide *A Primer for Implementing a Cisco Virtual Private Network*.

Remote Access Policy

Remote access is a broad concept. In general, it defines how the user can connect to the LAN, or from the LAN to outside resources (that is, the Internet). There are several ways connectivity is possible, dial-in, ISDN, wireless bridges, and secure Internet connections. Each method incurs its own advantages and disadvantages, and provides a unique challenge to providing AAA services. This closely ties remote

access policies to the enterprise network topology. In addition to the method of access, other decisions can also affect how ACS is deployed; these include specific network routing (access lists), time-of-day access, individual restrictions on AAA client access, access control lists (ACLs), and so on.

Remote access policies can be implemented for employees who telecommute, or mobile users who dial in over ISDN or a public switched telephone network (PSTN). Such policies are enforced at the corporate campus with ACS and the AAA client. Inside the enterprise network, remote access policies can control wireless access by individual employees.

ACS remote access policies provides control by using central authentication and authorization of remote users. The Cisco user database maintains all user IDs, passwords, and privileges. ACS access policies can be downloaded in the form of ACLs to network access servers such as the Cisco AS5300 Network Access Server, or by allowing access during specific periods, or on specific access servers.

Remote access policies are part of overall corporate security policy.

Security Policy

We recommend that every organization that maintains a network develop a security policy for the organization. The sophistication, nature, and scope of your security policy directly affect how you deploy ACS.

For more information about developing and maintaining a comprehensive security policy, refer to the following documents:

- Network Security Policy: Best Practices White Paper
- Cisco IOS Security Configuration Guide

Administrative Access Policy

Managing a network is a matter of scale. Providing a policy for administrative access to network devices depends directly on the size of the network and the number of administrators required to maintain the network. Local authentication on a network device can be performed, but it is not scalable. The use of network management tools can help in large networks; but if local authentication is used on each network device, the policy usually entails a single login on the network device. This does not promote adequate network device security. Using ACS allows a centralized administrator database, and administrators can be added or deleted at one location. TACACS+ is the recommended AAA protocol for controlling AAA client administrative access because of its ability to provide per-command control (command authorization) of AAA client administrator access to the device. RADIUS is not well suited for this purpose because of the one-time transfer of authorization information at the time of initial authentication.

The type of access is also an important consideration. In the case of different administrative access levels to the AAA clients, or if a subset of administrators is to be limited to certain systems, ACS can be used with command authorization per network device to restrict network administrators as necessary. Using local authentication restricts the administrative access policy to no login on a device or using privilege levels to control access. Controlling access by means of privilege levels is cumbersome and not very scalable. This requires that the privilege levels of specific commands are altered on the AAA client device and specific privilege levels are defined for the user login. You can easily create more problems by editing command privilege levels. Using command authorization on ACS does not require that you alter the privilege level of controlled commands. The AAA client sends the command to ACS to be parsed and ACS determines whether the administrator has permission to use the command. The use of AAA allows authentication on any AAA client to any user on ACS and limits access to these devices on a per-AAA-client basis.

A small network with a small number of network devices may require only one or two individuals to administer it. Local authentication on the device is usually sufficient. If you require more granular control than what authentication can provide, some means of authorization is necessary. As discussed earlier, controlling access by using privilege levels can be cumbersome. ACS reduces this problem.

In large enterprise networks, with many devices to administer, the use of ACS practically becomes a necessity. Because administration of many devices requires a larger number of network administrators, with varying levels of access, the use of local control is simply not a viable way of keeping track of network device configuration changes that are required when changing administrators or devices. The use of network management tools, such as CiscoWorks, helps to ease this burden; but maintaining security is still an issue. Because ACS can comfortably handle up to 300,000 users, the number of network administrators that ACS supports is rarely an issue. If a large remote-access population is using RADIUS for AAA support, the corporate IT team should consider separate TACACS+ authentication by using ACS for the administrative team. Separate TACACS+ authentication would isolate the general user population from the administrative team and reduce the likelihood of inadvertent access to network devices. If this is not a suitable solution, using TACACS+ for administrative (shell/exec) logins, and RADIUS for remote network access, provides sufficient security for the network devices.

Separation of Administrative and General Users

You should prevent the general network user from accessing network devices. Even though the general user may not intend to gain unauthorized access, inadvertent access could accidentally disrupt network access. AAA and ACS provide the means to separate the general user from the administrative user.

The easiest, and recommended, method to perform such separation is to use RADIUS for the general remote-access user and TACACS+ for the administrative user. One issue is that an administrator may also require remote network access, like the general user. If you use AC,S this issue poses no problem. The administrator can have RADIUS and TACACS+ configurations in ACS. Using authorization, RADIUS users can set PPP (or other network access protocols) as the permitted protocol. Under TACACS+, only the administrator would be configured to allow shell (exec) access.

For example, if the administrator is dialing in to the network as a general user, a AAA client would use RADIUS as the authenticating and authorizing protocol, and the PPP protocol would be authorized. In turn, if the same administrator remotely connects to a AAA client to make configuration changes, the AAA client would use the TACACS+ protocol for authentication and authorization. Because this administrator is configured on ACS with permission for shell under TACACS+, the administrator would be authorized to log in to that device. This does require that the AAA client have two separate configurations on ACS, one for RADIUS and one for TACACS+. An example of a AAA client configuration under IOS that effectively separates PPP and shell logins is:

```
aaa new-model
tacacs-server host ip-address
tacacs-server key secret-key
radius-server host ip-address
radius-server key secret-key
aaa authentication ppp default group radius
aaa authentication login default group tacacs+ local
aaa authentication login console none
aaa authorization network default group radius
aaa authorization exec default group tacacs+ none
aaa authorization command 15 default group tacacs+ none
username user password password
line con 0
login authentication console
```

Conversely, if a general user attempts to use his or her remote access to log in to a network device, ACS checks and approves the username and password; but the authorization process would fail because that user would not have credentials that allow shell or exec access to the device.

Database

Aside from topological considerations, the user database is one of the most influential factors in deployment decisions for ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of user database are all factors when deciding how ACS is deployed.

Number of Users

ACS is designed for the enterprise environment, and can handle 300,000 users. This capacity is usually more than adequate for a corporation. In an environment that exceeds these numbers, the user base would typically be geographically dispersed, which requires the use of more than one ACS configuration. A WAN failure could render a local network inaccessible because of the loss of the authentication server. In addition to this issue, reducing the number of users that a single ACS handles improves performance by lowering the number of logins occurring at any given time and reducing the load on the database.

Type of Database

ACS supports several database options, including the ACS internal database or using remote authentication with any of the external databases supported. For more information about database options, types, and features, see Table 1-2 specifies non-EAP authentication protocol support., page 1-7, Chapter 13, “User Databases,” or Chapter 17, “User Group Mapping and Specification.” Each database option has its own advantages and limitations in scalability and performance.

Network Latency and Reliability

Network latency and reliability are also important factors in how you deploy ACS. Delays in authentication can result in timeouts at the end-user client or the AAA client.

The general rule for large, extended networks, such as those in a globally dispersed corporation, is to have at least one ACS deployed in each region. This configuration may not be adequate without a reliable, high-speed connection between sites. Many corporations use secure VPN connections between sites so that the Internet provides the link. This option saves time and money; but it does not provide the speed and reliability of a dedicated frame relay or T1 link. If a reliable authentication service is critical to business functionality, such as retail outlets with cash registers that are linked by a WLAN, the loss of WAN connection to a remote ACS could be catastrophic.

The same issue can be applied to an external database used by ACS. The database should be deployed close enough to ACS to ensure reliable and timely access. Using a local ACS with a remote database can result in the same problems as using a remote ACS. Another possible problem in this scenario is that a user may experience timeout problems. The AAA client would be able to contact ACS, but ACS would wait for a reply that might be delayed or never arrive from the external user database. If the ACS were remote, the AAA client would time out and try an alternate method to authenticate the user; but in the latter case, it is likely the end-user client would time out first.

Suggested Deployment Sequence

While no single process for all ACS deployments is recommended, you should consider following the sequence, keyed to the high-level functions that are represented in the navigation toolbar. Also remember that many of these deployment activities are iterative in nature; you may find that you repeatedly return to such tasks as interface configuration as your deployment proceeds.

The recommended sequence of configuration tasks is:

- **Configure Administrators**—You should configure at least one administrator at the outset of deployment; otherwise, no remote administrative access is available, and all configuration activity must be done from the server. You should also have a detailed plan for establishing and maintaining an administrative policy.

  For more information about setting up administrators, see Chapter 1, "Overview." For more detailed information on administrative controls, see Chapter 12, "Administrators and Administrative Policy."

- **Configure the ACS Web Interface**—You can configure the ACS web interface to show only those features and controls that you intend to use. This option makes using ACS easier than it would be if you had to contend with multiple parts of the web interface that you do not plan to use. However, you should first ensure that you have correctly configured the features and controls that you require, in the Interface Configuration section. For guidance on configuring the web interface, see Interface Design Concepts, page 3-4.

  For information about configuring particular aspects of the web interface, see the following sections:

  - User Data Configuration Options, page 3-4
  - Advanced Options, page 3-5
  - Protocol Configuration Options for TACACS+, page 3-7
  - Protocol Configuration Options for RADIUS, page 3-9

- **Configure System**—The System Configuration section contains more than a dozen functions to be considered, from setting the format for the display of dates and password validation to configuring settings for database replication and RDBMS synchronization. These functions are detailed in Chapter 8, "System Configuration: Basic" and Chapter 9, "System Configuration: Advanced." Also note that during initial system configuration you must set up the logs and reports to be generated by ACS; for more information, see Chapter 1, "Overview."

- **Configure Network**—You control distributed and proxied AAA functions in the Network Configuration section of the web interface. From here, you establish the identity, location, and grouping of AAA clients and servers, and determine what authentication protocols each is to use. For more information, see Chapter 4, "Network Configuration."

- **Configure External User Database**—During this phase of deployment you must decide whether and how you intend to implement an external database to establish and maintain user authentication accounts. Typically, this decision is made according to your existing network administration mechanisms. For information about the types of databases ACS supports and instructions for establishing them, see Chapter 13, "User Databases."

  Along with the decision to implement an external user database (or databases), you should have detailed plans that specify your requirements for ACS database replication, backup, and synchronization. These aspects of configuring ACS internal database management are detailed in Chapter 8, "System Configuration: Basic."

- **Configure Shared Profile Components**—With most aspects of network configuration already established and before configuring user groups, you should configure your Shared Profile Components. When you set up and name the network access restrictions and command authorization

sets that you intend to employ, you lay out an efficient basis for specifying user group and single-user access privileges. For more information about Shared Profile Components, see Chapter 5, "Shared Profile Components."

- **Network Access Profiles**—Provides a way to set up network access classifications according to values that you set along with rules or policies for authentication, posture validation, and authorization. For information on network access profiles, see Chapter 15, "Network Access Profiles."
- **Configure Groups**—Having previously configured any external user databases that you intend to employ, and before configuring your user groups, you should decide how to implement two other ACS features that are related to external user databases: unknown user processing and database group mapping. For more information, see About Unknown User Authentication, page 16-3 and Chapter 17, "User Group Mapping and Specification." Then, you can configure your user groups with a complete plan of how ACS is to implement authorization and authentication. For more information, see Chapter 6, "User Group Management".
- **Configure Users**—With groups established, you can establish user accounts. Remember that a particular user can belong to only one user group, and that settings made at the user level override settings made at the group level. For more information, see Chapter 7, "User Management."
- **Configure Reports**—Using the Reports and Activities section of the ACS web interface, you can specify the nature and scope of logging that ACS performs. For a summary of the logging reports information, see Chapter 1, "Overview." For information on how to set up logging, see Chapter 11, "Logs and Reports."

CHAPTER 3

Using the Web Interface

Ease of use is the overriding design principle of the web interface in Cisco Secure Access Control Server Release 4.0 for Windows, henceforth referred to as ACS. ACS presents intricate concepts of network security from the perspective of an administrator. You can use the Interface Configuration section of ACS to configure the ACS web interface—you can tailor the interface to simplify the screens that you will use by hiding the features that you do not use and adding fields for your specific configuration.

Note We recommend that you return to this section to review and confirm your initial settings. While it is logical to begin your ACS configuration efforts with configuring the interface, sometimes a section of the web interface that you initially believed should be hidden from view may later require configuration from within this section.

Tip If a section of the ACS web interface appears to be missing or broken, return to the Interface Configuration section and confirm that the particular section has been activated.

This chapter contains the following topics:

- Administrative Sessions, page 3-1
- Interface Design Concepts, page 3-4
- User Data Configuration Options, page 3-4
- Advanced Options, page 3-5
- Protocol Configuration Options for TACACS+, page 3-7
- Protocol Configuration Options for RADIUS, page 3-9

Administrative Sessions

We recommend that administrative sessions take place without the use of an HTTP proxy server, without a firewall between the browser and ACS, and without a NAT gateway between the browser and ACS. Because these limitations are not always practical, this section discusses how various network environmental issues affect administrative sessions.

This section contains the following topics:

- Administrative Sessions and HTTP Proxy, page 3-2
- Administrative Sessions Through Firewalls, page 3-2
- Administrative Sessions Through a NAT Gateway, page 3-2

Administrative Sessions and HTTP Proxy

ACS does not support HTTP proxy for administrative sessions. If the browser used for an administrative session is configured to use a proxy server, ACS sees the administrative session originating from the IP address of the proxy server rather than from the actual address of the computer. Administrative session tracking assumes each browser resides on a computer with a unique IP.

Also, IP filtering of proxied administrative sessions has to be based on the IP address of the proxy server rather than the IP address of the computer. This conflicts with administrative session communication that does use the actual IP address of the computer. For more information about IP filtering of administrative sessions, see Access Policy, page 12-8.

For these reasons, we do not recommend performing administrative sessions using a web browser that is configured to use a proxy server. Administrative sessions using a proxy-enabled web browser is not tested. If your web browser is configured to use a proxy server, disable HTTP proxying when attempting ACS administrative sessions.

Administrative Sessions Through Firewalls

In the case of firewalls that do not perform network address translation (NAT), administrative sessions conducted across the firewall can require additional configuration of ACS and the firewall. This is because ACS assigns a random HTTP port at the beginning of an administrative session.

To allow administrative sessions from browsers outside a firewall that protects ACS, the firewall must permit HTTP traffic across the range of ports that ACS is configured to use. You can control the HTTP port range using the HTTP port allocation feature. For more information about the HTTP port allocation feature, see HTTP Port Allocation for Administrative Sessions, page 1-16.

While administering ACS through a firewall that is not performing NAT is possible, we do not recommend that you administer ACS through a firewall. For more information, see HTTP Port Allocation for Administrative Sessions, page 1-16.

Administrative Sessions Through a NAT Gateway

We do not recommend conducting administrative sessions across a network device performing NAT. If the administrator runs a browser on a computer behind a NAT gateway, ACS receives the HTTP requests from the public IP address of the NAT device, which conflicts with the computer private IP address, included in the content of the HTTP requests. ACS does not permit this.

If ACS is behind a NAT gateway and the URL used to access the web interface specifies ACS by its hostname, administrative sessions operate correctly, provided that DNS is functioning correctly on your network or that computers used to access the web interface have a hosts file entry for ACS.

If the URL used to access the web interface specifies ACS by its IP address, you could configure the gateway to forward all connections to port 2002 to ACS, using the same port. Additionally, all the ports allowed using the HTTP port allocation feature would have to be similarly mapped. We have not tested such a configuration and do not recommend implementing it.

Accessing the Web Interface

Remote administrative sessions always require that you log in using a valid administrator name and password, as configured in the Administration Control section. If the Allow automatic local login check box is cleared on the Sessions Policy Setup page in the Administration Control section, ACS requires a valid administrator name and password for administrative sessions accessed from a browser on the computer running ACS.

Before You Begin

Determine whether a supported web browser is installed on the computer you want to use to access the web interface. If not, install a supported web browser or use a computer that already has a supported web browser installed. For a list of supported browsers, see the Release Notes. The latest revision to the Release Notes is posted on Cisco.com (http://www.cisco.com).

Because the web interface uses Java in a few places, the computer running the browser used to access the web interface must have a Java Virtual Machine available for the use of the browser.

To access the web interface, follow these steps:

Step 1 Open a web browser. For a list of supported web browsers, see the Release Notes for the version of ACS you are accessing. The most recent revision to the Release Notes is posted on Cisco.com (http://www.cisco.com).

Step 2 In the Address or Location bar in the web browser, type the applicable URL. For a list of possible URLs, see Uniform Resource Locator for the Web Interface, page 1-18.

Step 3 If the ACS login page appears:

a. In the Username box, type a valid ACS administrator name.

b. In the Password box, type the password for the administrator name you specified.

c. Click **Login**.

The initial page appears, listing build and copyright information.

Logging Off the Web Interface

When you are finished using the web interface, we recommend that you log off. While ACS can timeout unused administrative sessions, logging off prevents unauthorized access by someone using the browser after you or by unauthorized persons using the HTTP port left open to support the administrative session.

To log off the ACS web interface, click the **X** in the upper-right corner of the screen.

Note The Logoff button appears in the upper-right corner of the browser window, except on the initial page, where it appears in the upper-left corner of the configuration area.

Interface Design Concepts

Before you begin to configure the ACS web interface for your particular configuration, you should understand a few basic precepts of the system operation. The information in the following sections is necessary for effective interface configuration.

Introduction of Network Access Profiles

Network-access profiles (NAPs) play a role with RADIUS provisioning and DACL assignment. You no longer only need to rely on user and group settings. With NAPs you can set up authorization rules that allow you to set user groups, RACs, and DACLs as part of a profile.

User-to-Group Relationship

A user can belong to only one group at a time. As long as there are no conflicting attributes, users inherit group settings.

Note If a user profile has an attribute configured differently from the same attribute in the group profile, the user setting always overrides the group setting.

If a user has a unique configuration requirement, you can make that user a part of a group and set unique requirements on the User Setup page; or you can assign that user to his or her own group.

User and group can be mapped to network-access profiles by using authorization rules. For more details on authorization rules, see Configuring Authorization Policies, page 15-43.

Per-User or Per-Group Features

You can configure most features at both the group and user levels, with the following exceptions:

- **User level only**—Static IP address, password, and expiration.
- **Group level only**—Password aging and time-of-day/day-of-week restrictions.

User Data Configuration Options

The Configure User Defined Fields page enables you to add (or edit) up to five fields for recording information on each user. The fields you define in this section subsequently appear in the Supplementary User Information section at the top of the User Setup page. For example, you could add the user's company name, telephone number, department, billing code, and so on. You can also include these fields in the accounting logs. For more information about the accounting logs, see About ACS Logs and Reports, page 11-4. For information on the data fields that compose the user data options, see User-Defined Attributes, page F-24.

Configuring New User Data Fields

To configure new user data fields:

Step 1 Click **Interface Configuration**, and then click **User Data Configuration**.

The Configure User Defined Fields page appears. Check boxes in the Display column indicate which fields are configured to appear in the Supplementary User Information section at the top of the User Setup page.

Step 2 Check a check box in the Display column.

Step 3 In the corresponding **Field Title** box, type a title for the new field.

Step 4 To configure another field, repeat Step 2 and Step 3.

Step 5 When you have finished configuring new user data fields, click **Submit**.

Advanced Options

You use the Advanced Options page to determine which advanced features ACS displays. You can simplify the pages that appear in other areas of the ACS web interface by hiding advanced features that you do not use.

Caution Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the web interface. Settings made while an advanced feature was visible remain in effect when that advanced feature is no longer visible. Further, the interface displays any advanced feature that has nondefault settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, ACS hides the advanced feature. The only exception is the Network Device Groups feature. Regardless of whether Network Device Groups are in use, they are hidden when you clear the appropriate check box on the Advanced Options page.

The advanced option features include:

- **Per-User TACACS+/RADIUS Attributes**—When selected, this feature enables TACACS+/RADIUS attributes to be set at a per-user level, in addition to being set at the group level. After this option is enabled, you must edit the TACACS+ (Cisco IOS) or any RADIUS page in the Interface Configuration section to specify which attributes you want to appear in user accounts. After you do this, user accounts display the selected attributes and enable them to be configured. Attributes configured at the user level override those defined at the group level.
- **User-Level Shared Network Access Restrictions**—When selected, this feature enables the Shared Profile Component network-access restrictions (NARs) options on the User Setup page. You use these options to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the user level. For information on defining a NAR, or NAR set, within Shared Profile Components, see Adding a Shared NAR, page 5-20.
- **User-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining user-level, IP-based and CLI/DNIS-based NARs, on the User Setup page.
- **User-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs (access-control lists) section on the User Setup page.

- **Default Time-of-Day/Day-of-Week Specification**—When selected, this feature enables the default time-of-day/day-of-week access settings grid on the Group Setup page.
- **Group-Level Shared Network Access Restrictions**—When selected, this feature enables the Shared Profile Component NAR options on the Group Setup page. You use these options to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the group level. For information on defining a NAR, or NAR set, within Shared Profile Components, see Adding a Shared NAR, page 5-20.
- **Group-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining group-level, IP-based and CLI/DNIS-based NARs on the Group Setup page.
- **Group-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs section on the Group Setup page.
- **Group-Level Password Aging**—When selected, this feature enables the Password Aging section on the Group Setup page. The Password Aging feature enables you to force users to change their passwords.
- **Network Access Filtering**—When selected, this feature enables the Network Access Filtering (NAF) section on the Shared Profiles Components pages. The Network Access Filtering option lets you set up groups of authentication, authorization, and accounting (AAA) client configurations (which may represent multiple network devices), network device groups (NDGs), or IP addresses of specific AAA client devices. You can use NAFs with downloadable IP ACLs and network-access restrictions to control access easily by device, which is important when creating your NAPs.
- **Max Sessions**—When selected, this feature enables the Max Sessions section on the User Setup and Group Setup pages. The Max Sessions option sets the maximum number of simultaneous connections for a group or a user.
- **Usage Quotas**—When selected, this feature enables the Usage Quotas sections on the User Setup and Group Setup pages. The Usage Quotas option sets one or more quotas for usage by a group or a user.
- **Distributed System Settings**—When selected, this feature displays the AAA server and proxy tables on the Network Interface page. If the tables have information other than the defaults in them, they always appear.
- **Remote Logging**—When selected, this feature enables the Remote Logging feature on the Logging page of the System Configuration section.
- **ACS Database Replication**—When selected, this feature enables the ACS database replication information on the System Configuration page.
- **RDBMS Synchronization**—When selected, this feature enables the Relational Database Management System (RDBMS) Synchronization option on the System Configuration page. If RDBMS Synchronization is configured, this option always appears.
- **IP Pools**—When selected, this feature enables the IP Pools Address Recovery and IP Pools Server options on the System Configuration page.
- **Network Device Groups**—When selected, this option enables network device groups (NDGs). When NDGs are enabled, the Network Configuration section and parts of the User Setup and Group Setup pages change to enable you to manage groups of network devices (AAA clients or AAA servers). This feature is useful if you have many devices to administer.
- **Voice-over-IP (VoIP) Group Settings**—When selected, this feature enables the VoIP option on the Group Setup page.

- **Voice-over-IP (VoIP) Accounting Configuration**—When selected, this feature enables the VoIP Accounting Configuration option on the System Configuration page. You use this option to determine the logging format of RADIUS VoIP accounting packets.
- **ODBC Logging**—When selected, this feature enables the ODBC logging sections on the Logging page of the System Configuration section.

Setting Advanced Options for the ACS User Interface

To set advanced options for the ACS web interface:

Step 1 Click **Interface Configuration**, and then click **Advanced Options**.

The Advanced Options table appears.

Step 2 Select each option that you want enabled in the ACS web interface.

Caution Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the web interface. Settings made while an advanced feature was visible remain in effect when that advanced feature is no longer visible. Furthermore, the interface displays any advanced feature that has nondefault settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, ACS hides the advanced feature. The only exception is the Network Device Groups feature. Regardless of whether Network Device Groups are in use, they are hidden when you clear the appropriate check box on the Advanced Options page.

Step 3 When you have finished making selections, click **Submit**.

ACS alters the contents of various sections of the web interface according to your selections.

Protocol Configuration Options for TACACS+

The TACACS+ (Cisco) page details the configuration of the ACS web interface for TACACS+ settings. You use the interface settings to display or hide TACACS+ administrative and accounting options. You can simplify the web interface by hiding the features that you do not use.

The TACACS+ (Cisco) page comprises three distinct areas:

Tip The default interface setting presents a single column of check boxes, at the group level only, for selecting TACACS+ Services Settings and New Service Settings. To view two columns of check boxes that you check to configure settings at the Group level or the User level, you must have enabled the Per-user TACACS+/RADIUS Attributes option on the Advanced Options page of Interface Configuration section.

- **TACACS+ Services Settings**—This area contains a list of the most commonly used services and protocols for TACACS+. You select each TACACS+ service that you want to appear as a configurable option on the User Setup page or Group Setup page.
- **New Services**—In this area you can enter any services or protocols that are particular to your network configuration.

Note If you have configured ACS to interact with device-management applications for other Cisco products, such as Management Center for Firewalls, ACS might display new TACACS+ services as dictated by these device-management applications. To ensure the proper functioning of ACS, of device-management applications with which ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

- **Advanced Configuration Options**—In this area you can add more detailed information for even more tailored configurations.

  The four items that you can choose to hide or display are:

  - **Advanced TACACS+ Features**—This option displays or hides the Advanced TACACS+ Options section on the User Setup page. These options include Privilege Level Authentication and Outbound Password Configuration for SENDPASS and SENDAUTH clients, such as routers.
  - **Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings**—If this option is checked, a grid appears on the User Setup page that you use to override the TACACS+ scheduling attributes on the Group Setup page.

    You can control the use of each TACACS+ service by the time of day and day of week. For example, you can restrict Exec (Telnet) access to business hours but permit PPP-IP access at any time.

    The default setting is to control time-of-day access for all services as part of authentication. However, you can override the default and display a time-of-day access grid for every service. This setting keeps user and group setup easy to manage, while making this feature available for the most sophisticated environments. This feature applies only to TACACS+ because TACACS+ can separate the authentication and authorization processes. RADIUS time-of-day access applies to all services. If TACACS+ and RADIUS are used simultaneously, the default time-of-day access applies to both. The default provides a common method by which to control access regardless of the access-control protocol.
  - **Display a window for each service selected in which you can enter customized TACACS+ attributes**—If you check this option, an area appears on the User Setup and Group Setup pages in which you enter custom TACACS+ attributes.

    ACS can also display a custom command field for each service. You use this text field to make specialized configurations to be downloaded for a particular service for users in a particular group.

    You can use this feature to send many TACACS+ commands to the access device for the service, provided that the device supports the command, and that the command syntax is correct. This feature is disabled by default, but you can enable it the same way you enable attributes and time-of-day access.
  - **Display enable Default (Undefined) Service Configuration**—If this check box is selected, an area appears on the User Setup and Group Setup pages in which you permit unknown TACACS+ services, such as Cisco Discovery Protocol (CDP).

    Note Only advanced system administrators should use this option.

Note Customized settings at the user level take precedence over settings at the group level.

Setting Options for TACACS+

Note The ACS web interface displays any protocol option that is enabled or has nondefault values, even if you have configured that protocol option to be hidden. If you later disable the option or delete its value and the protocol option is configured to be hidden, ACS hides the protocol option. This behavior prevents ACS from hiding active settings.

You use this procedure to display or hide TACACS+ administrative and accounting options. It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, you can use the TACACS+ (Cisco IOS) Edit page to customize the services and protocols that appear.

To configure the user interface for TACACS+ options:

Step 1 Click **Interface Configuration**, and then click **TACACS+ (Cisco IOS)**.

The TACACS+ (Cisco) page appears.

Step 2 In the **TACACS+ Services** table, check the check box for each TACACS+ service that you want to be visible on the applicable setup page.

Step 3 To add new services and protocols:

a. In the New Services section of the TACACS+ Services table, type in any Service and Protocol to be added.

Note If you have configured ACS to interact with device-management applications for other Cisco products, such as a Management Center for Firewalls, ACS may display new TACACS+ services as dictated by these device-management applications. To ensure the proper functioning of ACS, of device-management applications with which ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

b. Check the appropriate check box to select those that should be visible for configuration under User Setup, or Group Setup, or both.

Step 4 In the Advanced Configurations Options section, check the check boxes of the display options that you want to enable.

Step 5 When you have finished setting TACACS+ interface display options, click **Submit**.

The selections made in this procedure determine what TACACS+ options ACS displays in other sections of the web interface.

Protocol Configuration Options for RADIUS

It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group cumbersome. To simplify setup, use the options in this section to customize the attributes that are visible. For a list of supported RADIUS AV pairs and accounting AV pairs, see Appendix C, “RADIUS Attributes.”

Depending on which AAA client or clients you have configured, the Interface Configuration page displays different choices of RADIUS protocol configuration settings. The Interface Configuration page displays RADIUS Internet Engineering Task Force (IETF) settings whenever any RADIUS AAA client is configured. The Interface Configuration page also displays additional settings for each vendor-specific RADIUS type. The settings that appear for various types of AAA client depend on what settings that type of device can employ. These combinations are detailed in Table 3-1.

Table 3-1 RADIUS Listings in Interface

Configure this Type of AAA Client	The Interface Configuration Page Lists the Types of Settings Shown										
	RADIUS (IETF)	RADIUS (Cisco Airespace)	RADIUS (Cisco Aironet)	RADIUS (BBSM)	RADIUS (Cisco IOS/PIX 6.0)	RADIUS (Microsoft)	RADIUS (Ascend)	RADIUS (Cisco VPN 3000/ ASA/ PIX 7.x+)	RADIUS (Cisco VPN 5000)	RADIUS (Juniper)	RADIUS (Nortel)
RADIUS (IETF)/ RADIUS (iPass)	Yes	No	No	No	No	No	No	No	No	No	No
RADIUS (Cisco Airespace)	Yes	Yes	No	No	No	No	No	No	No	No	No
RADIUS (Cisco Aironet)	Yes	No	Yes	No	Yes	No	No	No	No	No	No
RADIUS (BBSM)	Yes	No	No	Yes	No	No	No	No	No	No	No
RADIUS (Cisco IOS/ PIX 6.0)	Yes	No	No	No	Yes	Yes	Yes	No	No	No	No
RADIUS (Ascend)	Yes	No	No	No	No	Yes	Yes	No	No	No	No
RADIUS (Cisco VPN3000/ASA/ PIX 7.x+)	Yes	No	No	No	Yes	Yes	No	Yes	No	No	No
RADIUS (Cisco VPN 5000)	Yes	No	No	No	No	No	No	No	Yes	No	No
RADIUS (Juniper)	Yes	No	No	No	No	No	No	No	No	Yes	No
RADIUS (Nortel)	Yes	No	No	No	No	No	No	No	No	No	Yes

Tip You must configure your network devices before you can select, on the Interface Configuration page, a type of setting for further configuration.

From the Interface Configuration page, when you select a type of RADIUS setting to configure, the web interface displays the corresponding list of available RADIUS attributes and associated check boxes. If you have selected the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options, a User check box appears alongside the Group check box for each attribute. Otherwise, only the Group check box for each attribute appears. By checking check boxes in a list of attributes, you determine whether the corresponding (IETF) RADIUS attribute or vendor-specific attribute (VSA) is configurable from the User Setup and Group Setup sections.

Details regarding the types of RADIUS settings pages:

- **(IETF) RADIUS Settings**—This page lists attributes available for (IETF) RADIUS.

  These standard (IETF) RADIUS attributes are available for any network device configuration when using RADIUS. If you want to use IETF attribute number 26 (for VSAs), select Interface Configuration and then RADIUS for the vendors whose network devices you use. Attributes for (IETF) RADIUS and the VSA for each RADIUS network device vendor supported by ACS appear in User Setup or Group Setup.

  Note The RADIUS (IETF) attributes are shared with RADIUS VSAs. You must configure the first RADIUS attributes from RADIUS (IETF) for the RADIUS vendor.

  The Tags to Display Per Attribute option (located under Advanced Configuration Options) enables you to specify how many values to display for tagged attributes on the User Setup and Group Setup pages. Examples of tagged attributes include [064]Tunnel-Type and [069]Tunnel-Password.

  For detailed steps, see Setting Protocol Configuration Options for IETF RADIUS Attributes, page 3-12.

- **RADIUS (Cisco IOS/PIX 6.0) Settings**—You use this section to enable the specific attributes for RADIUS (Cisco IOS/PIX 6.0). Selecting the first attribute listed under RADIUS (Cisco IOS/PIX 6.0), 026/009/001, displays an entry field under User Setup and/or Group Setup in which any TACACS+ commands can be entered to fully leverage TACACS+ in a RADIUS environment. For detailed steps, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.

- RADIUS (Cisco Aironet) Settings—This section is now obsolete. You can now use the session-timeout in a dedicated WLAN RADIUS Authorization Component (RAC).

Tip We recommend that you do not use the RADIUS Cisco Aironet settings to enable a specific attribute for RADIUS (Cisco Aironet) unless it is an existing configuration.

When ACS responds to an authentication request from a Cisco Aironet Access Point and the Cisco-Aironet-Session-Timeout attribute is configured in the RAC, ACS sends to the wireless device this value in the IETF Session-Timeout attribute. This setting enables you to provide different session-timeout values for wireless and wired end-user clients. For steps on adding a WLAN RAC session-timeout, see Adding RADIUS Authorization Components, page 5-9.

- **RADIUS (Cisco Airespace) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco Airespace). This page appears if you have configured a RADIUS (Cisco Airespace) device. For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.

- **RADIUS (Ascend) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Ascend). This page appears if you have configured a RADIUS (Ascend) or a RADIUS (Cisco IOS/PIX 6.0) device. For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.
- **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 3000/ASA/PIX 7.x+). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.
- **RADIUS (Cisco VPN 5000) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 5000). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.
- **RADIUS (Microsoft) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Microsoft). This page appears if you configure a RADIUS (Ascend), or a RADIUS (VPN 3000/ASA/PIX 7.x+), or a RADIUS (Cisco IOS/PIX 6.0) device. For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.
- **RADIUS (Nortel) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Nortel). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.
- **RADIUS (Juniper) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Juniper). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.
- **RADIUS (BBSM) Settings**—From this section you enable the RADIUS VSAs for RADIUS Building Broadband Service Manager (BBSM). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13.

While ACS ships with these prepackaged VSAs, you can also define and configure custom attributes for any VSA set that is not already contained in ACS. If you have configured a custom VSA and a corresponding AAA client, from the Interface Configuration section you can select the custom VSA and then set the options for how particular attributes appear as configurable options on the User Setup or Group Setup page. For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-19.

Setting Protocol Configuration Options for IETF RADIUS Attributes

This procedure enables you to hide or display any of the standard IETF RADIUS attributes for configuration from other portions of the ACS web interface.

Note If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is selected, a User check box appears alongside the Group check box for each attribute.

Note Your RADIUS network devices must support each checked RADIUS attribute.

To set protocol configuration options for IETF RADIUS attributes:

Step 1 Click **Interface Configuration**, and then click **RADIUS (IETF)**.

The RADIUS (IETF) page appears.

Step 2 For each IETF RADIUS attribute that you want to appear as a configurable option on the User Setup or Group Setup page, check the corresponding check box.

Note Your RADIUS network devices must support each checked RADIUS attribute.

Step 3 To specify how many values to display for tagged attributes on the User Setup and Group Setup pages, select the **Tags to Display Per Attribute** option, and then select a value from the corresponding list. Examples of tagged attributes are `[064] Tunnel-Type` and `[069] Tunnel-Password`.

Step 4 When you have finished selecting the attributes, click **Submit**.

Each IETF RADIUS attribute that you checked appears as a configurable option on the User Setup or Group Setup page, as applicable.

Setting Protocol Configuration Options for Non-IETF RADIUS Attributes

You use this procedure to hide or display various RADIUS VSAs for configuration from the User Setup and Group Setup portions of the ACS web interface.

To set protocol configuration options for a set of RADIUS VSAs:

Step 1 Click **Interface Configuration**.

Step 2 Click one of the RADIUS VSA set types, for example, `RADIUS (Ascend)`.

Step 3 The page listing the selected set of available RADIUS VSAs appears.

Note If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is checked, a User check box appears beside the Group check box for each attribute.

Step 4 For each RADIUS VSA that you want to appear as a configurable option on the User Setup or Group Setup page, check the corresponding check box.

Note Each checked attribute must be supported by your RADIUS network devices.

Step 5 Click **Submit** at the bottom of the page.

According to your selections, the RADIUS VSAs appear on the User Setup or Group Setup pages, or both, as a configurable option.

Network Configuration

This chapter details concepts and procedures for configuring Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS. You use the configuration process to establish a distributedd system and set up interaction with authentication, authorization, and accounting (AAA) clients and servers.

This chapter contains the following topics:

- About Network Configuration, page 4-1
- About Distributed Systems, page 4-2
- Proxy in Distributed Systems, page 4-3
- Network Device Searches, page 4-6
- AAA Client Configuration, page 4-7
- AAA Server Configuration, page 4-15
- Network Device Group Configuration, page 4-19
- Proxy Distribution Table Configuration, page 4-23

About Network Configuration

The appearance of the page that you see when you click Network Configuration differs according to the network-configuration selections that you made in the Interface Configuration section.

The four tables that might appear in this section are:

- **AAA Clients**—This table lists each AAA client that is configured on the network, together with its IP address and associated protocol.

  If you are using Network Device Groups (NDGs), this table does not appear on the initial page, but is accessed through the Network Device Group table. For more information about this interface configuration, see Advanced Options, page 3-5.

- **AAA Servers**—This table lists each AAA server that is configured on the network together with its IP address and associated type.

  If you are using NDGs, this table does not appear on the initial page, but is accessed through the Network Device Groups table. For more information about this interface configuration, see Advanced Options, page 3-5.

- **Network Device Groups**—This table lists the name of each NDG that has been configured, and the number of AAA clients and AAA servers that are assigned to each NDG. If you are using NDGs, the AAA Clients table and AAA Servers table do not appear on the opening page. To configure AAA clients or AAA servers, you must click the name of the NDG to which the device is assigned. If the newly configured device is not assigned to an NDG, it belongs to the (Not Assigned) group.

  This table appears only when you have configured the interface to use NDGs. For more information about this interface configuration, see Advanced Options, page 3-5.

- **Proxy Distribution Table**—You can use the Proxy Distribution Table to configure proxy capabilities including domain stripping. For more information, see Proxy Distribution Table Configuration, page 4-23.

  This table appears only when you have configured the interface to enable Distributed Systems Settings. For more information about this interface configuration, see Advanced Options, page 3-5.

About Distributed Systems

ACS can be used in a distributed system; that is, multiple ACSs and AAA servers can be configured to communicate with one another as primary, backup, client, or peer systems. You can, therefore, use powerful features such as:

- Proxy
- Fallback on failed connection
- ACS internal database replication
- Remote and centralized logging

AAA Servers in Distributed Systems

AAA server is the generic term for an access-control server (ACS), and the two terms are often used interchangeably. You can configure AAA servers to determine who can access the network and what services are authorized for each user. The AAA server stores a profile containing authentication and authorization information for each user. Authentication information validates user identity, and authorization information determines what network services a user can to use. A single AAA server can provide concurrent AAA services to many dial-up access servers, routers, and firewalls. Each network device can be configured to communicate with a AAA server. You can, therefore, centrally control dial-up access, and secure network devices from unauthorized access.

These types of access control have unique authentication and authorization requirements. With ACS, system administrators can use a variety of authentication methods that are used with different degrees of authorization privileges.

Completing the AAA functionality, ACS serves as a central repository for accounting information. Each user session that ACS grants can be fully accounted for, and its accounting information can be stored in the server. You can use this accounting information for billing, capacity planning, and security audits.

Note If the fields mentioned in this section do not appear in the ACS web interface, you can enable them by choosing **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

Default Distributed System Settings

You use the AAA Servers table and the Proxy Distribution Table to establish distributed system settings. The parameters that are configured within these tables create the foundation so that you can configure multiple ACSs to work with one another. Each table contains an ACS entry for itself. In the AAA Servers table, the only AAA server that is initially listed is itself; the Proxy Distribution Table lists an initial entry of `(Default)`, which displays how the local ACS is configured to handle each authentication request locally.

You can configure additional AAA servers in the AAA Servers table. These devices can, therefore, become visible in the web interface so that they can be configured for other distributed features such as proxy, ACS internal database replication, remote logging, and RDBMS synchronization. For information about configuring additional AAA servers, see Adding AAA Servers, page 4-16.

Proxy in Distributed Systems

Proxy is a powerful feature that enables you to use ACS for authentication in a network that uses more than one AAA server. Using proxy, ACS automatically forwards an authentication requests from AAA clients to AAA servers. After the request has been successfully authenticated, the authorization privileges that you configured for the user on the remote AAA server are passed back to the original ACS, where the AAA client applies the user profile information for that session.

Proxy provides a useful service to users, such as business travelers, who dial in to a network device other than the one they normally use and would otherwise be authenticated by a foreign AAA server. To configure proxy, you choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

Whether, and where, an authentication request is to be forwarded is defined in the Proxy Distribution Table on the Network Configuration page. You can use multiple ACSs throughout your network. For information about configuring the Proxy Distribution Table, see Proxy Distribution Table Configuration, page 4-23.

ACS employs character strings that the administrator defines to determine whether an authentication request should be processed locally or forwarded, and where. When an end user dials in to the network device and ACS finds a match for the character string defined in the Proxy Distribution Table, ACS forwards the authentication request to the associated remote AAA server.

Note When an ACS receives a TACACS+ authentication request forwarded by proxy, any requests for Network Access Restrictions for TACACS+ are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

Note When an ACS proxies to a second ACS, the second ACS responds to the first by using only IETF attributes, no VSAs, when it recognizes the first ACS as the AAA server. Alternatively, you can configure the second ACS to see an ACS as a AAA client; in this case, the second ACS responses include the RADIUS VSAs for whatever RADIUS vendor is specified in the AAA client definition table entry—in the same manner as any other AAA client.

For example, an ACS receives an authentication request for *mary.smith@corporate.com*, where *@corporate.com* is a character string that you define in the server distribution table as being associated with another specific AAA server. The ACS receiving the authentication request for *mary.smith@corporate.com* then forwards the request to the AAA server with which that character string is associated. The entry in the Proxy Distribution Table defines the association.

Administrators with geographically dispersed networks can configure and manage the user profiles of employees within their immediate location or building. The administrator can, therefore, manage the policies of just their users and all authentication requests from other users within the company can be forwarded to their respective AAA server for authentication. Not every user profile must reside on every AAA server. Proxies save administration time and server space, and allows end users to receive the same privileges regardless of the access device through which they connect.

Fallback on Failed Connection

You can configure the order in which ACS checks remote AAA servers if a failure of the network connection to the primary AAA server occurs. If an authentication request cannot be sent to the first listed server, because of a network failure for example, the next listed server is checked. This checking continues, in order, down the list, until the AAA servers handles the authentication request. (Failed connections are detected by failure of the nominated server to respond within a specified time period. That is, the request is timed out.) If ACS cannot connect to any server in the list, authentication fails.

Character String

ACS forwards authentication requests by using a configurable set of characters with a delimiter, such as periods (.), slashes (/), or hyphens (-). When configuring the ACS character string, you must specify whether the character string is the prefix or suffix. For example, you can use *domain.us* as a suffix character string in *username*domain.us*, where the asterisk (*) represents any delimiter. An example of a prefix character string is *domain.*username*, where the asterisk (*) would be used to detect the slash(/).

Stripping

Stripping allows ACS to remove, or strip, the matched character string from the username. When you enable stripping, ACS examines each authentication request for matching information. When ACS finds a match by character string in the Proxy Distribution Table, as described in the example under Proxy in Distributed Systems, page 4-3, ACS strips off the character string if you have configured it to do so. For example, in the following proxy example, the character string that accompanies the username establishes the ability to forward the request to another AAA server. If the user must enter the user ID of *mary@corporate.com* to be forwarded correctly to the AAA server for authentication, ACS might find a match on the *@corporate.com* character string, and strip the *@corporate.com*, leaving a username of *mary*, which might be the username format that the destination AAA server requires to identify the correct entry in its database.

Note Realm stripping does not work with Extensible Authentication Protocol (EAP)-based authentication protocols, such as Protected Extensible Authentication Protocol (PEAP) or Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). For example, if you are using Protected Extensible Authentication Protocol Microsoft Challenge Authentication Handshake Protocol (PEAP MSCHAP), authentication will fail if a realm is stripped by proxy.

Proxy in an Enterprise

This section presents a scenario of proxy that is used in an enterprise system. Mary is an employee with an office in the corporate headquarters in Los Angeles. Her username is *mary@la.corporate.com*. When Mary needs access to the network, she accesses the network locally and authenticates her username and password. Because Mary works in the Los Angeles office, her user profile, which defines her authentication and authorization privileges, resides on the local Los Angeles AAA server.

However, Mary occasionally travels to a division within the corporation in New York, where she still needs to access the corporate network to get her e-mail and other files. When Mary is in New York, she dials in to the New York office and logs in as *mary@la.corporate.com*. The New York ACS does not recognize her username, but the Proxy Distribution Table contains an entry, *@la.corporate.com,* to forward the authentication request to the Los Angeles ACS. Because the username and password information for Mary reside on that AAA server, when she authenticates correctly, the AAA client in the New York office applies the authorization parameters that are assigned to her.

Remote Use of Accounting Packets

When proxy is employed, ACS can dispatch AAA accounting packets in one of three ways:

- Log them locally.
- Forward them to the destination AAA server.
- Log them locally and forward copies to the destination AAA server.

Sending accounting packets to the remote ACS offers several benefits. When ACS is configured to send accounting packets to the remote AAA server, the remote AAA server logs an entry in the accounting report for that session on the destination server. ACS also caches the user connection information and adds an entry in the List Logged on Users report. You can then view the information for users that are currently connected. Because the accounting information is sent to the remote AAA server, even if the connection fails, you can view the Failed Attempts report to troubleshoot the failed connection.

Sending the accounting information to the remote AAA server also enables you to use the Max Sessions feature. The Max Sessions feature uses the Start and Stop records in the accounting packet. If the remote AAA server is an ACS and the Max Sessions feature is implemented, you can track the number of sessions that are allowed for each user or group.

You can also choose to have Voice-over-IP (VoIP) accounting information logged remotely, appended to the RADIUS Accounting log, entered in a separate VoIP Accounting log, or both.

Other Features Enabled by System Distribution

Beyond basic proxy and fallback features, configuring an ACS to interact with distributed systems enables several other features that are beyond the scope of this chapter. These features include:

- **Replication**—For more information, see ACS Internal Database Replication, page 9-1.
- **RDBMS synchronization**—For more information, see RDBMS Synchronization, page 9-17.
- **Remote and centralized logging**—For more information, see Remote Logging, page 11-19.

Network Device Searches

You can search for any network device that is configured in the Network Configuration section of the ACS web interface.

This section contains the following topics:

- Network Device Search Criteria, page 4-6
- Searching for Network Devices, page 4-6

Network Device Search Criteria

You can specify search criteria for network device searches. ACS provides the following search criteria:

- **Name**—The name assigned to the network device in ACS. You can use an asterisk (*) as a wildcard character. For example, if you wanted to find all devices with names starting with the letter M, you would enter *M** or *m**. Name-based searches are case insensitive. If you do not want to search based on device name, you can leave the Name box blank or you can put only an asterisk (*) in the Name box.
- **IP Address**—The IP address specified for the network device in ACS. For each octet in the address, you have three options:
  - **Number**—You can specify a number, for example, 10.3.157.98.
  - **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen (-), for example, 10.3.157.10-50.
  - **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

  ACS allows any octet or octets in the IP Address box to be a number, a numeric range, or an asterisk (*), for example 172.16-31.*.*.
- **Type**—The device type, as specified by the AAA protocol that it is configured to use, or the kind of AAA server it is. If you do not want to limit the search based on device type, choose **Any** from the Type list.
- **Device Group**—The NDG to which the device is assigned. This search criterion only appears if you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration section. If you do not want to limit the search based on NDG membership, select **Any** from the Device Group list.

Searching for Network Devices

To search for a network device:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Click **Search**.

The Search for Network Devices page appears. In the configuration area, the controls for setting search criteria appear above the search results for the most recent search that was previously conducted for this session, if any.

Tip When you leave the Search for Network Devices page, ACS retains your search criteria and results for the duration of the current administrative session. Until you log out of ACS, you can return to the Search for Network Devices page to view your most recent search criteria and results.

Step 3 Set the criteria for a device search. For information about search criteria, see Network Device Search Criteria, page 4-6.

Tip To reset the search criteria to default settings, click **Clear**.

Step 4 Click **Search**.

A table lists each network device configured in ACS that matches the search criteria you specified. If ACS did not find a matching network device, the message `No Search Results` appears.

The table listing that matches network devices includes the device name, IP address, and type. If you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration Section, the table also includes the NDG of each matching network device.

Tip You can sort the table rows by whichever column you want, in ascending or descending order. Click a column title once to sort the rows by the entries in that column in ascending order. Click the column a second time to sort the rows by the entries in that column in descending order.

Step 5 If you want to view the configuration settings for a network device found by the search, click the network device name in the Name column in the table of matching network devices.

ACS displays the applicable setup page. For information about the AAA Client Setup page, see AAA Client Configuration Options, page 4-8. For information about the AAA Server Setup page, see AAA Server Configuration Options, page 4-15.

Step 6 If you want to download a file containing the search results in a comma-separated value format, click **Download**, and use your browser to save the file to a location and filename of your choice.

Step 7 If you want to search again by using different criteria, repeat Step 3 and Step 4.

AAA Client Configuration

This guide uses the term “AAA client” comprehensively to signify the device through which or to which service access is attempted. This is the RADIUS or TACACS+ client device, and may comprise Network Access Servers (NASs), PIX Firewalls, routers, or any other RADIUS or TACACS+ hardware or software client.

This section contains the following topics:

- AAA Client Configuration Options, page 4-8
- Adding AAA Clients, page 4-11
- Editing AAA Clients, page 4-13
- Deleting AAA Clients, page 4-14

AAA Client Configuration Options

AAA client configurations enable ACS to interact with the network devices that the configuration represents. A network device that does not have a corresponding configuration in ACS, or whose configuration in ACS is incorrect, does not receive AAA services from ACS.

The Add AAA Client and AAA Client Setup pages include:

- **AAA Client Hostname**—The name that you assign to the AAA client configuration. Each AAA client configuration can represent multiple network devices; thus, the AAA client hostname configured in ACS is not required to match the hostname configured on a network device. We recommend that you adopt a descriptive, consistent naming convention for AAA client hostnames. Maximum length for AAA client hostnames is 32 characters.

  Note After you submit the AAA client hostname, you cannot change it. If you want to use a different name for AAA clients, delete the AAA client configuration and create a new AAA client configuration by using the new name.

- **AAA Client IP Address**—At a minimum, a single IP address of the AAA client or the keyword **dynamic**.

  If you only use the keyword **dynamic**, with no IP addresses, the AAA client configuration can only be used for command authorization for Cisco multidevice-management applications, such as Management Center for Firewalls. ACS only provides AAA services to devices based on IP address; so it ignores such requests from a device whose AAA client configuration only has the keyword **dynamic** in the Client IP Address box.

  If you want the AAA client configuration in ACS to represent multiple network devices, you can specify multiple IP addresses. Separate each IP address by pressing **Enter**.

  In each IP address that you specify, you have three options for each octet in the address:

  - **Number**—You can specify a number, for example, 10.3.157.98.
  - **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen (-), for example, 10.3.157.10-50.
  - **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

  ACS allows any octet or octets in the IP Address box to be a number, a numeric range, or an asterisk (*), for example 172.16-31.*.*.

- **Key**—The shared secret of the AAA client. Maximum length for the AAA client key is 32 characters.

  For correct operation, the key must be identical on the AAA client and ACS. Keys are case sensitive. If the shared secret does not match, ACS discards all packets from the network device.

- **Network Device Group**—The name of the NDG to which this AAA client should belong. To make the AAA client independent of NDGs, use the Not Assigned selection.

  Note This option does not appear if you have not configured ACS to use NDGs. To enable NDGs, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- **Authenticate Using**—The AAA protocol to use for communications with the AAA client. The Authenticate Using list includes Cisco IOS TACACS+ and several vendor-specific implementations of RADIUS. If you have configured user-defined RADIUS vendors and VSAs, those vendor-specific RADIUS implementations appear on the list also. For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-19.

  The Authenticate Using list always contains:

  - **TACACS+ (Cisco IOS)**—The Cisco IOS TACACS+ protocol, which is the standard choice when using Cisco Systems access servers, routers, and firewalls. If the AAA client is a Cisco device-management application, such as Management Center for Firewalls, you must use this option.
  - **RADIUS (Cisco Airespace)**—RADIUS using Cisco Airespace VSAs. Select this option if the network device is a Cisco Airespace WLAN device supporting authentication via RADIUS.
  - **RADIUS (Cisco Aironet)**—RADIUS using Cisco Aironet VSAs. Select this option if the network device is a Cisco Aironet Access Point used by users who authenticate with the Lightweight and Efficient Application Protocol (LEAP) or the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) protocol, provided that these protocols are enabled on the Global Authentication Setup page in the System Configuration section.

    When an authentication request from a RADIUS (Cisco Aironet) AAA client arrives, ACS first attempts authentication by using LEAP; if this fails, ACS fails over to EAP-TLS. If LEAP is not enabled on the Global Authentication Setup page, ACS immediately attempts EAP-TLS authentication. If neither LEAP nor EAP-TLS is enabled on the Global Authentication Setup, any authentication attempt received from a Cisco Aironet RADIUS client fails. For more information about enabling LEAP or EAP-TLS, see Global Authentication Setup, page 10-19.

    Using this option enables ACS to send the wireless network device a different session-timeout value for user sessions than ACS sends to wired end-user clients.

    Note If all authentication requests from a particular Cisco Aironet Access Point are PEAP or EAP-TLS requests, use RADIUS (IETF) instead of RADIUS (Cisco Aironet). ACS cannot support PEAP authentication by using the RADIUS (Cisco Aironet) protocol.

  - **RADIUS (Cisco BBSM)**—RADIUS using Cisco Broadband Services Manager (BBSM) Vendor Specific Attributes (VSAs). Select this option if the network device is a Cisco BBSM network device supporting authentication via RADIUS.
  - **RADIUS (Cisco IOS/PIX 6.0)**—RADIUS using Cisco IOS/PIX 6.0 VSAs. This option enables you to pack commands sent to a Cisco IOS or Project Information Exchange (PIX)S 6.0 AAA client. The commands are defined in the Group Setup section. Select this option for RADIUS environments in which key TACACS+ functions are required to support Cisco IOS and PIX equipment.
  - **RADIUS (Cisco VPN 3000/ASA/PIX7.x+)**—RADIUS using Cisco VPN 3000 concentrator, ASA device, and PIX 7.x device VSAs. Select this option if the network device is a Cisco VPN 3000 series concentrator, an ASA, or PIX 7.x+ device supporting authentication via RADIUS.
  - **RADIUS (Cisco VPN 5000)**—RADIUS using Cisco VPN 5000 VSAs. Select this option if the network device is a Cisco VPN 5000 series Concentrator.
  - **RADIUS (IETF)**—IETF-standard RADIUS, using no VSAs. Select this option if the AAA client represents RADIUS-enabled devices from more than one manufacturer and you want to use standard IETF RADIUS attributes. If the AAA client represents a Cisco Aironet Access Point used only by users who authenticate with PEAP or EAP-TLS, this is also the protocol to select.

  - **RADIUS (Ascend)**—RADIUS using Ascend RADIUS VSAs. Select this option if the network device is an Ascend network device that supports authentication via RADIUS.
  - **RADIUS (Juniper)**—RADIUS using Juniper RADIUS VSAs. Select this option if the network device is a Juniper network device that supports authentication via RADIUS.
  - **RADIUS (Nortel)**—RADIUS using Nortel RADIUS VSAs. Select this option if the network device is a Nortel network device that supports authentication via RADIUS.
  - **RADIUS (iPass)**—RADIUS for AAA clients using iPass RADIUS. Select this option if the network device is an iPass network device supporting authentication via RADIUS. The iPass RADIUS is identical to IETF RADIUS.

- **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)**—If you select TACACS+ (Cisco IOS) from the Authenticate Using list, you can use this option to specify that ACS use a single TCP connection for all TACACS+ communication with the AAA client, rather than a new one for every TACACS+ request. In single connection mode, multiple requests from a network device are multiplexed over a single TCP session. By default, this check box is not checked.

  Note If TCP connections between ACS and the AAA client are unreliable, do not use this feature.

- **Log Update/Watchdog Packets from this AAA Client**—Enables logging of update or watchdog packets. Watchdog packets are interim packets that are sent periodically during a session. They provide you with an approximate session length if the AAA client fails and, therefore, no stop packet is received to mark the end of the session. By default, this check box is not selected.
- **Log RADIUS Tunneling Packets from this AAA Client**—Enables logging of RADIUS tunneling accounting packets. Packets are recorded in the RADIUS Accounting reports of Reports and Activity. By default, this check box is not selected.
- **Replace RADIUS Port info with Username from this AAA Client**—Enables use of username, rather than port number, for session-state tracking. This option is useful when the AAA client cannot provide unique port values, such as a gateway GPRS support node (GGSN). For example, if you use the ACS IP pools server and the AAA client does not provide a unique port for each user, ACS assumes that a reused port number indicates that the previous user session has ended and ACS may reassign the IP address that was previously assigned to the session with the nonunique port number. By default, this check box is not checked.

  Note If this option is enabled, ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users accessing the network through the AAA client with this feature enabled.

Adding AAA Clients

You can use this procedure to add AAA client configurations.

Before You Begin

For descriptions of the options that are available while adding AAA client configurations, see AAA Client Configuration Options, page 4-8.

For ACS to provide AAA services to AAA clients, you must ensure that gateway devices between AAA clients and ACS allow communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see AAA Protocols—TACACS+ and RADIUS, page 1-3.

To add AAA clients:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which you want to assign the AAA client. Then, click **Add Entry** below the AAA Clients table.
- To add AAA clients when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.

The Add AAA Client page appears.

Step 3 In the **AAA Client Hostname** box, type the name assigned to this AAA client (up to 32 alphanumeric characters).

Step 4 In the AAA Client IP Address box, do one of the following:

- Type the AAA client IP address or addresses. For information about using wildcards, octet ranges, or multiple IP address, see AAA Client Configuration Options, page 4-8.
- If the AAA client configuration will only be used for command authorization of Cisco multidevice-management applications, type **dynamic**.

Note If you only provide the keyword **dynamic**, ACS cannot use the AAA client configuration to provide AAA services to a network device; rather, it is used solely for command authorization of Cisco multidevice-management applications, such as Management Center for Firewalls.

Step 5 In the **Key** box, type the shared secret that the AAA client and ACS use to encrypt the data (up to 32 characters).

Note For correct operation, the identical key must be configured on the AAA client and ACS. Keys are case sensitive.

Step 6 If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs.

Note If you want to enable NDGs, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

Step 7 From the Authenticate Using list, select the network security protocol that the AAA client uses.

Tip If you are uncertain which protocol to select on the Authenticate Using list, see AAA Client Configuration Options, page 4-8.

Step 8 If you want to enable a single connection from the AAA client, rather than a new one for every TACACS+ request, select the **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)** check box.

Note If TCP connections between ACS and the AAA client are unreliable, do not use this feature.

Step 9 If you want to enable logging of watchdog packets, select the **Log Update/Watchdog Packets from this AAA Client** check box.

Step 10 If you want to enable logging of RADIUS tunneling accounting packets, select the **Log RADIUS tunneling Packets from this AAA Client** check box.

Step 11 If you want to track session state by username, rather than port number, select the **Replace RADIUS Port info with Username from this AAA** check box.

Note If this option is enabled, ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users who access the network through the AAA client with this feature enabled.

Step 12 If you want to save your changes and apply them immediately, click **Submit + Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter.

Tip If you want to save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

Editing AAA Clients

Use the following procedure to edit the settings for AAA client configurations.

Note You cannot directly edit the names of AAA clients; rather, you must delete the AAA client entry and then reestablish the entry with the corrected name. For steps about deleting AAA client configurations, see Deleting AAA Clients, page 4-14. For steps about creating AAA client configurations, see Adding AAA Clients, page 4-11.

Before You Begin

For descriptions of the options that are available while editing AAA client configurations, see AAA Client Configuration Options, page 4-8.

For ACS to provide AAA services to AAA clients, you must ensure that gateway devices between AAA clients and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see AAA Protocols—TACACS+ and RADIUS, page 1-3.

To edit AAA clients:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the name of the AAA client.
- To edit AAA clients when you have not enabled NDGs, click the name of the AAA client in the AAA Client Hostname column of the AAA Clients table.

The AAA Client Setup For *Name* page appears.

Step 3 Modify the AAA client settings, as needed. For information about the configuration options available for the AAA client, see AAA Client Configuration Options, page 4-8.

Note You cannot directly edit the name of the AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name. For steps about deleting the AAA client entry, see Deleting AAA Clients, page 4-14. For steps about creating the AAA client entry, see Adding AAA Clients, page 4-11.

Step 4 To save your changes and apply them immediately, click **Submit + Restart**.

Tip To save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter.

Configuring a Default AAA Client

You can configure a default AAA Client to accommodate any unrecognized AAA Clients (NAS):

Step 1 Follow the steps for Adding AAA Clients, page 4-11.

Step 2 Omit Step 3 and Step 4 leaving the AAA Client Hostname and AAA Client IP address blank.

Step 3 Enter a key and continue with the rest of the procedure for adding AAA Clients.

Note Only TACACS+ can have a default AAA Client configured. The default name for the client is **Others** and the default IP address is 0.0.0.0.

Deleting AAA Clients

To delete AAA clients:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the AAA client hostname in the AAA Clients table.
- To delete AAA clients when you have not enabled NDGs, click the AAA client hostname in the AAA Clients table.

The AAA Client Setup for the *Name* page appears.

Step 3 To delete the AAA client and have the deletion take effect immediately, click **Delete + Restart**.

Note Restarting ACS services clears the Logged-in User report and temporarily interrupts all ACS services. As an alternative to restarting when you delete AAA clients, you can click **Delete**. However, when you do, the change does not take effect until you restart the system, which you can do by choosing **System Configuration > Service Control**. Then, choose **Restart**.

A confirmation dialog box appears.

Step 4 Click **OK**.

ACS restarts AAA services and the AAA client is deleted.

If you have a configured RADIUS/TACACS source-interface command on the AAA client, ensure that you configure the client on ACS by using the IP address of the interface that is specified.

AAA Server Configuration

This section presents procedures for configuring AAA servers in the ACS web interface. For additional information about AAA servers, see AAA Servers in Distributed Systems, page 4-2.

To configure distributed system features for a given ACS, you must first define the other AAA server(s). For example, all ACSs that are involved in replication, remote logging, authentication proxying, and RDBMS synchronization must have AAA server configurations for each other; otherwise, incoming communication from an unknown ACS is ignored and the distributed system feature will fail.

Tip If the AAA Servers table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

This section contains the following topics:

- AAA Server Configuration Options, page 4-15
- Adding AAA Servers, page 4-16
- Editing AAA Servers, page 4-18
- Deleting AAA Servers, page 4-19

AAA Server Configuration Options

AAA server configurations enable ACS to interact with the AAA server that the configuration represents. AAA servers that do not have a corresponding configuration in ACS, or whose configuration in ACS is incorrect, does not receive AAA services from ACS, such as proxied authentication requests, database replication communication, remote logging, and RDBMS synchronization. Also, several distributed systems features require that the other ACSs included in the distributed system be represented in the AAA Servers table. For more information about distributed systems features, see About Distributed Systems, page 4-2.

The Add AAA Server and AAA Server Setup pages include the following options:

- **AAA Server Name**—The name that you assign to the AAA server configuration. The AAA server hostname that is configured in ACS does not have to match the hostname configured on a network device. We recommend that you adopt a descriptive, consistent naming convention for AAA server names. Maximum length for AAA server names is 32 characters.

  Note After you submit the AAA server name, you cannot change it. If you want to use a different name for the AAA server, delete the AAA server configuration and create the AAA server configuration by using the new name.

- **AAA Server IP Address**—The IP address of the AAA server, in dotted, four-octet format. For example, 10.77.234.3.
- **Key**—The shared secret of the AAA server. Maximum length for AAA server keys is 32 characters.

  For correct operation, the key must be identical on the remote AAA server and ACS. Keys are case sensitive. Because shared secrets are not synchronized, you could easily to make mistakes when entering them on remote AAA servers and ACS. If the shared secret does not match, ACS discards all packets from the remote AAA server.

- **Network Device Group**—The name of the NDG to which this AAA server should belong. To make the AAA server independent of NDGs, use the Not Assigned selection.

Note This option does not appear if you have not configured ACS to use NDGs. To enable NDGs, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- **Log Update/Watchdog Packets from this remote AAA Server**—Enables logging of update or watchdog packets from AAA clients that are forwarded by the remote AAA server to this ACS. Watchdog packets are interim packets that are sent periodically during a session. They provide you with an approximate session length if the AAA client fails and, therefore, no stop packet is received to mark the end of the session.
- **AAA Server Type**—One of types:
  - **RADIUS**—Select this option if the remote AAA server is configured by using any type of RADIUS protocol.
  - **TACACS+**—Select this option if the remote AAA server is configured by using the TACACS+ protocol.
  - **ACS**—Select this option if the remote AAA server is another ACS. This action enables you to configure features that are only available with other ACSs, such as ACS internal database replication and remote logging.

Note The remote ACS must be using version 2.1 or later.

- **Traffic Type**—The Traffic Type list defines the direction in which traffic to and from the remote AAA server is permitted to flow from this ACS. The list includes:
  - **Inbound**—The remote AAA server accepts requests that have been forwarded to it and does not forward the requests to another AAA server. Select this option if you do not want to permit any authentication requests to be forwarded from the remote AAA server.
  - **Outbound**—The remote AAA server sends out authentication requests but does not receive them. If a Proxy Distribution Table entry is configured to proxy authentication requests to the AAA server that is configured for Outbound, the authentication request is not sent.
  - **Inbound/Outbound**—The remote AAA server forwards and accepts authentication requests, allowing the selected server to handle authentication requests in any manner that is defined in the distribution tables.

Adding AAA Servers

Before You Begin

For descriptions of the options that are available while adding a remote AAA server configuration, see AAA Server Configuration Options, page 4-15.

For ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see AAA Protocols—TACACS+ and RADIUS, page 1-3.

To add and configure AAA servers:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is to be assigned. Then, click **Add Entry** below the [name] AAA Servers table.
- To add AAA servers when you have not enabled NDGs, below the AAA Servers table, click **Add Entry**.

The Add AAA Server page appears.

Step 3 In the **AAA Server Name** box, type a name for the remote AAA server (up to 32 characters).

Step 4 In the **AAA Server IP Address** box, type the IP address assigned to the remote AAA server.

Step 5 In the **Key** box, type the shared secret that the remote AAA server and the ACS use to encrypt the data (up to 32 characters).

Note The key is case sensitive. If the shared secret does not match, ACS discards all packets from the remote AAA server.

Step 6 From the Network Device Group list, select the NDG to which this AAA server belongs.

Note To enable NDGs, choose **Interface Configuration > Advanced Options**. Then, choose **Network Device Groups**.

Step 7 To enable watchdog packets, select the **Log Update/Watchdog Packets from this remote AAA Server** check box.

Step 8 From the AAA Server Type list, select the AAA server type applicable to the remote AAA server. If the remote AAA server is another ACS, identify it as such by selecting **Cisco Secure ACS**.

Step 9 From the Traffic Type list, select the type of traffic that you want to permit between the remote AAA server and ACS.

Step 10 To save your changes and apply them immediately, click **Submit + Restart**.

Tip To save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to (0).

Editing AAA Servers

Use this procedure to edit the settings for AAA servers that you have previously configured.

Note You cannot edit the names of AAA servers. To rename AAA servers, you must delete the existing AAA server entry and then add a new server entry with the new name.

Before You Begin

For descriptions of the options available while editing a remote AAA server entry, see AAA Server Configuration Options, page 4-15.

For ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see AAA Protocols—TACACS+ and RADIUS, page 1-3.

To edit AAA servers:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, in the AAA Servers table, click the name of the AAA server to be edited.
- If you have not enabled NDGs, in the AAA Servers table, click the name of the AAA server to be edited.

The AAA Server Setup for *X* page appears.

Step 3 Enter or select new settings for one or more of the following fields:

- **AAA Server IP Address**
- **Key**
- **Log Update/Watchdog Packets from this remote AAA Server**
- **AAA Server Type**
- **Traffic Type**

Step 4 To save your changes and apply them immediately, click **Submit + Restart**.

Tip To save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to (0).

Deleting AAA Servers

To delete AAA servers:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, click the AAA server name in the AAA Servers table.
- If you have not enabled NDGs, click the AAA server name in the AAA Servers table.

The AAA Server Setup for *X* page appears.

Step 3 To delete the AAA server and have the deletion take effect immediately, click **Delete + Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. As an alternative to restarting when you delete AAA servers, in the preceding step you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by choosing **System Configuration > Service Control**. Then, choose **Restart**.

A confirmation dialog box appears.

Step 4 Click **OK**.

ACS performs a restart and the AAA server is deleted.

Network Device Group Configuration

Network Device Grouping is an advanced feature that you use to view and administer a collection of network devices as a single logical group. To simplify administration, you can assign each group a name that can be used to refer to all devices within that group. This action creates two levels of network devices within ACS—single discrete devices such as an individual router or network-access server, and an NDG; that is, a collection of routers or AAA servers.

Caution To see the Network Device Groups table in the web interface, you must check the Network Device Groups option on the Advanced Options page of the Interface Configuration section. Unlike in other areas of Interface Configuration, it is possible to remove from sight an active NDG if you uncheck the Network Device Groups option. Therefore, if you choose to configure NDGs, ensure that you leave the Network Device Groups option selected on the Advanced Option page.

This section contains the following topics:

- Adding a Network Device Group, page 4-20
- Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-21
- Reassigning AAA Clients or AAA Servers to an NDG, page 4-21

- Renaming a Network Device Group, page 4-22
- Deleting a Network Device Group, page 4-22

Adding a Network Device Group

You can assign users or groups of users to NDGs. For more information, see:

- Setting TACACS+ Enable Password Options for a User, page 7-23
- Setting Enable Privilege Options for a User Group, page 6-13

To add an NDG:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Under the Network Device Groups table, click **Add Entry**.

Tip If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then, choose **Network Device Groups**.

Step 3 In the Network Device Group Name box, type the name of the new NDG.

Tip The maximum name length is 24 characters. Quotation marks (“) and commas (,) are not allowed. Spaces are allowed.

Step 4 In the **Key** box, enter a key for the Network Device Group. The maximum length is 32 characters.

Each device that is assigned to the Network Device Group will use the shared key that you enter here. The key that was assigned to the device when it was added to the system is ignored. If the key entry is null, the AAA client key is used. See AAA Client Configuration Options, page 4-8. This feature simplifies key management for devices.

Step 5 Click **Submit**.

The Network Device Groups table displays the new NDG.

Step 6 To populate the newly established NDG with AAA clients or AAA servers, perform one or more of the following procedures, as applicable:

- Adding AAA Clients, page 4-11
- Adding AAA Servers, page 4-16
- Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-21
- Reassigning AAA Clients or AAA Servers to an NDG, page 4-21

Assigning an Unassigned AAA Client or AAA Server to an NDG

You use this procedure to assign an unassigned AAA client or AAA server to an NDG. Before you begin this procedure, you should have already configured the client or server and it should appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

To assign a network device to an NDG:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Network Device Groups table, click **Not Assigned**.

Tip If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

Step 3 Click the name of the network device that you want to assign to an NDG.

Step 4 From the Network Device Groups list, select the NDG to which you want to assign the AAA client or AAA server.

Step 5 Click **Submit**.

The client or server is assigned to an NDG.

Reassigning AAA Clients or AAA Servers to an NDG

To reassign AAA clients or AAA servers to a new NDG:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Network Device Groups table, click the name of the current group of the network device.

Step 3 In the AAA Clients table or AAA Servers table, as applicable, click the name of the client or server that you want to assign to a new NDG.

Step 4 From the Network Device Group list, select the NDG to which you want to reassign the network device.

Step 5 Click **Submit**.

The network device is assigned to the NDG you selected.

Renaming a Network Device Group

Caution When renaming an NDG, ensure that there are no NARs or other shared profile components (SPCs) that invoke the original NDG name. ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user's authentication request incorporates an SPC that invokes a nonexistent (or renamed) NDG, the attempt will fail and the user will be rejected.

To rename an NDG:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Network Device Groups table, click the NDG that you want to rename.

Tip If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

Step 3 At the bottom of the page, click **Rename**.

The Rename Network Device Group page appears.

Step 4 In the Network Device Group Name box, type the new name (up to 24 characters).

Step 5 Click **Submit**.

The name of the NDG is changed.

Deleting a Network Device Group

When you delete an NDG, all AAA clients and AAA servers that belong to the deleted group appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

Tip It might be useful to empty an NDG of AAA clients and AAA servers before you delete it. You can do this manually by performing the procedure Reassigning AAA Clients or AAA Servers to an NDG, page 4-21; or, in cases where you have a large number of devices to reassign, use the RDBMS Synchronization feature.

Caution When deleting an NDG, ensure that there are no NARs or other SPCs that invoke the original NDG. ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user authentication request incorporates an SPC that invokes a nonexistent (or renamed) NDG, the attempt will fail and the user will be rejected.

To delete an NDG:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Network Device Groups table, click the NDG that you want to delete.

Tip If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then check the **Network Device Groups** check box.

Step 3 At the bottom of the page, click **Delete Group**.

A confirmation dialog box appears.

Step 4 Click **OK**.

The NDG is deleted and its name is removed from the Network Device Groups table. Any AAA clients and AAA servers that were in the NDG are now in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

Proxy Distribution Table Configuration

This section describes the Proxy Distribution Table and provides procedures for working with the Proxy Distribution Table.

This section contains the following topics:

- About the Proxy Distribution Table, page 4-23
- Adding a New Proxy Distribution Table Entry, page 4-24
- Sorting the Character String Match Order of Distribution Entries, page 4-25
- Editing a Proxy Distribution Table Entry, page 4-25
- Deleting a Proxy Distribution Table Entry, page 4-26

About the Proxy Distribution Table

If you enabled the Distributed Systems Settings, when you click Network Configuration, you will see the Proxy Distribution Table.

Tip To enable Distributed Systems Settings in the ACS, choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

The Proxy Distribution Table includes entries that show the character strings on which to proxy, the AAA servers to proxy to, whether to strip the character string, and where to send the accounting information (Local/Remote, Remote, or Local). For more information about the proxy feature, see Proxy in Distributed Systems, page 4-3.

The entries that you define and place in the Proxy Distribution Table are treated one at a time for each authentication request that ACS receives from the AAA client. The authentication request is defined in the Proxy Distribution Table according to the forwarding destination. If a match to an entry in the Proxy Distribution Table that contains proxy information is found, ACS forwards the request to the appropriate AAA server.

The Character String column in the Proxy Distribution Table always contains an entry of (Default). The (Default) entry matches authentication requests that are received by the local ACS that do not match any other defined character strings. While you cannot change the character string definition for the (Default) entry, you can change the distribution of authentication requests matching the (Default) entry. At installation, the AAA server associated with the (Default) entry is the local ACS. You might sometimes find it easier to define strings that match authentication requests to be processed locally rather than defining strings that match authentication requests to be processed remotely. In such a case, associating the (Default) entry with a remote AAA server permits you to configure your Proxy Distribution Table with the more easily written entries.

Adding a New Proxy Distribution Table Entry

To create a Proxy Distribution Table entry:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Under the Proxy Distribution Table, click **Add Entry**.

Note If the Proxy Distribution Table does not appear, choose **Interface Configuration > Advanced Options**. Then, select the **Distributed System Settings** check box.

Step 3 In the Character String box, type the string of characters, including the delimiter to forward on when users dial in to be authenticated. For example, *.uk*.

Note Angle brackets (<>) cannot be used.

Step 4 From the Position list, select **Prefix** if the character string that you typed appears at the beginning of the username or **Suffix** if the character string appears at the end of the username.

Step 5 From the Strip list, select **Yes** to strip the character string from the username that you entered, or select **No** to leave it.

Step 6 In the AAA Servers column, select the AAA server that you want to use for proxy. Click the **-->** (right arrow button) to move it to the Forward To column.

Tip You can also select additional AAA servers to use for backup proxy if the prior servers fail. To set the order of AAA servers, in the Forward To column, click the name of the applicable server and click **Up** or **Down** to move it into the position that you want.

Tip If the AAA server that you want to use is not listed, choose **Network Configuration > AAA Servers**. Then, choose **Add Entry** and complete the applicable information.

Step 7 From the Send Accounting Information list, select one of the following areas to which to report accounting information:

- **Local**—Keep accounting packets on the local ACS.
- **Remote**—Send accounting packets to the remote ACS.
- **Local/Remote**—Keep accounting packets on the local ACS and send them to the remote ACS.

Tip This information is especially important if you are using the Max Sessions feature to control the number of connections that a user is allowed. Max Sessions depends on accounting start and stop records, and where the accounting information is sent determines where the Max Sessions counter is tracked. The Failed Attempts log and the Logged in Users report are also affected by where the accounting records are sent. See Remote Use of Accounting Packets, page 4-5 for an example.

Step 8 When you finish, click **Submit** or **Submit + Restart**.

Sorting the Character String Match Order of Distribution Entries

You can use this procedure to set the priority by which ACS searches character string entries in the Proxy Distribution Table when users dial in.

To determine the order by which ACS searches entries in the Proxy Distribution Table:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Below the Proxy Distribution Table, click **Sort Entries**.

Tip Before you sort the entries, you must configure at least two unique Proxy Distribution Table entries in addition to the (Default) table entry.

Step 3 Select the character string entry to reorder, and then click **Up** or **Down** to move its position to reflect the search order that you want.

Step 4 When you finish sorting, click **Submit** or **Submit + Restart**.

Editing a Proxy Distribution Table Entry

To edit a Proxy Distribution Table entry:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Character String column of the Proxy Distribution Table, click the distribution entry that you want to edit.

The Edit Proxy Distribution Entry page appears.

Step 3 Edit the entry as necessary.

Tip For information about the parameters that make up a distribution entry, see Adding a New Proxy Distribution Table Entry, page 4-24.

Step 4 When you finish editing the entry, click **Submit** or **Submit + Restart**.

Deleting a Proxy Distribution Table Entry

To delete a Proxy Distribution Table entry:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Character String column of the Proxy Distribution Table, click the distribution entry that you want to delete.

The Edit Proxy Distribution Entry page appears.

Step 3 Click **Delete**.

A confirmation dialog box appears.

Step 4 Click **OK**.

The distribution entry is deleted from the Proxy Distribution Table.

Shared Profile Components

This chapter contains information about the features in the Shared Profile Components section of the web interface for Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains the following topics:

- About Shared Profile Components, page 5-1
- Network Access Filters, page 5-2
- RADIUS Authorization Components, page 5-6
- Downloadable IP ACLs, page 5-13
- Network Access Restrictions, page 5-17
- Command Authorization Sets, page 5-24

About Shared Profile Components

You use the Shared Profile Components section to develop and name reusable, shared sets of authorization components that may be applied to one or more users or groups of users, and referenced by name within their profiles. These include network-access filters (NAFs), RADIUS Authorization Components (RACs), downloadable IP access control lists (IP ACLs), Network Access Restrictions (NARs), and command-authorization sets.

The Shared Profile Components section addresses the scalability of selective authorization. Shared profile components can be configured and then applied to many users or groups. Without this ability, you could only accomplish flexible and comprehensive authorization explicitly configuring the authorization of each user group on each device. Creating and applying these named shared-profile components (downloadable IP ACLs, NAFs, RACs, NARs, and command-authorization sets) makes it unnecessary to repeatedly enter long lists of devices or commands when defining network-access parameters.

802.1X Example Setup

Table 5-1 describes an example scenario to help you understand how SPCs are deployed. If, for example, you are deploying 802.1X and Network Admission Control (NAC), you might configure:

Table 5-1 802.1X Example SPC Scenario

Shared Profile Component	Description	Notes
Network Access Filters	NAFs are the most common way of defining which devices will be part of a given network service and, therefore, Network Access Profile (NAP).	• If you have switches or routers being upgraded for NAC, you can use a NAF to distinguish between those devices that can and cannot do NAC. • If you have Network Device Groups (NDGs) for groups of devices based on geography, NAFs allow you to aggregate the NDGs. In this case, you might want to set up a NAF for each NAP configured.
ACLs	NAC uses ACLs in order to manage clients that required limited access (for example, if there is no NAC-supplicant or to enforce an upgrade policy).	• Create ACLs related to posture and NAC agentless hosts (NAH). • Use ACLs to control access to servers running network applications (such as software for sales, human resource, or accounting) which can be mapped from the users group. For example, the HR group gets an HR ACL.
RACs	Use RACs to set up service-differentiated RADIUS authorization.	• Set up RACs for each network service (VPN, WLAN, dial, and so on). For example, set different session-timeouts for VPN and WLAN. • Use NAP templates to save time setting up 802.1X profiles. They require different provisioning and so require SRACs for each.
NARs	Use NARs to create additional conditions that must be met before a user can access the network. ACS applies these conditions by using information from attributes sent by authentication, authorization, and accounting (AAA) clients.	• Create a CLI/DNIS NAR listing the MAC addresses of all the non-NAC devices (maybe a printer or legacy system) that are allowed to access the network. This method will protect your network. • With NAC, use NARs for NAH scenarios with MAC and IP exceptions handling. Wildcarding the MAC and IP addresses is allowed.

Network Access Filters

This section describes NAFs and provides instructions for creating and managing them.

This section contains the following topics:

- About Network Access Filters, page 5-3
- Adding a Network Access Filter, page 5-3
- Editing a Network Access Filter, page 5-5
- Deleting a Network Access Filter, page 5-6

About Network Access Filters

A NAF is a named group of any combination of one or more of the following network elements:

- IP addresses
- AAA clients (network devices)
- Network device groups (NDGs)

Using a NAF to specify a downloadable IP ACL or NAR—based on the AAA clients by which the user may access the network—saves you the effort of listing each AAA client explicitly. NAFs are the most common way of defining which devices will be part of a given network service and, therefore, Network Access Profile (NAP). NAFs exhibit the following characteristics:

- **NAFs in downloadable IP ACLs**—You can associate a NAF with specific ACL contents. A downloadable IP ACL comprises one or more ACL contents (sets of ACL definitions) that are associated with a single NAF or, by default, "All-AAA-Clients". This pairing of ACL content with a NAF permits ACS to determine which ACL content is downloaded according to the IP address of the AAA client making the access request. For more information on using NAFs in downloadable IP ACLs, see About Downloadable IP ACLs, page 5-13.
- **NAFs in shared Network Access Restrictions**—An essential part of specifying a shared NAR is listing the AAA clients from which user access is permitted or denied. Rather than list every AAA client that makes up a shared NAR, you can simply list one or more NAFs instead of, or in combination with, individual AAA clients. For more information on using NAFs in shared NARs, see About Network Access Restrictions, page 5-18.

Tip Shared NARs can contain NDGs, or NAFs, or both. NAFs can contain one or more NDGs.

You can add a NAF that contains any combination of NDG, network devices (AAA clients), or IP addresses. For these network devices or NDGs to be selectable you must have previously configured them in ACS.

The network elements that a NAF comprises can be arranged in any order. For best performance, place the elements most commonly encountered at the top of the Selected Items list. For example, in a NAF where the majority of users gain network access through the NDG accounting, but you also grant access to a single technical support AAA client with the IP address 205.205.111.222, you would list the NDG first (higher) in the list of network elements to prevent all NAF members from having to be examined against the specified IP address.

Adding a Network Access Filter

To add a NAF:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Filtering**.

The Network Access Filtering table page appears.

Tip If Network Access Filtering does not appear as a selection on the Shared Profile Components page, you must enable it on the Advanced Options page of the Interface Configuration section.

Step 3 Click **Add**.

The Network Access Filtering edit page appears.

Step 4 In the **Name** box, type the name of the new network-access filter.

Note The name of a NAF can contain up to 31 characters. Spaces are not allowed. Names cannot contain: left bracket ([), right bracket (]), comma(,), slash (/), dash (–), hyphen (-), quotes (“), apostrophe (‘), right angle bracket (>), left angle bracket (<).

Step 5 In the **Description** box, type a description of the new network-access filter. The description can be up to 30,000 characters.

Step 6 Add network elements to the NAF definition as applicable:

a. To include an NDG in the NAF definition, from the **Network Device Groups** box, select the NDG; then click **-->** (right arrow button) to move it to the **Selected Items** box.

b. To include a AAA client in the NAF definition, from the **Network Device Groups** box, select the applicable NDG and then, from the **Network Devices** box, select the AAA client you want to include. Finally, click **-->** (right arrow button) to move it to the **Selected Items** box.

Tip If you are using NDGs, the AAA clients appear in the Network Devices box only when you have selected the NDG to which they belong. Otherwise, if you are not using NDGs, you can select the AAA client from the **Network Devices** box with no prior NDG selection.

c. To include an IP address in the NAF definition, type the IP address in the **IP Address** box. Click **-->** (right arrow button) to move it to the **Selected Items** box.

Note You can use the asterisk (*), which is the wildcard character, to designate a range within an IP address.

Step 7 Ensure that the order of the items is correct. To change the order of items, in the **Selected Items** box, click the name of an item, and then click **Up** or **Down** to move it to the position that you want.

Tip You can also remove an item from the Selected Items box by selecting the item and then clicking **<--** (left arrow button) to remove it from the list.

Step 8 To save your NAF and apply it immediately, choose **Submit + Restart**.

Tip To save your NAF and apply it later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to zero (0).

The Network Access Filtering table page appears, and lists the name and description of the new NAF.

Editing a Network Access Filter

To edit a NAF:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Filtering**.

The Network Access Filtering table appears.

Step 3 In the Name column, click the NAF that you want to edit.

The Network Access Filter page appears with information visible for the selected NAF.

Step 4 Edit the Name or Description of the NAF; type and delete information, as applicable. The description can be up to 30,000 characters.

Caution If you change the name of a NAF, you invalidate all existing references to that NAF; this action might affect the access of users or groups that are associated with NARs or downloadable ACLs that use that NAF.

Step 5 To add a NDG to the NAF definition, from the Network Device Groups box, select the NDG that you want to add. Click **-->** (right arrow button) to move it to the **Selected Items** box.

Step 6 To add a AAA client in the NAF definition, from the **Network Device Groups** box select the applicable NDG and then, from the Network Devices box, select the AAA client that you want to add. Click **-->** (right arrow button) to move it to the Selected Items box.

Tip If you are not using NDGs, you begin by selecting the AAA client from the **Network Devices** box.

Step 7 To add an IP address to the NAF definition, in the **IP Address** box, type the IP address that you want to add. Click **-->** (right arrow button) to move it to the **Selected Items** box.

Step 8 To edit an IP address, choose it in the **Selected Items** box and then click **<--** (left arrow button) to move it to the IP address box. Type the changes to the IP address and then click **-->** (right arrow button) to move it back to the **Selected Items** box.

Step 9 To remove an element from the **Selected Items** box, choose the item and then click **<--** (left arrow button) to remove it.

Step 10 To change the order of items, in the **Selected Items** box, click the name of an item, and then click **Up** or **Down** to move it into the position that you want. For more information on arranging the order of NAFs see About Network Access Filters, page 5-3.

Step 11 To save the changes to your NAF and apply them immediately, click **Submit + Restart**.

Tip To save your NAF and apply it later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to zero (0).

ACS reenters the NAF with the new information, which takes effect immediately.

Deleting a Network Access Filter

Before You Begin

Before you delete a NAF you should remove its association with any NAR, downloadable IP ACL, or network access profile that uses it. Otherwise, any NAR, downloadable IP ACL, or network access profile that references the deleted NAF will be misconfigured and will produce an error.

To delete a NAF:

Step 1 In the navigation bar, click **Network Access Filtering**.

The Network Access Filtering table page appears.

Step 2 Click the name of the NAF that you want to delete.

The Network Access Filtering edit page appears.

Step 3 Click **Delete** and then click **OK** to confirm.

The Network Access Filtering table page appears with the name and description of the NAF removed from the table.

RADIUS Authorization Components

This section describes RADIUS Authorization Components (RACs) and provides instructions for configuring and managing them.

The following topics are described:

- About RADIUS Authorization Components, page 5-7
- Before You Begin Using RADIUS Authorization Components, page 5-8
- Adding RADIUS Authorization Components, page 5-9
- Cloning a RADIUS Authorization Component, page 5-10
- Editing a RADIUS Authorization Component, page 5-10
- Deleting a RADIUS Authorization Component, page 5-11

About RADIUS Authorization Components

Shared Radius Authorization Components (RACs) contain groups of RADIUS attributes that you can dynamically assign to user sessions based on a policy. Using the Network Access Profile configuration, you can map a policy type with set conditions, such as Network Device Groups and posture, to a shared RAC.

Understanding RACs and Groups

In ACS, RACs contain attributes that can be specific to a single network service (also referred to as a network-access policy). The access policy can map from various groups and postures to a set of RACs and ACLs. For more information on setting up network-access policies, see Chapter 15, "Network Access Profiles."

ACS groups contain attributes that are related to the user group (for example, administrators, contractors, and so on) and do not cater to the same groups of users that require authorization for different network services (WLAN and VPN, for example).

Use RACs when you require service-differentiated RADIUS authorization. For example, when you must set the session-timeout to be several days for VPN and several hours for WLAN.

You can still use group attributes (if the authorization policy check box is selected) so that service-independent attributes can be applied to all users of the group without having to duplicate into each RAC for each service.

Caution If Group and RAC attributes are merged, the final result might be unpredictable. See Chapter 15, "Network Access Profiles," for complete information.

Migrating Away from Groups to RACs

If your network strategy demands service-based profiles and you migrate away from groups to RACs, you must define appropriate access services and policies:

- Define appropriate network-access policies and define rules.
- Design what user group and posture should get which level of authorization by creating a matrix.
- Group all similar authorization cases and create RACs for them.
- Remove any legacy attributes from the user groups if necessary.

Vendors

Note RADIUS security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco IOS/PIX 6.0) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco IOS/PIX 6.0) in the Authenticate Using list.

The RADIUS vendor-specific attribute (VSA) sets that ACS supports are:

- **Cisco Aironet**—VSAs for Cisco Aironet Access Point products. *Not* supported for shared RAC; use IETF session timeout instead.

- **Cisco Airespace**—VSAs for Cisco Airespace wireless LAN devices.
- **Cisco BBSM**—VSAs for Cisco Building Broadband Service Manager (BBSM) products.
- **Cisco IOS/PIX 6.0**—VSAs for Cisco IOS products and Cisco PIX firewalls earlier than 6.0 releases.
- **Cisco VPN 3000/ASA/PIX 7.x+**—VSAs for Cisco VPN 3000-series Concentrators, ASA devices, and PIX devices later than 7.x releases.
- **Cisco VPN 5000**—VSAs for Cisco VPN 5000-series Concentrators.
- **Ascend**—VSAs for Ascend products.
- **Microsoft**—VSAs for Microsoft Point-to-Point Encryption and Point-to-Point Compression.
- **Nortel**—VSAs for Nortel products.
- **Juniper**—VSAs for Juniper products.

Attribute Types

The vendor-specific attributes are not defined. Definitions can be found in the documentation for that vendor software. For Cisco vendor-specific attributes, see Appendix C, "RADIUS Attributes." To add attributes by using the **CsUtil** command, see Appendix D, "CSUtil Database Utility."

Before You Begin Using RADIUS Authorization Components

For you to use the Shared Profile Components' RACs, you must ensure that you have properly set up ACS. Review this checklist before you create shared profile components:

Tip Use the Network Access Profile templates to save time. NAP templates automatically create a set of shared profile components if none are configured. For details, see Shared-profile Components, page 15-13.

1. Add devices to ACS. For ACS to interact with AAA clients and servers you must add their network information. For instructions on how to add devices by using Network Configuration, see Adding AAA Clients, page 4-11.
2. Enable the attributes (VSAs) that you want to use. Disable those attributes that you do not want to use. If attributes are not enabled, they will not appear on the RADIUS Authorization Components page. the Interface Configuration set up pages. For details on enabling VSAs, see Chapter 3, "Interface Design Concepts."
3. Map out your network access profile design. You must identify the network services that require provisioning. You will probably identify at least one shared RADIUS authorization component (SRAC) for each profile. For details on linking a SRAC to a profile, see Setting Up a Profile, page 15-3 or Using Profile Templates, page 15-13.
4. For each profile that you are creating, identify how you plan to classify network-access requests and any exception cases (for example, special users or groups, bad posture status, and so on) and create SRACs for each. See About RADIUS Authorization Components, page 5-7.
5. Decide whether any attributes are user or group-specific (rather than network service-specific). If you must assign attributes to a user or group, regardless of network service, add these to the user or group record and enable attribute merging in the network access profile. For details on attribute merging, see Merging Attributes, page 15-47.

For specific steps on enabling RADIUS Authorization Components, see Enabling Use of RAC, page 5-9.

Enabling Use of RAC

To enable use of RAC:

Step 1 Before setting RADIUS Authorization Components, add your devices by using Network Configuration and configure them to authenticate by using the correct security protocol (such as RADIUS Cisco VPN 3000/ASA/PIX 7.x+).

If your attribute does not appear in the Authenticate Using list, check the Interface Configuration or your User Setup/Group Setup parameters.

Step 2 In the navigation bar, click **Interface Configuration** and select **RADIUS (IETF)**.

Note RADIUS security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) in the Authenticate Using list.

Step 3 Select the desired RADIUS attributes and click **Submit**.

Step 4 Repeat Step 2 and Step 3 for each RADIUS security protocol in your network configuration.

Step 5 Ensure that Tunneling RADIUS attributes are selected in Advanced Options.

- Choose **Interface Configuration > RADIUS (IETF)**.
- Choose the Tunnel attributes.
- Click **Submit**.

Step 6 In the navigation bar, click **Shared Profile Components** and select **RADIUS Authorization Components**.

For details on adding RACs, see Adding RADIUS Authorization Components, page 5-9. For details on changing RACs, see Editing a RADIUS Authorization Component, page 5-10. For details on how to add RACs to network access profiles, see Configuring an Authorization Rule, page 15-44.

Adding RADIUS Authorization Components

Before You Begin

You should have already configured any RADIUS options that you plan to use on ACS. For details on what to configure, see Vendors, page 5-7.

To add an RAC, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **RADIUS Authorization Components**.

The RADIUS Authorization Components Table Page appears.

Step 3 Click **Add** to create a new RADIUS Authorization Component.

The Edit RADIUS Authorization Component Page appears.

Step 4 To add a new attribute, select the correct vendor attribute by using the drop-down list and click the **Add** button.

The RAC Attribute Add/Edit Page appears.

Note The vendors that are available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at the group or user level) under Interface Configuration.

Step 5 Select the attribute value and click **Submit**.

Cloning a RADIUS Authorization Component

To make a copy of an existing RAC by using the clone feature:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **RADIUS Authorization Components**.

The RADIUS Authorization Components Table Page appears.

Step 3 Select the RAC name of the component that you want to clone.

The Edit RADIUS Authorization Component Page appears.

Step 4 To clone an existing RAC with all of its attributes, click **Clone**.

A clone named Copy of RACname is created in the Edit RADIUS Authorization Component page.

Step 5 Click **Submit to save the new RAC**.

Editing a RADIUS Authorization Component

To edit an existing RAC:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **RADIUS Authorization Components**.

The RADIUS Authorization Components Table Page appears.

Step 3 Select the RAC name of the component that you want to edit.

The Edit RADIUS Authorization Component Page appears.

Step 4 To add a new attribute, select the correct vendor attribute by using the drop-down list and click the adjacent **Add** button.

Step 5 To alter an existing attribute, select the value in Assigned Attributes.

The RAC Attribute Add/Edit Page appears.

- To delete an attribute and its value, click **Delete**.
- To edit the attribute, change the attribute value and click **Submit**.

Deleting a RADIUS Authorization Component

Before You Begin

You should remove the association of an RAC with any network access profile before deleting the RAC.

To delete an RAC:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **RADIUS Authorization Components**.

The RADIUS Authorization Components Table Page appears.

Step 3 Select the RAC name of the component that you want to delete.

The Edit RADIUS Authorization Component Page appears.

Step 4 Click **Delete** to remove the RADIUS Authorization Component.

Step 5 Click **OK** to remove the RADIUS Authorization Component.

The current configuration changes. A dialog box appears and asks that you restart ACS by choosing **System Configuration > Service Control** to adopt the new settings.

RADIUS Authorization Components Table Page

Use this page to list or activate the configuration for a shared RAC.

Field	Description
Name	Click to activate the configuration for the RAC. Opens the Edit RADIUS Authorization Component Page.
Description	Displays the RAC description. The description can be up to 30,000 characters.
Add	Click to add a new RAC. Opens the Edit RADIUS Authorization Component Page.

Edit RADIUS Authorization Component Page

Use this page to configure the RAC.

Field	Description
Name	Enter the name that you want to assign to the RADIUS Authorization Components.
Description	Enter a description for the RAC. The description can be up to 30,000 characters.
Add New Attribute	Use the Vendor and Service Type fields to add new attribute values. Vendors available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at group level) under Interface Configuration. For details on setting up devices, see Chapter 4, "Network Configuration." For details on setting up the interface, see Chapter 3, "Using the Web Interface." Select the vendor attribute from the drop-down list and click **Add**. This action opens the RAC Attribute Add/Edit Page.
Assigned Attributes	Use this table to view, edit, and select the list of RADIUS attributes assigned to the Authorization Component. To edit or delete an already assigned attribute, click on the attribute value. Opens the RAC Attribute Add/Edit Page.
Vendor Attribute Value	Appears if assigned attributes are present. Click on the value to edit or delete. Opens the RAC Attribute Add/Edit Page.
Submit	Click to submit the RAC configuration to ACS.
Delete	Appears if assigned attributes are present. Click to delete the RAC. To delete a single attribute, go to the RAC Attribute Add/Edit Page.

RAC Attribute Add/Edit Page

Field	Description
RAC	Name assigned to the RADIUS Authorization Component.
Vendor	Name of the organization the vendor-specific attributes.
Clone	Copy an existing RAC attributes into a new RAC named Copy of RAC name.
Attribute	Attribute defined for RAC.
Type	Attribute type of integer or text.
Value	Drop-down box or text value settings.
Submit	Click to submit the RAC configuration to ACS.
Delete	Click to delete this single attribute.

Downloadable IP ACLs

This section describes downloadable ACLs and provides detailed instructions for configuring and managing them.

This section contains the following topics:

- About Downloadable IP ACLs, page 5-13
- Adding a Downloadable IP ACL, page 5-15
- Editing a Downloadable IP ACL, page 5-16
- Deleting a Downloadable IP ACL, page 5-17

About Downloadable IP ACLs

You can use downloadable IP ACLs to create sets of ACL definitions that you can apply to many users or user groups. These sets of ACL definitions are called ACL contents. Also, by incorporating NAFs, you can control the ACL contents that are sent to the AAA client from which a user is seeking access. That is, a downloadable IP ACL comprises one or more ACL content definitions, each of which is associated with a NAF or (by default) associated to all AAA clients. (The NAF controls the applicability of specified ACL contents according to the AAA client's IP address. For more information on NAFs and how they regulate downloadable IP ACLs, see About Network Access Filters, page 5-3).

Downloadable IP ACLs operate this way:

1. When ACS grants a user access to the network, ACS determines whether a downloadable IP ACL is assigned to that user or the user's group.
2. If ACS locates a downloadable IP ACL that is assigned to the user or the user's group, it determines whether an ACL content entry is associated with the AAA client that sent the RADIUS authentication request.
3. ACS sends, as part of the user session, RADIUS access-accept packet an attribute specifying the named ACL and the version of the named ACL.
4. If the AAA client responds that it does not have the current version of the ACL in its cache (that is, the ACL is new or has changed), ACS sends the ACL (new or updated) to the device.

Downloadable IP ACLs are an alternative to configuring ACLs in the RADIUS Cisco **cisco-av-pair** attribute [26/9/1] of each user or user group. You can create a downloadable IP ACL once, give it a name, and then assign the downloadable IP ACL to each applicable user or user group by referencing its name. This method is more efficient than configuring the RADIUS Cisco **cisco-av-pair** attribute for each user or user group.

Further, by employing NAFs, you can apply different ACL contents to the same user or group of users, according to the AAA client that they are using. No additional configuration of the AAA client is necessary after you have configured the AAA client to use downloadable IP ACLs from ACS. Downloadable ACLs are protected by the backup or replication regimen that you have established.

While entering the ACL definitions in the ACS web interface, do not use keyword and name entries; in all other respects, use standard ACL command syntax and semantics for the AAA client on which you intend to apply the downloadable IP ACL. The ACL definitions that you enter into ACS comprise one or more ACL commands. Each ACL command must be on a separate line.

You can add one or more named ACL contents to a downloadable IP ACL. By default each ACL content applies to all AAA clients; however, if you have defined NAFs, you can limit the applicability of each ACL content to the AAA clients that are listed in the NAF that you associate to it. That is, by employing

NAFs, you can make each ACL content, within a single downloadable IP ACL, applicable to multiple different network devices or network device groups in accordance with your network security strategy. For more information on NAFs, see About Network Access Filters, page 5-3.

Also, you can change the order of the ACL contents in a downloadable IP ACL. ACS examines ACL contents starting from the top of the table and downloads the *first* ACL content that it finds with a NAF that includes the AAA client that is being used. In setting the order, you should seek to ensure system efficiency by positioning the most widely applicable ACL contents higher on the list. You should realize that, if your NAFs include overlapping populations of AAA clients, you must proceed from the more specific to the more general. For example, ACS will download any ACL contents with the **All-AAA-Clients** NAF setting and not consider any that are lower on the list.

To use a downloadable IP ACL on a particular AAA client, the AAA client must:

- Use RADIUS for authentication.
- Support downloadable IP ACLs.

Examples of Cisco devices that support downloadable IP ACLs are:

- PIX Firewalls
- VPN 3000-series concentrators, ASA and PIX devices
- Cisco devices running IOS version 12.3(8)T or greater

An example of the format that you should use to enter PIX Firewall ACLs in the ACL Definitions box is:

```
permit tcp any host 10.0.0.254
permit udp any host 10.0.0.254
permit icmp any host 10.0.0.254
permit tcp any host 10.0.0.253
```

An example of the format that you should use to enter VPN 3000/ASA/PIX 7.x+ ACLs in the **ACL Definitions** box is:

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

For detailed ACL definition information, see the command reference section of your device configuration guide.

Adding a Downloadable IP ACL

Before You Begin

You should have already configured any NAFs that you intend to use in your downloadable IP ACL.

To add a downloadable IP ACL:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Downloadable IP ACLs**.

Tip If Downloadable IP ACLs does not appear on the Shared Profile Components page, you must enable the User-Level Downloadable ACLs or Group-Level Downloadable ACLs option, or both, on the Advanced Options page of the Interface Configuration section.

Step 3 Click **Add**.

The Downloadable IP ACLs page appears.

Step 4 In the **Name** box, type the name of the new IP ACL.

Note The name of an IP ACL may contain up to 27 characters. The name must *not* contain spaces nor any of the following characters: hyphen (-), left bracket ([), right bracket (]), slash (/), backslash (\), quotes ("), left angle bracket (<), right angle bracket (>), dash (-).

Step 5 In the **Description** box, type a description of the new IP ACL. The description can be up to 30,000 characters.

Step 6 To add an ACL content to the new IP ACL, click **Add**.

Step 7 In the **Name** box, type the name of the new ACL content.

Note The name of an ACL content may contain up to 27 characters. The name must *not* contain spaces nor any of the following characters: hyphen (-), left bracket ([), right bracket (]), slash (/), backslash (\), quotes ("), left angle bracket (<), right angle bracket (>), dash (-).

Step 8 In the **ACL Definitions** box, type the new ACL definition.

Tip In entering ACL definitions in the ACS web interface, you do not use keyword and name entries; rather, you begin with a **permit** or **deny** keyword. For an example of the proper format of the ACL definitions, see About Downloadable IP ACLs, page 5-13.

Step 9 To save the ACL content, click **Submit**.

The Downloadable IP ACLs page appears with the new ACL content listed by name in the ACL Contents column.

Step 10 To associate a NAF to the ACL content, select a NAF from the Network Access Filtering box to the right of the new ACL content. For information on adding a NAF see Adding a Network Access Filter, page 5-3.

Note If you do not assign a NAF, ACS associates the ACL content to all network devices, which is the default.

Step 11 Repeat Step 3 through Step 10 until you have completely specified the new IP ACL.

Step 12 To set the order of the ACL contents, click the radio button for an ACL definition, and then click **Up** or **Down** to reposition it in the list.

Tip The order of ACL contents is significant. Working from top to bottom, ACS downloads only the *first* ACL definition that has an applicable NAF setting (including the **All-AAA-Clients** default setting if used). Typically your list of ACL contents will proceed from the one with the most specific (narrowest) NAF to the one with the most general (**All-AAA-Clients**) NAF.

Step 13 To save the IP ACL, click **Submit**.

ACS enters the new IP ACL, which takes effect immediately. For example, if the IP ACL is for use with PIX Firewalls, it is available to be sent to any PIX Firewall that is attempting authentication of a user who has that downloadable IP ACL assigned to his or her user or group profile. For information on assigning a downloadable IP ACL to user or a user group, see Assigning a Downloadable IP ACL to a User, page 7-14, or Assigning a Downloadable IP ACL to a Group, page 6-22.

Editing a Downloadable IP ACL

Before You Begin

You should have already configured any NAFs that you intend to use in your editing of the downloadable IP ACL.

To edit a downloadable IP ACL:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Downloadable IP ACLs**.

The Downloadable IP ACLs table appears.

Step 3 In the Name column, click the IP ACL that you want to edit.

The Downloadable IP ACLs page appears and displays with information for the selected ACL.

Step 4 Edit the Name or Description information, as applicable. The description can be up to 30,000 characters.

Step 5 To edit ACL content, click on the ACL Contents entry that you want to change.

The Downloadable IP ACL Content page appears.

Step 6 Edit the Name or ACL Definitions, as applicable.

Tip Do not use keyword and name entries in the ACL Definitions box; instead, begin with a permit or deny keyword. For an example of the proper format of the ACL definitions, see About Downloadable IP ACLs, page 5-13.

Step 7 To save the edited ACL definition, click **Submit**.

Step 8 To change the NAF that is associated with an ACL content, select a new NAF setting from the corresponding Network Access Filtering box. You can change as many of the NAF associations in a downloadable IP ACL as you want. For more information on NAFs, see About Network Access Filters, page 5-3.

Step 9 Repeat Step 3 through Step 8 until you are finished.

Step 10 To change the order of the ACL contents, select the radio button for an ACL definition, and then click **Up** or **Down** to reposition it in the list.

Step 11 To save the edited IP ACL, click **Submit**.

ACS saves the IP ACL with the new information, which takes effect immediately.

Deleting a Downloadable IP ACL

Before You Begin

You should remove the association of a IP ACL with any user, user group profile, or network access profile before deleting the IP ACL.

To delete an IP ACL:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Downloadable IP ACLs**.

Step 3 Click the name of the downloadable IP ACL that you want to delete.

The Downloadable IP ACLs page appears and displays information for the selected IP ACL.

Step 4 At the bottom of the page, click **Delete**.

A dialog box warns you that you are about to delete an IP ACL.

Step 5 To confirm that you want to delete the IP ACL, click **OK**.

The selected IP ACL is deleted.

Network Access Restrictions

This section describes network access restrictions (NARs), and provides detailed instructions for configuring and managing shared NARs.

This section contains the following topics:

- About Network Access Restrictions, page 5-18
- Adding a Shared NAR, page 5-20
- Editing a Shared NAR, page 5-22
- Deleting a Shared NAR, page 5-23

About Network Access Restrictions

A network access restriction (NAR) is a definition, which you make in ACS, of additional conditions that you must meet before a user can access the network. ACS applies these conditions by using information from attributes that your AAA clients sent. Although you can set up NARs in several ways, they all are based on matching attribute information that a AAA client sent. Therefore, you must understand the format and content of the attributes that your AAA clients sends if you want to employ effective NARs.

In setting up a NAR you can choose whether the filter operates positively or negatively. That is, in the NAR you specify whether to permit or deny network access, based on information sent from AAA clients when compared to the information stored in the NAR. However, if a NAR does not encounter sufficient information to operate, it defaults to denied access. Table 5-2 shows these conditions.

Table 5-2 NAR Permit or Deny Conditions

	IP-Based	Non-IP Based	Insufficient Information
Permit	Access Granted	Access Denied	Access Denied
Deny	Access Denied	Access Granted	Access Denied

ACS supports two types of NAR filters:

- **IP-based filters**—IP-based NAR filters limit access based on the IP addresses of the end-user client and the AAA client. For more information on this type of NAR filter, see About IP-based NAR Filters, page 5-19.
- **Non-IP-based filters**—Non-IP-based NAR filters limit access based on simple string comparison of a value sent from the AAA client. The value may be the calling line identification (CLI) number, the Dialed Number Identification Service (DNIS) number, the MAC address, or other value originating from the client. For this type of NAR to operate, the value in the NAR description must exactly match what is being sent from the client, including whatever format is used. For example, the telephone number (217) 555-4534 does not match 217-555-4534. For more information on this type of NAR filter, see About Non-IP-based NAR Filters, page 5-19.

You can define a NAR for, and apply it to, a specific user or user group. For more information, see Setting Network Access Restrictions for a User, page 7-8, or Setting Network Access Restrictions for a User Group, page 6-6. However, in the Shared Profile Components section of ACS you can create and name a *shared* NAR without directly citing any user or user group. You give the shared NAR a name that can be referenced in other parts of the ACS web interface. Then, when you set up users or user groups, you can select none, one, or multiple shared restrictions to be applied. When you specify the application of multiple shared NARs to a user or user group, you choose one of two access criteria:

- **All selected filters must permit**
- **Any one selected filter must permit**

You must understand the order of precedence that is related to the different types of NARs. The order of NAR filtering is:

1. Shared NAR at the user level
2. Shared NAR at the group level
3. Nonshared NAR at the user level
4. Nonshared NAR at the group level

You should also understand that denial of access at *any* level takes precedence over settings at another level that do not deny access. This is the one exception in ACS to the rule that user-level settings override group-level settings. For example, a particular user might have no NAR restrictions at the user level that apply; but, if that user belongs to a group that is restricted by a shared or nonshared NAR, the user is denied access.

Shared NARs are kept in the ACS internal database. You can use the ACS backup and restore features to back up, and restore them. You can also replicate the shared NARs, along with other configurations, to secondary ACSs.

About IP-based NAR Filters

For IP-based NAR filters, ACS uses the following attributes, depending on the AAA protocol of the authentication request:

- **If you are using TACACS+**—The `rem_addr` field from the TACACS+ start packet body is used.

  Note When an authentication request is forwarded by proxy to an ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

- **If you are using RADIUS IETF**—The `calling-station-id` (attribute 31) must be used.

Note IP-based NAR filters work only if ACS receives the Radius Calling-Station-Id (31) attribute. The Calling-Station-Id (31) must contain a valid IP address. If it does not, it will fall over to DNIS rules.

AAA clients that do not provide sufficient IP address information (for example, some types of firewall) do not support full NAR functionality.

Other attributes for **IP-based** restrictions, per protocol, include the following NAR fields:

- **If you are using TACACS+**—The NAR fields in ACS use the following values:
  - **AAA client**—The `NAS-IP-address` is taken from the source address in the socket between ACS and the TACACS+ client.
  - **Port**—The `port` field is taken from the TACACS+ start packet body.

About Non-IP-based NAR Filters

A non-IP-based NAR filter (that is, a DNIS/CLI-based NAR filter) is a list of permitted or denied calling or point of access locations that you can use in restricting a AAA client when you do not have an established IP-based connection. The non-IP-based NAR feature generally uses the CLI number and the Dialed Number Identification Service (DNIS) number.

However, by entering an IP address in place of the CLI, you can use the non-IP-based filter; even when the AAA client does not use a Cisco IOS release that supports CLI or DNIS. In another exception to entering a CLI, you can enter a MAC address to permit or deny access; for example, when you are using a Cisco Aironet AAA client. Likewise, you could enter the Cisco Aironet AP MAC address in place of the DNIS. The format of what you specify in the CLI box—CLI, IP address, or MAC address—must match the format of what you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

Attributes for DNIS/CLI-based restrictions, per protocol, include the following NAR fields:

- **If you are using TACACS+**—The NAR fields listed employ the following values:
  - **AAA client**—The `NAS-IP-address` is taken from the source address in the socket between ACS and the TACACS+ client.
  - **Port**—The `port` field in the TACACS+ start packet body is used.
  - **CLI**—The `rem-addr` field in the TACACS+ start packet body is used.
  - **DNIS**—The `rem-addr` field taken from the TACACS+ start packet body is used. In cases in which the `rem-addr` data begins with the slash (/) the DNIS field contains the `rem-addr` data without the slash (/).

Note When an authentication request is forwarded by proxy to an ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

- **If you are using RADIUS**—The NAR fields listed use the following values:
  - **AAA client**—The `NAS-IP-address` (attribute 4) or, if NAS-IP-address does not exist, `NAS-identifier` (RADIUS attribute 32) is used.
  - **Port**—The `NAS-port` (attribute 5) or, if NAS-port does not exist, `NAS-port-ID` (attribute 87) is used.
  - **CLI**—The `calling-station-ID` (attribute 31) is used.
  - **DNIS**—The `called-station-ID` (attribute 30) is used.

When specifying a NAR you can use an asterisk (*) as a wildcard for any value, or as part of any value to establish a range. All the values or conditions in a NAR description must be met for the NAR to restrict access; that is, the values contain a Boolean AND.

Adding a Shared NAR

You can create a shared NAR that contains many access restrictions. Although the ACS web interface does not enforce limits to the number of access restrictions in a shared NAR or to the length of each access restriction, you must adhere to the following limits:

- The combination of fields for each line item cannot exceed 1024 characters.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

Before You Begin

Before defining a NAR, you should be certain that you have established the elements you intend to use in that NAR. You must, therefore, have specified all NAFs and NDGs, and defined all relevant AAA clients, before making them part of the NAR definition. For more information see About Network Access Restrictions, page 5-18.

To add a shared NAR:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

Step 3 Click **Add**.

The Network Access Restriction page appears.

Step 4 In the **Name** box, type a name for the new shared NAR.

Note The name can contain up to 31 characters. Leading and trailing spaces are not allowed. Names cannot contain the following characters: left bracket ([), right bracket (]), comma (,), or slash (/).

Step 5 In the **Description** box, type a description of the new shared NAR. The description can be up to 30,000 characters.

Step 6 If you want to permit or deny access based on IP addressing:

a. Check the **Define IP-based access descriptions** check box.

b. To specify whether you are listing addresses that are permitted or denied, from the Table Defines list, select the applicable value.

c. Select or type the applicable information in each of the following boxes:

- **AAA Client**—Select **All AAA clients**, or the name of the NDG, or the NAF, or the individual AAA client, to which access is permitted or denied.
- **Port**—Type the number of the port to which you want to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.
- **Src IP Address**—Type the IP address to filter on when performing access restrictions. You can use the asterisk (*) as a wildcard to specify all IP addresses.

Note The total number of characters in the AAA Client list, and the Port and Src IP Address boxes, must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **Enter**.

The AAA client, port, and address information appear as a line item in the table.

e. To enter additional IP-based line items, repeat steps c and d.

Step 7 If you want to permit or deny access based on calling location or values other than IP addresses:

a. Select the **Define CLI/DNIS based access restrictions** check box.

b. To specify whether you are listing locations that are permitted or denied from the Table Defines list, select the applicable value.

c. To specify the clients to which this NAR applies, select one of the following values from the AAA Client list:

- The name of the NDG
- The name of the particular AAA client
- All AAA clients

Tip Only NDGs that you have already configured are listed.

d. To specify the information on which this NAR should filter, type values in the following boxes, as applicable:

Tip You can type an asterisk (*) as a wildcard to specify **all** as a value.

- **Port**—Type the number of the port on which to filter.
- **CLI**—Type the CLI number on which to filter. You can also use this box to restrict access based on values other than CLIs, such as an IP address or MAC address; for information, see About Network Access Restrictions, page 5-18.
- **DNIS**—Type the number being dialed in to on which to filter.

Note The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

e. Click **Enter**.

The information specifying the NAR line item appears in the table.

f. To enter additional non-IP-based NAR line items, repeat steps c. through e.

Step 8 To save the shared NAR definition, click **Submit**.

ACS saves the shared NAR and lists it in the **Network Access Restrictions** table.

Editing a Shared NAR

To edit a shared NAR:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

The Network Access Restrictions table appears.

Step 3 In the Name column, click the shared NAR that you want to edit.

The Network Access Restriction page appears and displays information for the selected NAR.

Step 4 Edit the Name or Description of the NAR, as applicable. The description can be up to 30,000 characters.

Step 5 To edit a line item in the IP-based access-restrictions table:

a. Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

b. Edit the information, as necessary.

Note The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and ACS cannot accurately apply it to users.

c. Click **Enter**.

The edited information for this line item is written to the IP-based access-restrictions table.

Step 6 To remove a line item from the IP-based access-restrictions table:

a. Select the line item.

b. Below the table, click **Remove**.

The line item is removed from the IP-based access-restrictions table.

Step 7 To edit a line item in the CLI/DNIS access-restrictions table:

a. Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

b. Edit the information, as necessary.

Note The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and ACS cannot accurately apply it to users.

c. Click **Enter**.

The edited information for this line item is written to the CLI/DNIS access-restrictions table.

Step 8 To remove a line item from the CLI/DNIS access-restrictions table:

a. Select the line item.

b. Below the table, click **Remove**.

The line item is removed from the CLI/DNIS access-restrictions table.

Step 9 To save the changes you have made, click **Submit**.

ACS reenters the filter with the new information, which takes effect immediately.

Deleting a Shared NAR

Before You Begin

Ensure that you remove the association of a shared NAR to any user or group before you delete that NAR.

To delete a shared NAR:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

Step 3 Click the **Name** of the shared NAR that you want to delete.

The Network Access Restriction page appears and displays information for the selected NAR.

Step 4 At the bottom of the page, click **Delete**.

A dialog box warns you that you are about to delete a shared NAR.

Step 5 To confirm that you want to delete the shared NAR, click **OK**.

The selected shared NAR is deleted.

Command Authorization Sets

This section describes command-authorization sets and pattern matching, and provides detailed instructions for configuring and managing them.

This section contains the following topics:

- About Command Authorization Sets, page 5-24
  - Command Authorization Sets Description, page 5-24
  - Command Authorization Sets Assignment, page 5-26
  - Case Sensitivity and Command Authorization, page 5-26
  - Arguments and Command Authorization, page 5-27
  - About Pattern Matching, page 5-27
- Adding a Command Authorization Set, page 5-28
- Editing a Command Authorization Set, page 5-29
- Deleting a Command Authorization Set, page 5-30

About Command Authorization Sets

This section contains the following topics:

- Command Authorization Sets Description, page 5-24
- Command Authorization Sets Assignment, page 5-26
- Case Sensitivity and Command Authorization, page 5-26
- Arguments and Command Authorization, page 5-27
- About Pattern Matching, page 5-27

Command Authorization Sets Description

Command authorization sets provide a central mechanism to control the authorization of each command that is issued on any given network device. This feature greatly enhances the scalability and manageability of setting authorization restrictions. In ACS, the default command-authorization sets

include Shell Command Authorization Sets and PIX Command Authorization Sets. Cisco device-management applications, such as Management Center for Firewalls, can instruct ACS to support additional command-authorization set types.

Note PIX Command Authorization Sets require that the TACACS+ command-authorization request identify the service as **pixshell**. Verify that this service has been implemented in the version of PIX OS that your firewalls use; if not, use Shell Command Authorization Sets to perform command authorization for PIX devices. For information, see Configuring a Shell Command Authorization Set for a User Group, page 6-24.

Tip As of PIX OS version 6.3, the pixshell service has not been implemented.

To offer more control of device-hosted, administrative Telnet sessions, a network device using TACACS+ can request authorization for each command line before its execution. You can define a set of commands that are permitted or denied for execution by a particular user on a given device. ACS has further enhanced this capability with:

- **Reusable Named Command Authorization Sets**—Without directly citing any user or user group, you can create a named set of command authorizations. You can define several command-authorization sets, each delineating different access profiles. For example:
  - A **Help desk** command-authorization set could permit access to high level browsing commands, such as **show run**, and deny any configuration commands.
  - An **All network engineers** command-authorization set could contain a limited list of permitted commands for any network engineer in the enterprise.
  - A **Local network engineers** command-authorization set could permit all commands, including IP address configuration.
- **Fine Configuration Granularity**—You can create associations between named command-authorization sets and NDGs. Thus, you can define different access profiles for users depending on which network devices they access. You can associate the same named command-authorization set with more than one NDG and use it for more than one user group. ACS enforces data integrity. Named command-authorization sets are kept in the ACS internal database. You can use the ACS Backup and Restore features to back up and restore them. You can also replicate command-authorization sets to secondary ACSs along with other configuration data.

For command-authorization set types that support Cisco device-management applications, the benefits of using command-authorization sets are similar. You can enforce authorization of various privileges in a device-management application by applying command-authorization sets to ACS groups that contain users of the device-management application. The ACS groups can correspond to different roles within the device-management application and you can apply different command-authorization sets to each group, as applicable.

ACS has three sequential stages of command-authorization filtering. Each command-authorization request is evaluated in the following order:

1. **Command Match**—ACS determines whether the command being processed matches a command listed in the command-authorization set. If no matching command is found, command-authorization is determined by the Unmatched Commands setting: permit or deny. Otherwise, if the command is matched, evaluation continues.

2. **Argument Match**—ACS determines whether the command arguments presented match the command arguments listed in the command-authorization set.
   - If any argument is unmatched, command authorization is determined by whether the Permit Unmatched Args option is enabled. If unmatched arguments are permitted, the command is authorized and evaluation ends; otherwise, the command is not authorized and evaluation ends.
   - If all arguments are matched, evaluation continues.
3. **Argument Policy**—Having determined that the arguments in the command being evaluated match the arguments listed in the command-authorization set, ACS determines whether each command argument is explicitly permitted. If all arguments are explicitly permitted, ACS grants command authorization. If any arguments is not permitted, ACS denies command authorization.

Command Authorization Sets Assignment

For information on assigning command-authorization sets, see the following procedures:

- **Shell Command Authorization Sets**—See one of the following:
  - Configuring a Shell Command Authorization Set for a User Group, page 6-24
  - Configuring a Shell Command Authorization Set for a User, page 7-17
- **PIX Command Authorization Sets**—See one of the following:
  - Configuring a PIX Command Authorization Set for a User Group, page 6-25
  - Configuring a PIX Command Authorization Set for a User, page 7-19
- **Device Management Command Authorization Sets**—See one of the following:
  - Configuring Device Management Command Authorization for a User Group, page 6-26
  - Configuring Device-Management Command Authorization for a User, page 7-20

Case Sensitivity and Command Authorization

When performing command authorization, ACS evaluates commands and arguments in a case-sensitive manner. For successful command authorization, you must configure command-authorization sets with case-sensitive commands and arguments.

As an additional complication, a device requesting command authorization might send commands and arguments by using a case different from the one you typed to issue the command.

For example, if you type the following command during a router-hosted session:

```
interface FASTETHERNET 0/1
```

the router might submit the command and arguments to ACS as:

```
interface FastEthernet 0 1
```

If, for the **interface** command, the command-authorization set explicitly permits the FastEthernet argument by using the spelling **fastethernet**, ACS fails the command-authorization request. If the command-authorization rule instead permits the argument **FastEthernet**, ACS grants the command-authorization request. The case used in command-authorization sets must match what the device sends, which might or might not match the case you use when you type the command.

Arguments and Command Authorization

When you explicitly permit or deny arguments rather than rely on ACS to permit unmatched arguments, you must make certain that you know how devices send arguments to ACS. A device requesting command authorization might send different arguments than what the user typed to issue the command.

For example, if during a router-hosted session a user typed the following command:

```
interface FastEthernet0/1
```

the router might send the following command and arguments ACS:

```
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd=interface
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=FastEthernet
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=0
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=1
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=<cr>
```

In this example, the router sees multiple arguments where the user typed one string of characters without spaces after the command. It also omits the slash (/) that separated 0 and 1 when the user issued the command.

If the command-authorization rule for the **interface** command explicitly permits the FastEthernet argument to use the spelling **FastEthernet0/1**, ACS fails the command-authorization request because it does not match what the router submitted to ACS. If the command-authorization rule instead permits the argument **FastEthernet 0 1**, ACS grants the command-authorization request. The case of arguments specified in command-authorization sets must match what the device sends, which might or might not match the case that you use when you type the arguments.

About Pattern Matching

For **permit** or **deny** command arguments, ACS applies pattern matching. That is, the argument **permit wid** matches any argument that contains the string **wid**. Thus, for example, **permit wid** would allow not only the argument **wid** but also the arguments **anywid** and **widget**.

To limit the extent of pattern matching you can add the following expressions:

- **Dollarsign ($)**—Expresses that the argument must end with what has gone before. Thus **permit wid$** would match **wid** or **anywid**, but not **widget**.
- **Caret (^)**—Expresses that the argument must begin with what follows. Thus **permit ^wid** would match **wid** or **widget**, but not **anywid**.

You can combine these expressions to specify absolute matching. In the example given, you would use **permit ^wid$** to ensure that only **wid** was permitted, and not **anywid** or **widget**.

To **permit** or **deny** commands that carry no arguments, you can use absolute matching to specify the null argument condition. For example, you use **permit ^$** to permit a command with no arguments. Alternatively, entering **permit <cr>** has the same effect. You can use either method, with the **Permit Unmatched Args** option unchecked, to match and, therefore, permit or deny commands that have no argument.

Adding a Command Authorization Set

To add a command-authorization set:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command-authorization set types that are available. These always include Shell Command Authorization Sets and may include others, such as command-authorization set types that support Cisco device-management applications.

Step 2 Click one of the listed command-authorization set types, as applicable.

The selected Command Authorization Sets table appears.

Step 3 Click **Add**.

The applicable Command Authorization Set page appears. Depending on the type of command-authorization set that you are adding, the contents of the page vary. Below the Name and Description boxes, ACS displays additional boxes or an expandable checklist tree. The expandable checklist tree appears for device command set types that support a Cisco device-management application.

Step 4 In the **Name** box, type a name for the command-authorization set.

Note The set name can contain up to 27 characters. Names cannot contain the following characters: pound sign (#), question mark (?), quotes ("), asterisk (*), right angle bracket (>), left angle bracket (<). Leading and trailing spaces are not allowed.

Step 5 In the **Description** box, type a description of the command-authorization set. The description can be up to 30,000 characters.

Step 6 If ACS displays an expandable checklist tree below the Name and Description boxes, use the checklist tree to specify the actions permitted by the command-authorization set:

a. To expand a checklist node, click the plus sign (+) to its left.

b. To enable an action, select its check box. For example, to enable a Device View action, select the **View** check box under the Device checklist node.

Tip Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.

c. To enable other actions in this command-authorization set, repeat Step a and Step b, as needed.

Step 7 If ACS displays additional boxes below the Name and Description boxes, use the boxes to specify the commands and arguments permitted or denied by the command-authorization set:

a. To specify how ACS should handle unmatched commands, select the **Permit** or **Deny** option, as applicable.

Note The default setting is **Deny**.

b. In the box just above the Add Command button, type a command that is to be part of the set.

Caution Enter the full command; if you use command abbreviations, authorization control might not function.

Note Enter only the command portion of the command/argument string here. Arguments are added only after the command is listed. For example, with the command/argument string **show run** you would type only the command **show**.

c. Click **Add Command**.

The typed command is added to the command list box.

d. To add an argument to a command, in the **Command List** box, select the command and then type the argument in the box to the right of the command.

Note The correct format for arguments is <permit | deny> <***argument***>. For example, with the command **show** already listed, you might enter **permit run** as the argument.

Tip You can list several arguments for a single command by pressing **Enter** between arguments.

e. To allow arguments, which you have not listed, to be effective with this command, select the **Permit Unmatched Args** check box.

f. To add other commands to this command-authorization set, repeat Step a through Step e.

Step 8 To save the command-authorization set, click **Submit**.

ACS displays the name and description of the new command-authorization set in the applicable Command Authorization Sets table.

Editing a Command Authorization Set

To edit a command-authorization set:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command-authorization set types available.

Step 2 Click a command-authorization set type, as applicable.

The selected Command Authorization Sets table appears.

Step 3 From the Name column, click the name of the set you want to change.

Information for the selected set appears on the applicable Command Authorization Set page.

Step 4 If an expandable checklist tree appears below the Name and Description boxes, you can do any or all of the following:

- To expand a checklist node, click the plus (+) symbol to its left. To collapse an expanded checklist node, click the minus (-) symbol to its left.

- To enable an action, select its check box. For example, to enable a Device View action, select the **View** check box under the Device checklist node.

Tip Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.

- To disable an action, uncheck its check box. For example, to disable a Device View action, uncheck the **View** check box under the Device checklist node.

Step 5 If additional boxes appear below the Name and Description boxes, you can do any or all of the following:

- To change the set Name or Description, edit the words in the corresponding box. The description can be up to 30,000 characters.
- To remove a command from the set, from the Matched Commands list, select the command, and then click **Remove Command**.
- To edit arguments of a command, from the command list box, select the command and then type changes to the arguments in the box to the right of the command list box.

Step 6 To save the set, click **Submit**.

Deleting a Command Authorization Set

To delete a command-authorization set:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command-authorization set types available.

Step 2 Click a command-authorization set type, as applicable.

The selected Command Authorization Sets table appears.

Step 3 From the Name column, click the name of the command set that you want to delete.

Information for the selected set appears on the applicable Command Authorization Set page.

Step 4 Click **Delete**.

A dialog box warns you that you are about to delete a command-authorization set.

Step 5 To confirm that you want to delete that command-authorization set, click **OK**.

ACS displays the applicable Command Authorization Sets table. The command-authorization set is no longer listed.

CHAPTER 6

User Group Management

This chapter contains information about setting up and managing user groups for authorization control in Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS. You use ACS to group network users for more efficient administration. Each user can belong to only one group in ACS. You can establish up to 500 groups for different levels of authorization.

ACS also supports external database group mapping; that is, if your external user database distinguishes user groups, you can map these groups into ACS. And if the external database does not support groups, you can map all users from that database to an ACS user group. For information about external database mapping, see Group Mapping by External User Database, page 17-1.

Caution ACS 4.0 introduces the concept of Network Access Profiles (NAPs) that affects how group authorization is performed. If you are not using NAPs, ACS functions similar to previous versions. If you do plan to use NAPs, you must understand how Remote Access Dial-in User Service (RADIUS) authorization can be split between group, user, and NAP (via RACs).

This chapter contains the following topics:

- About User Group Setup Features and Functions, page 6-2
- Basic User Group Settings, page 6-3
- Configuration-Specific User Group Settings, page 6-12
- Group Setting Management, page 6-39

Before you configure Group Setup, you should understand how this section functions. ACS dynamically builds the Group Setup section interface depending on the configuration of your network devices and the security protocols being used. That is, what you see under Group Setup is affected by settings in the Network Configuration and Interface Configuration sections. Also, you can replace any group settings for downloadable access-control lists (DACLs) and RADIUS authorization components (RACs) with the settings in the network authorization policies (NAPs). Not every setting that you add to a group may work if you perform attribute merging. For more information on attribute merging, see Understanding RACs and Groups, page 5-7.

About User Group Setup Features and Functions

The Group Setup section of the ACS web interface is the centralized location for operations regarding user group configuration and administration. For information about network device groups (NDGs), see Network Device Group Configuration, page 4-19.

This section contains the following topics:

- Default Group, page 6-2
- Group TACACS+ Settings, page 6-2
- Group RADIUS Settings, page 6-3

Default Group

If you have not configured group mapping for an external user database, ACS assigns users who are authenticated by the Unknown User Policy to the Default Group the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of ACS and kept your database information, ACS retains the group mappings that you configured before upgrading.

Group TACACS+ Settings

You can use ACS to create a full range of settings for Terminal Access Controller Access Control System (TACACS+) at the group level. If you have configured an authentication, authorization, and accounting (AAA) client to use TACACS+ as the security control protocol, you can configure standard service protocols, including Point-to-Point Protocol (PPP IP), Point-to-Point Protocol Link Control Protocol (PPP LCP), AppleTalk Remote Access Protocol (ARAP), Serial Line Internet Protocol (SLIP), and shell (exec), to apply for the authorization of each user who belongs to a particular group.

Note You can also configure TACACS+ settings at the user level. User-level settings always override group-level settings.

You can also use ACS to enter and configure new TACACS+ services. For information about how to configure a new TACACS+ service to appear on the group setup page, see Protocol Configuration Options for TACACS+, page 3-7.

If you have configured ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about ACS interaction with device-management applications, see Support for Cisco Device-Management Applications, page 1-13.

You can use the Shell Command Authorization Set feature to configure TACACS+ group settings. You use this feature to apply shell commands to a particular user group:

- Assign a shell command-authorization set, which you have already configured, for any network device.
- Assign a shell command-authorization set, which you have already configured, to particular NDGs.
- Permit or deny specific shell commands, which you define, on a per-group basis.

For more information about shell command-authorization sets, see Command Authorization Sets, page 5-24.

Group RADIUS Settings

ACS contains a full range of settings for RADIUS at the group level. If a AAA client has been configured to use RADIUS as the security control protocol, you can configure standard services, including Internet Engineering Task Force (IETF), Microsoft, and Ascend, to apply to the authorization of each user who belongs to a particular group.

Note You can also configure RADIUS settings at the user level. User-level settings always override group-level settings.

You can also use ACS to enter and configure new RADIUS services. For information about how to configure a new RADIUS service to appear on the group setup page, see Protocol Configuration Options for RADIUS, page 3-9.

IIf you decide to allow attribute merging in ACS, any RADIUS settings in all three (user, Shared Radius Authorization Component (SRAC), or group) will be overwritten by the user attributes first, then the shared RADIUS authorization component attributes, before allowing any group attributes settings.

Basic User Group Settings

This section presents the basic activities that you perform when configuring a new user group.

This section contains the following topics:

- Group Disablement, page 6-3
- Enabling VoIP Support for a User Group, page 6-4
- Setting Default Time-of-Day Access for a User Group, page 6-5
- Setting Callback Options for a User Group, page 6-5
- Setting Network Access Restrictions for a User Group, page 6-6
- Setting Max Sessions for a User Group, page 6-9
- Setting Usage Quotas for a User Group, page 6-10

Group Disablement

You perform this procedure to disable a user group and, therefore, to prevent any member of the disabled group from authenticating.

Note Group Disablement is the only setting in ACS where the setting at the group level may override the setting at the user level. If group disablement is set, all users within the disabled group are denied authentication, regardless of whether the user account is disabled. However, if a user account is disabled, it remains disabled; regardless of the status of the corresponding user group disablement setting. In other words, when group and user account disablement settings differ, ACS defaults to preventing network access.

To disable a group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, choose the group you want to disable, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 In the Group Disabled table, check the check box labeled **Members of this group will be denied access to the network**.

Step 4 To disable the group immediately, click **Submit + Restart**.

For more information, see Saving Changes to User Group Settings, page 6-41.

The group is disabled, and all members of the group are disabled.

Enabling VoIP Support for a User Group

Note If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Voice-over-IP (VoIP) Group Settings** check box.

Perform this procedure to enable support for the null password function of VoIP. This action enables users to authenticate (session or telephone call) on only the user ID (telephone number).

When you enable VoIP at the group level, all users in this group become VoIP users, and the user IDs are treated similarly to a telephone number. VoIP users must not enter passwords to authenticate.

Caution Enabling VoIP disables password authentication and most advanced settings, including password aging and protocol attributes. If a password is submitted with a VoIP user ID, ACS fails the attempt.

To enable VoIP support for a group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, choose the group that you want to configure for VoIP support, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 In the Voice-over-IP Support table, check the check box labeled **This is a Voice-over-IP (VoIP) group - and all users of this group are VoIP users**.

Step 4 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 5 To continue and specify other group settings, perform other procedures in this chapter, as applicable.

Setting Default Time-of-Day Access for a User Group

Note If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Default Time-of-Day / Day-of-Week Specification** check box.

To define the times during which users in a particular group are permitted or denied access:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 In the Default Time-of-Day Access Settings table, check the **Set as default Access Times** check box.

Note You must check the **Set as default Access Times** check box to limit access based on time or day.

Times at which the system permits access are highlighted in green on the day-and-hour matrix.

Note The default sets accessibility during all hours.

Step 4 In the day-and-hour matrix, click the times at which you do *not* want to permit access to members of this group.

Tip Clicking times of day on the graph clears those times; clicking again rechecks them. At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 5 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Callback Options for a User Group

Callback is a command string that is passed back to the access server. You can use callback strings to initiate a modem to call the user back on a specific number for added security or reversal of line charges. The three options are:

- **No callback allowed**—Disables callback for users in this group. This is the default setting.
- **Dialup client specifies callback number**—Allows the dialup client to specify the callback number. The dialup client must support RFC 1570, PPP LCP Extensions.

- **Use Windows Database callback settings (where possible)**—Uses the Microsoft Windows callback settings. If a Windows account for a user resides in a remote domain, the domain in which ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.

Note If you enable the Windows Database callback settings, the Windows Callback feature must also be enabled in the Windows Database Configuration Settings. See Windows User Database Configuration Options, page 13-18.

Note The **Password Aging** feature does not operate correctly if you also use the callback feature. When you use callback, users cannot receive password aging messages at login.

To set callback options for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 Select a group from the Group list, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 In the Callback table, select one of the following three options:

- No callback allowed.
- Dialup client specifies callback number.
- Use Windows Database callback settings (where possible).

Step 4 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 5 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Network Access Restrictions for a User Group

You use the Network Access Restrictions table in Group Setup to apply network-access restrictions (NARs) in three distinct ways:

- Apply existing shared NARs by name.
- Define IP-based group access restrictions to permit or deny access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established.
- Define CLI/DNIS-based group NARs to permit or deny access to either, or both, the calling line ID (CLI) number or the Dialed Number Identification Service (DNIS) number used.

Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see About Network Access Restrictions, page 5-18.

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can apply to more than one group or user. For more information, see Adding a Shared NAR, page 5-20. You must check the **Group-Level Shared Network Access Restriction** check box on the **Advanced Options** page of the Interface Configuration section for these options to appear in the ACS web interface.

However, you can also use ACS to define and apply a NAR for a single group from within the **Group Setup** section. You must check the **Group-Level Network Access Restriction** setting under the Advanced Options page of the Interface Configuration section for single group IP-based filter options and single group CLI/DNIS-based filter options to appear in the ACS web interface.

Note When an authentication request is forwarded by proxy to an ACS server, any NARs for RADIUS requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 To apply a previously configured shared NAR to this group:

Note To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see Adding a Shared NAR, page 5-20.

a. Check the **Only Allow network access when** check box.

b. To specify whether one or all shared NARs must apply for a member of the group to be permitted access, check one of the following options:

- All selected shared NARS result in permit
- Any one selected shared NAR results in permit

c. Select a shared NAR name in the Shared NAR list, and then click **-->** (right arrow button) to move the name into the Selected Shared NARs list.

Tip To view the server details of the shared NARs that you have applied, you can click **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

Step 4 To define and apply a NAR for this particular user group, that permits or denies access to this group based on IP address, or IP address and port:

Tip You should define most NARs from within the Shared Components section so that the restrictions can apply to more than one group or user. For more information, see Adding a Shared NAR, page 5-20.

a. In the Per Group Defined Network Access Restrictions section of the Network Access Restrictions table, check the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select **Permitted Calling/Point of Access Locations** or **Denied Calling/Point of Access Locations**.

c. Select or enter the information in the following boxes:

- **AAA Client**—Select All AAA Clients or the name of the NDG or the name of the individual AAA client to which you want to permit or deny access.
- **Port**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.
- **Address**—Type the IP address or addresses to filter on when performing access restrictions. You can use the asterisk (*) as a wildcard.

Note The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **enter**.

The specified the AAA client, port, and address information appears in the **NAR Access Control** list.

Step 5 To permit or deny access to this user group based on calling location or values other than an established IP address:

a. Check the **Define CLI/DNIS-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one:

- **Permitted Calling/Point of Access Locations**
- **Denied Calling/Point of Access Locations**

c. From the AAA Client list, choose **All AAA Clients**, or the name of the NDG or the name of the particular AAA client to which to permit or deny access.

d. Complete the following boxes:

Note You must type an entry in each box. You can use the asterisk (*) as a wildcard for all or part of a value. The format that you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **PORT**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number or all numbers.

Tip **CLI** is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet client MAC address. For more information, see About Network Access Restrictions, page 5-18.

- **DNIS**—Type the DNIS number to restrict access based on the number into which the user will be dialing. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number or all numbers.

Tip **CLI** is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet AP MAC address. For more information, see About Network Access Restrictions, page 5-18.

Note The total number of characters in the AAA Client list, and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

e. Click **enter**.

The information, that specifies the AAA client, port, CLI, and DNIS appears in the list.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Max Sessions for a User Group

Note If the **Max Sessions** feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Max Sessions** check box.

Perform this procedure to define the maximum number of sessions that are available to a group, or to each user in a group, or both. The settings are:

- **Sessions available to group**—Sets the maximum number of simultaneous connections for the entire group.
- **Sessions available to users of this group**—Sets the maximum number of total simultaneous connections for each user in this group.

Tip As an example, Sessions available to group is set to 10 and Sessions available to users of this group is set to 2. If each user is using the maximum 2 simultaneous sessions, no more than five users can log in.

A session is any type of connection that RADIUS or TACACS+ supports, such as PPP, NAS prompt, Telnet, ARAP, and IPX/SLIP.

The default setting for group Max Sessions is Unlimited for the group and the user within the group.

To configure Max Sessions settings for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 In the Max Sessions table, under Sessions available to group, select one of the following options:

- **Unlimited**—Allows this group an unlimited number of simultaneous sessions. (This action effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow this group.

Step 4 In the lower portion of the Max Sessions table, under Sessions available to users of this group, select one of the following two options:

- **Unlimited**—Allows each individual in this group an unlimited number of simultaneous sessions. (This action effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow each user in this group.

Note Settings made in User Setup override group settings. For more information, see Setting Max Sessions Options for a User, page 7-11.

Step 5 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 6 Ensure the AAA client device has accounting enabled to allow Max Sessions checks to work. If accounting is not enabled, Max Sessions will not work.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Usage Quotas for a User Group

Note If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Usage Quotas** check box.

Perform this procedure to define usage quotas for members of a group. Session quotas affect each user of a group individually, not the group collectively. You can set quotas for a given period in two ways:

- Total duration of session
- The total number of sessions

If you make no selections in the Usage Quotas section for a group, no usage quotas are enforced on users who are assigned to that group; unless you configure usage quotas for the individual users.

Note The Usage Quotas section on the Group Settings page does not show usage statistics. Usage statistics are available only on the settings page for an individual user. For more information, see Options for Setting User Usage Quotas, page 7-12.

When a user exceeds his or her assigned quota, ACS denies that user access on attempting to start a session. If a quota is exceeded during a session, ACS allows the session to continue.

You can reset the usage quota counters for all users of a group from the Group Settings page. For more information about resetting usage quota counters for a whole group, see Resetting Usage Quota Counters for a User Group, page 6-40.

Tip To support time-based quotas, we recommend enabling accounting-update packets on all AAA clients. If update packets are not enabled, the quota is updated when the user logs off. If the AAA client through which the user is accessing your network fails, the quota is not updated. In the case of multiple sessions, such as with Integrated Services Digital Network (ISDN), the quota is not updated until all sessions terminate. A second channel will, therefore, be accepted; even if the first channel has exhausted the quota for the user.

To set user usage quotas for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 To define usage quotas based on duration of sessions:

a. In the Usage Quotas table, check the **Limit each user of this group to** *x* **hours of online time** *per time unit* check box.

b. Type the number of hours to which you want to limit group members in the **to** *x* **hours** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal ten hours and 30 minutes.

Note Up to five characters are allowed in the to *x* hours box.

c. Select the period for which the quota is effective:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of hours, with no end.

Step 4 To define user session quotas based on number of sessions:

a. In the Usage Quotas table, check the **Limit each user of this group to** *x* **sessions** check box.

b. Type the number of sessions to which you want to limit users in the **to** *x* **sessions** box.

Note Up to five characters are allowed in the to *x* sessions box.

c. Select the period for which the session quota is effective:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of session, with no end.

Step 5 To save the group settings, that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuration-Specific User Group Settings

This section details procedures that you perform only as applicable to your particular network-security configuration. For instance, if you have no token server configured, you do not have to set token card settings for each group.

Note When you configure a vendor-specific variety of RADIUS for use by network devices, the RADIUS (IETF) attributes are available because they are the base set of attributes, that all RADIUS vendors use per the RADIUS IETF specifications.

The web interface content corresponding to these procedures is dynamic and its appearance is based on:

- For a particular protocol (RADIUS or TACACS+) to be listed, at least one AAA client entry in the Network Configuration section of the web interface must use that protocol. For more information, see AAA Client Configuration, page 4-7.
- For specific protocol attributes to appear on a group profile page, you must enable the display of those attributes in the Interface Configuration section of the web interface. For more information, see Protocol Configuration Options for TACACS+, page 3-7, or Protocol Configuration Options for RADIUS, page 3-9.

Caution If you are using SRACs in 4.0, you should be aware of certain issues regarding attribute merging, and overwriting DACLs and RADIUS attributes on a user or group level. You should not assign RADIUS attributes to an individual user (only as a last resort). Use group or SRACs to assign RADIUS attributes in the user's group or profile levels. For more information on how to select RAC, the authorization rules that allow you to set up your network profiles, see Configuring an Authorization Rule, page 15-44.

This section contains the following topics:

- Setting Enable Privilege Options for a User Group, page 6-13
- Setting Enable Privilege Options for a User Group, page 6-13
- Enabling Password Aging for the ACS Internal Database, page 6-15

- Enabling Password Aging for Users in Windows Databases, page 6-19
- Setting IP Address Assignment Method for a User Group, page 6-21
- Assigning a Downloadable IP ACL to a Group, page 6-22
- Configuring TACACS+ Settings for a User Group, page 6-22
- Configuring a Shell Command Authorization Set for a User Group, page 6-24
- Configuring a PIX Command Authorization Set for a User Group, page 6-25
- Configuring Device Management Command Authorization for a User Group, page 6-26
- Configuring IETF RADIUS Settings for a User Group, page 6-27
- Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group, page 6-28
- Configuring Cisco Airespace RADIUS Settings for a User Group, page 6-29
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-30
- Configuring Ascend RADIUS Settings for a User Group, page 6-32
- Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group, page 6-33
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-34
- Configuring Microsoft RADIUS Settings for a User Group, page 6-35
- Configuring Nortel RADIUS Settings for a User Group, page 6-36
- Configuring Juniper RADIUS Settings for a User Group, page 6-37
- Configuring BBSM RADIUS Settings for a User Group, page 6-38
- Configuring Custom RADIUS VSA Settings for a User Group, page 6-39

Setting Enable Privilege Options for a User Group

Note If this section does not appear, choose **Interface Configuration > TACACS+ (Cisco)**. At the bottom of the page in the Advanced Configuration Options table, check the **Advanced TACACS+ features** check box.

Perform this procedure to configure group-level TACACS+ enabling parameters. The three possible TACACS+ enable options are:

- **No Enable Privilege**—(default) Disallows enable privileges for this user group.
- **Max Privilege for Any AAA Client**—Selects the maximum privilege level for this user group for any AAA client on which this group is authorized.
- **Define max Privilege on a per-network device group basis**—Defines maximum privilege levels for an NDG. To use this option, you create a list of device groups and corresponding maximum privilege levels. See your AAA client documentation for information about privilege levels.

Note To define levels in this manner, you must have configured the option in Interface Configuration; if you have not done so already, choose **Interface Configuration > Advanced Settings**. Then, check the **Network Device Groups** check box.

If you are using NDGs, you use this option to configure the NDG for enable-level mapping; rather than having to do it for each user in the group.

To set enable privilege options for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **Enable Options**.

Step 4 Do one of the following:

- Disallow enable privileges for this user group, choose the **No Enable Privilege** option.
- Set the maximum privilege level for this user group, for any ACS on which this group is authorized. Choose:
  - **Max Privilege for Any Access Server** option
  - Maximum privilege level from the list
- Define the maximum NDG privilege level for this user group:
  - select the **Define max Privilege on a per-network device group basis** option
  - from the lists, choose the NDG and a corresponding privilege level
  - click **Add Association**

Result: The association of NDG and maximum privilege level appears in the table.

Step 5 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Token Card Settings for a User Group

Note If this section does not appear, configure a token server. Then, choose **External User Databases> Database Configuration**. Then, add the applicable token card server.

Perform this procedure to allow a token to be cached. Users, therefore, can use a second B channel without having to enter a second one-time password (OTP).

Caution This option is for use with token caching only for ISDN terminal adapters. You should fully understand token caching, and ISDN concepts and principles before implementing this option. Token caching allows you to connect to multiple B channels without having to provide a token for each channel connection. Token card settings are applied to all users in the selected group.

Options for token caching include the following:

- **Session**—You can select Session to cache the token for the entire session. This option allows the second B channel to dynamically go in and out of service.
- **Duration**—You can select Duration and specify a period of time to have the token cached (from the time of first authentication). If this time period expires, the user cannot start a second B channel.
- **Session and Duration**—You can select Session and Duration so that, if the session runs longer than the duration value, a new token is required to open a second B channel. Type a value high enough to allow the token to be cached for the entire session. If the session runs longer than the duration value, a new token is required to open a second B channel.

To set token card settings for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **Token Cards**.

Step 4 In the Token Card Settings table, to cache the token for the entire session, choose **Session**.

Step 5 Also in the Token Card Settings table, to cache the token for a specified time period (measured from the time of first authentication):

a. Choose **Duration**.

b. Type the duration length in the box.

c. Choose the unit of measure: **Seconds**, **Minutes** or **Hours**.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Enabling Password Aging for the ACS Internal Database

You use the Password Aging feature of ACS to force users to change their passwords under one or more of the following conditions:

- After a specified number of days (age-by-date rules).
- After a specified number of logins (age-by-uses rules).
- The first time a new user logs in (password change rule).

Varieties of Password Aging Supported by ACS

ACS supports four distinct password-aging mechanisms:

- **Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) Windows Password Aging**—Users must be in the Windows user database and be using a Microsoft client that supports

EAP, such as Windows XP. For information on the requirements and configuration of this password-aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-19.

- **RADIUS-based Windows Password Aging**—Users must be in the Windows user database and be using a RADIUS client/supplicant that supports changing passwords by using Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP). For information on the requirements and configuration of this password aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-19.
- **Password Aging for Device-hosted Sessions**—Users must be in the ACS internal database, the AAA client must be running TACACS+, and the connection must use Telnet. You can control the ability of users to change passwords during a device-hosted Telnet session. You can also control whether ACS propagates passwords changed by using this feature. For more information, see Local Password Management, page 8-4.
- **Password Aging for Transit Sessions**—Users must be in the ACS internal database. Users must use a PPP dialup client. Further, the end-user client must have Cisco Authentication Agent (CAA) installed.

Tip The CAA software is available at http://www.cisco.com.

Also, to run password aging for transit sessions, the AAA client can be running RADIUS or TACACS+; moreover, the AAA client must be using Cisco IOS Release 11.2.7 or later and be configured to send a watchdog accounting packet (`aaa accounting new-info update`) with the IP address of the calling station. (Watchdog packets are interim packets sent periodically during a session. They provide an approximate session length in the event that no stop packet is received to mark the end of the session.)

You can control whether ACS propagates passwords changed by using this feature. For more information, see Local Password Management, page 8-4.

ACS supports password aging by using the RADIUS protocol under MS CHAP versions 1 and 2. ACS does not support password aging over Telnet connections that use the RADIUS protocol.

Caution If a user with a RADIUS connection tries to make a Telnet connection to the AAA client during or after the password aging warning or grace period, the Change Password option does not appear, and the user account is expired.

Password Aging Feature Settings

This section details only the Password Aging for Device-hosted Sessions and Password Aging for Transit Sessions mechanisms. For information on the Windows Password Aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-19. For information on configuring local password validation options, see Local Password Management, page 8-4.

Note The Password Aging feature does not operate correctly if you also use the Callback feature. When callback is used, users cannot receive password-aging messages at login.

The Password Aging feature in ACS has the following options:

- **Apply age-by-date rules**—Configures ACS to determine password aging by date. The age-by-date rules contain the following settings:
  - **Active period**—The number of days users will be allowed to log in before being prompted to change their passwords. For example, if you enter 20, users can use their passwords for 20 days without being prompted to change them. The default Active period is 20 days.
  - **Warning period**—The number of days, after which users will be notified to change their passwords. The existing password can be used; but the ACS presents a warning indicating that the password must be changed and displays the number of days left before the password expires. For example, if you enter 5 in this box and 20 in the Active period box, users will be notified to change their passwords on the 21st through 25th days.
  - **Grace period**—The number of days for the user grace period, which allows a user to log in once to change the password. The existing password can be used one last time after the number of days specified in the active and warning period fields has been exceeded. Then, a dialog box warns the user that the account will be disabled if the password is not changed, and prompts the user to change it. Continuing with the previous examples, if you allow a 5-day grace period, a user who did not log in during the active and warning periods would be permitted to change passwords up to and including the 30th day. However, even though the grace period is set for 5 days, a user is allowed only one attempt to change the password when the password is in the grace period. ACS displays the "last chance" warning only once. If the user does not change the password, this login is still permitted, but the password expires, and the next authentication is denied. An entry is logged in the Failed-Attempts log, and the user must contact an administrator to have the account reinstated.

Note All passwords expire at midnight of the date that you enter, not the time of day at which they were set.

- **Apply age-by-uses rules**—Configures ACS to determine password aging by the number of logins. The age-by-uses rules contain the following settings:
  - **Issue warning after** *x* **logins**—The number of the login after which ACS begins prompting users to change their passwords. For example, if you enter 10, users are allowed to log in 10 times without a change-password prompt. On the 11th login, they are prompted to change their passwords.

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

  - **Require change after** *x* **logins**—The number of logins after which to notify users that they must change their passwords. If this number is set to 12, users receive prompts requesting them to change their passwords on their 11th and 12th login attempts. On the 13th login attempt, they receive a prompt telling them that they must change their passwords. If users do not change their passwords now, their accounts expire and they cannot log in. This number must be greater than the **Issue warning after** *x* **login** number.

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Apply password change rule**—Forces new users to change their passwords the first time they log in.
- **Generate greetings for successful logins**—Displays Greetings message to display whenever users log in successfully via the CAA client. The message contains the latest password information specific to this user account.

The password aging rules are not mutually exclusive; a rule is applied for each check box that is selected. For example, users can be forced to change their passwords every 20 days, and every 10 logins, and to receive warnings and grace periods accordingly.

If no options are selected, passwords never expire.

Unlike most other parameters, which have corresponding settings at the user level, password aging parameters are configured only on a group basis.

Users who fail authentication because they have not changed their passwords and have exceeded their grace periods are logged in the Failed Attempts log. The accounts expire and appear in the Accounts Disabled list.

Before You Begin

- Verify that your AAA client is running the TACACS+ or RADIUS protocol. (TACACS+ only supports password aging for device-hosted sessions.)
- Set up your AAA client to perform authentication *and* accounting using the same protocol, TACACS+ or RADIUS.
- Verify that you have configured your password validation options. For more information, see Local Password Management, page 8-4.
- Set up your AAA client to use Cisco IOS Release 11.2.7 or later and to send a watchdog accounting packet (`aaa accounting new-info update`) with the IP address of the calling station.

To set **Password Aging** rules for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **Password Aging**.

The Password Aging Rules table appears.

Step 4 To set password aging by date, check the **Apply age-by-date rules** check box and type the number of days for the following options, as applicable:

- Active period
- Warning period
- Grace period

Note Up to five characters are allowed in each field.

Step 5 To set password aging by use, check the **Apply age-by-uses rules** check box and type the number of logins for each of the following options, as applicable:

- Issue warning after *x* logins

- Require change after *x* logins

Note Up to five characters are allowed in each field.

Step 6 To force the user to change the password on the first login after an administrator has changed it, check the **Apply password change rule** check box.

Step 7 To display a Greetings message, check the **Generate greetings for successful logins** check box.

Step 8 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 9 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Enabling Password Aging for Users in Windows Databases

ACS supports three types of password aging for users in Windows databases. Both types of Windows password aging mechanisms are separate and distinct from the other ACS password aging mechanisms. For information on the requirements and settings for the password aging mechanisms that control users in the ACS internal database, see Enabling Password Aging for the ACS Internal Database, page 6-15.

Note You can run Windows Password Aging and ACS Password Aging for Transit Sessions mechanisms concurrently, provided that the users authenticate from the two different databases.

The types of password aging in Windows databases are:

- **RADIUS-based password aging**—RADIUS-based password aging depends on the RADIUS AAA protocol that you use to send and receive the password change messages. Requirements for implementing the RADIUS-based Windows password aging mechanism include the following:
  - Communication between ACS and the AAA client must be using RADIUS.
  - The AAA client must support MS CHAP password aging in addition to MS CHAP authentication.
  - Users must be in a Windows user database.
  - Users must be using the Windows RADIUS client and server that supports changing passwords by using MS-CHAP.
  - You must enable MS CHAP version 1 or MS CHAP version 2, or both, in the Windows configuration within the External User Databases section.

Tip For information on enabling MS CHAP for password changes, see Configuring a Windows External User Database, page 13-21. For information on enabling MS CHAP in System Configuration, see Global Authentication Setup, page 10-19.

- **PEAP password aging**—PEAP password aging depends on the PEAP (EAP-GTC) or PEAP (EAP-MSCHAPv2) authentication protocol to send and receive the password change messages. Requirements for implementing the PEAP Windows password aging mechanism include:
  - The AAA client must support EAP.

- Users must be in a Windows user database.
- Users must be using a Microsoft PEAP client, such as Windows XP.
- You must enable PEAP on the Global Authentication Configuration page within the System Configuration section.

Tip For information about enabling PEAP in System Configuration, see Global Authentication Setup, page 10-19.

- You must enable PEAP password changes on the Windows Authentication Configuration page within the External User Databases section.

Tip For information about enabling PEAP password changes, see Windows User Database, page 13-5.

- **EAP-FAST password aging**—If password aging occurs during phase zero of EAP-FAST, it depends on EAP-MSCHAPv2 to send and receive the password change messages. If password aging occurs during phase two of EAP-FAST, it depends on Extensible Authentication Protocol - Generic Token Card (EAP-GTC) to send and receive the password change messages. Requirements for implementing the EAP-FAST Windows password aging mechanism include:
  - The AAA client must support EAP.
  - Users must be in a Windows user database.
  - Users must be using a client that supports EAP-FAST.
  - You must enable EAP-FAST on the Global Authentication Configuration page within the System Configuration section.

Tip For information about enabling EAP-FAST in System Configuration, see Global Authentication Setup, page 10-19.

- You must enable EAP-FAST password changes on the Windows Authentication Configuration page within the External User Databases section.

Tip For information about enabling EAP-FAST password changes, see Windows User Database, page 13-5.

Users whose Windows accounts reside in remote domains (that is, not the domain within which ACS is running) can only use the Windows-based password aging if they supply their domain names.

The methods and functionality of Windows password aging differ according to the Microsoft Windows operating system that you are using, and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). Setting password aging for users in the Windows user database is only one part of the larger task of setting security policies in Windows. For comprehensive information on Windows procedures, refer to your Windows system documentation.

Setting IP Address Assignment Method for a User Group

Perform this procedure to configure the way ACS assigns IP addresses to users in the group. The four possible methods are:

- **No IP address assignment**—No IP address is assigned to this group.
- **Assigned by dialup client**—Use the IP address that is configured on the dialup client network settings for TCP/IP.
- **Assigned from AAA Client pool**—The IP address is assigned by an IP address pool that is assigned on the AAA client.
- **Assigned from AAA server pool**—The IP address is assigned by an IP address pool that is assigned on the AAA server.

To set an IP address assignment method for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, choose a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **IP Address Assignment**.

Step 4 In the IP Assignment table, select one:

- **No IP address assignment**.
- **Assigned by dialup client**.
- **Assigned from AAA Client pool**. Then, type the AAA client IP pool name.
- **Assigned from AAA pool**. Then, choose the AAA server IP pool name in the Available Pools list and click **-->** (right arrow button) to move the name into the Selected Pools list.

Note If the Selected Pools list contains more than one pool, the users in this group are assigned to the first available pool in the order listed.

Tip To change the position of a pool in the list, choose the pool name and click **Up** or **Down** until the pool is in the order that you want.

Step 5 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Assigning a Downloadable IP ACL to a Group

You use the Downloadable ACLs feature to assign an IP ACL at the group level.

Note You must have established one or more IP ACLs before attempting to assign one. For instructions on how to add a downloadable IP ACL by using the Shared Profile Components section of the ACS web interface, see Adding a Downloadable IP ACL, page 5-15.

Tip The Downloadable ACLs table does not appear if you have not enabled it. To enable the Downloadable ACLs table, choose **Interface Configuration > Advanced Options**. Then, check the **Group-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **Downloadable ACLs**.

Step 4 Under the Downloadable ACLs section, click the **Assign IP ACL** check box.

Step 5 Select an IP ACL from the list.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring TACACS+ Settings for a User Group

Perform this procedure to configure and enable the service or protocol parameters to apply to the authorization of each user who belongs to the group. For information on how to configure settings for the Shell Command Authorization Set, see Configuring a Shell Command Authorization Set for a User Group, page 6-24.

Note To display or hide additional services or protocols, choose **Interface Configuration > TACACS+ (Cisco IOS)**, and then choose or clear items in the group column, as applicable.

To configure TACACS+ settings for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

Step 4 To configure services and protocols in the TACACS+ Settings table to be authorized for the group:

a. Select one or more service or protocol check boxes (for example, PPP IP or ARAP).

b. Under each service or protocol that you selected in Step a, select attributes and then type in the corresponding values, as applicable, to further define authorization for that service or protocol.

To employ custom attributes for a particular service, you must check the **Custom attributes** check box under that service, and then specify the attribute or value in the box below the check box.

For more information about attributes, see Appendix B, "TACACS+ Attribute-Value Pairs," or your AAA client documentation.

Tip For ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. (An ACL is a list of Cisco IOS commands that you use to restrict access to or from other devices and users on the network.)

Note Leave the attribute value box blank to use the default (as defined on the AAA client).

Note You can define and download an ACL. Click **Interface Configuration > TACACS+ (Cisco IOS)**, and then select **Display a window for each service selected in which you can enter customized TACACS+ attributes**. A box opens under each service or protocol in which you can define an ACL.

Step 5 To allow all services to be permitted unless specifically listed and disabled, check the **Default (Undefined) Services** check box under the Checking this option will PERMIT all UNKNOWN Services table.

Caution The Default (Undefined) Services option is an advanced feature and should only be used by administrators who understand the security implications.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring a Shell Command Authorization Set for a User Group

Use this procedure to specify the shell command-authorization set parameters for a group. The four options are:

- **None**—No authorization for shell commands.
- **Assign a Shell Command Authorization Set for any network device**—One shell command-authorization set is assigned, and it applies to all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Associates particular shell command-authorization sets to be effective on particular NDGs.
- **Per Group Command Authorization**—Permits or denies specific Cisco IOS commands and arguments at the group level.

Note This feature requires that you have previously configured a shell command-authorization set. For detailed steps, see Adding a Command Authorization Set, page 5-28.

To specify shell command-authorization set parameters for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

Step 4 Use the vertical scrollbar to scroll to the Shell Command Authorization Set feature area.

Step 5 To prevent the application of any shell command-authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular shell command-authorization set to be effective on any configured network device:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, choose the shell command-authorization set that you want applied to this group.

Step 7 To create associations that assign a particular shell command-authorization set to be effective on a particular NDG, for each association:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and a corresponding **Command Set**.

Tip You can select a **Command Set** that will be effective for all **Device Groups**, that are not otherwise assigned, by assigning that set to the <*default*> Device Group.

c. Click **Add Association**.

The associated NDG and shell command-authorization set appear in the table.

Step 8 To define the specific Cisco IOS commands and arguments to be permitted or denied at the group level:

a. Select the **Per Group Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select **Permit** or **Deny**.

If you select Permit, users can issue all commands not specifically listed. If you select **Deny**, users can issue only those commands listed.

c. To list particular commands to be permitted or denied, check the **Command** check box and then type the name of the command, define its arguments by using standard **Permit** or **Deny** syntax, and select whether unlisted arguments should be permitted or denied.

Caution Only an administrator who is skilled with Cisco IOS commands should use this powerful, advanced feature. Correct syntax is the responsibility of the administrator. For information on how ACS uses pattern matching in command arguments, see About Pattern Matching, page 5-27.

Tip To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box that you just completed.

Configuring a PIX Command Authorization Set for a User Group

Use this procedure to specify the PIX command-authorization set parameters for a user group. The three options are:

- **None**—No authorization for PIX commands.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command-authorization set is assigned and it applies all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command-authorization sets are to be effective on particular NDGs.

Before You Begin:

- Ensure that you configure a AAA client to use TACACS+ as the security control protocol.
- On the TACACS+ (Cisco) page of Interface Configuration section, ensure that you check the PIX Shell (**pixShell**) option in the Group column.
- Be certain that you have already configured one or more PIX command-authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-28.

To specify PIX command-authorization set parameters for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

Step 4 Scroll down to the PIX Command Authorization Set feature area within the TACACS+ Settings table.

Step 5 To prevent the application of any PIX command-authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular PIX command-authorization set that is to be effective on any configured network device:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, choose the PIX command-authorization set that you want applied to this user group.

Step 7 To create associations that assign a particular PIX command-authorization set to be effective on a particular NDG, for each association:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

The associated NDG and PIX command-authorization sets appear in the table.

Note To remove or edit an existing PIX command-authorization set association, you can select the association from the list, and then click **Remove Association**.

Configuring Device Management Command Authorization for a User Group

Use this procedure to specify the device-management command-authorization set parameters for a group. Device-management command-authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use ACS for authorization. The three options are:

- **None**—No authorization is performed for commands that are issued in the applicable Cisco device-management application.
- **Assign a** *device-management application* for any network device—For the applicable device-management application, one command-authorization set is assigned and it applies to management tasks on all network devices.
- **Assign a** *device-management application* on a per Network Device Group Basis—For the applicable device-management application, you use this option to apply command-authorization sets to specific NDGs, so that it affects all management tasks on the network devices belonging to the NDG.

Note To use this feature, you must configure a command-authorization set for the applicable Cisco device-management application. For detailed steps, see Adding a Command Authorization Set, page 5-28.

To specify device-management application command-authorization for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

Step 4 Use the vertical scrollbar to scroll to the *device-management application* feature area, where *device-management application* is the name of the applicable Cisco device-management application.

Step 5 To prevent the application of any command-authorization set for the applicable device-management application, select the **None** option.

Step 6 To assign a particular command-authorization set that affects device-management application actions on any network device:

a. Select the **Assign a** *device-management application* for any network device option.

b. Then, from the list directly below that option, choose the command-authorization set that you want applied to this group.

Step 7 To create associations that assign a particular command-authorization set that affects device-management application actions on a particular NDG, for each association:

a. Select the **Assign a** *device-management application* on a per Network Device Group Basis option.

b. Select a **Device Group** and a corresponding **device-management application**.

c. Click **Add Association**.

The associated NDG and command-authorization sets appear in the table.

Configuring IETF RADIUS Settings for a User Group

These parameters appear only when the following are true. You have configured:

- A AAA client to use one of the RADIUS protocols in Network Configuration.
- Group-level RADIUS attributes on the RADIUS (IETF) page in the Interface Configuration section of the web interface.

RADIUS attributes are sent as a profile for each user from ACS to the requesting AAA client. To display or hide any of these attributes, see Protocol Configuration Options for RADIUS, page 3-9. For a list and explanation of RADIUS attributes, see Appendix C, "RADIUS Attributes." For more information about how your AAA client uses RADIUS, refer to your AAA client vendor documentation.

To configure IETF RADIUS attribute settings to apply as an authorization for each user in the current group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **RADIUS (IETF)**.

Step 4 For each IETF RADIUS attribute you must authorize the current group. Check the check box next to the attribute, and then define the authorization for the attribute in the field or fields next to it.

Step 5 To save the group settings that you have just made and apply them immediately, click **Submit + Restart**.

Tip To save your group settings and apply them later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 6 To configure the vendor-specific attributes (VSAs) for any RADIUS network device vendor that ACS supports, see the appropriate section:

- Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group, page 6-28
- Configuring Cisco Airespace RADIUS Settings for a User Group, page 6-29
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-30
- Configuring Ascend RADIUS Settings for a User Group, page 6-32
- Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group, page 6-33
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-34
- Configuring Microsoft RADIUS Settings for a User Group, page 6-35
- Configuring Nortel RADIUS Settings for a User Group, page 6-36
- Configuring Juniper RADIUS Settings for a User Group, page 6-37
- Configuring BBSM RADIUS Settings for a User Group, page 6-38

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group

The Cisco IOS/PIX 6.x RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use RADIUS (Cisco IOS/PIX 6.x) in Network Configuration.
- Group-level RADIUS (Cisco IOS/PIX 6.x) attributes in Interface Configuration: RADIUS (Cisco IOS/PIX 6.x).

Cisco IOS/PIX 6.x RADIUS represents only the Cisco VSAs. You must configure the IETF RADIUS and Cisco IOS/PIX 6.x RADIUS attributes.

Note To hide or display Cisco IOS/PIX 6.x RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have configured no AAA clients of this (vendor) type, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco IOS/PIX 6.x RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Before you configure Cisco IOS/PIX 6.x RADIUS attributes, you must configure your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 If you want to use the [009\001] `cisco-av-pair` attribute to specify authorizations, check the check box next to the attribute and then type the attribute-value pairs in the text box. Separate each attribute-value pair by pressing **Enter**.

For example, you use the current group for assigning authorizations to Network Admission Control (NAC) clients to which ACS assigns a system posture token of `Infected`, you could specify the following values for the `url-redirect`, `posture-token`, and `status-query-timeout` attributes:

```
url-redirect=http://10.1.1.1
posture-token=Infected
status-query-timeout=150
```

Step 3 If you want to use other Cisco IOS/PIX 6.x RADIUS attributes, check the corresponding check box and specify the required values in the adjacent text box.

Step 4 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 5 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Advanced Configuration Options

You use the Advanced Configuration Options section to enable the `cisco-av-pair` for authenticated port mapping.

When you enable the `cisco-av-pair` attribute, the following string is sent to the Cisco IOS/PIX device:

```
aaa:supplicant_name=username_attribute <content of User-Name attribute>
```

Note The Enable Authenticated Port `cisco-av-pair` check box is ignored when the `cisco-av-pair` has the value `aaa:supplicant_name=` configured on the User level, Group level, or both.

The `cisco-av-pair` attribute for Layer 2 802.1X Authenticated Port Mapping is supported for the Catalyst 6000 devices that are running Cat OS.

Configuring Cisco Airespace RADIUS Settings for a User Group

The Cisco Airespace RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use **RADIUS (Cisco Airespace)** in **Network Configuration**.
- Group-level **RADIUS (Cisco Airespace)** attributes in **Interface Configuration > RADIUS (Cisco-Airespace)**.

Cisco Airespace RADIUS represents only the Cisco VSAs. Interface Configuration will display IETF RADIUS and Cisco IOS/PIX 6.x RADIUS attributes. You must configure the specific attributes manually.

Note To hide or display Cisco Airespace RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA that is applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco Airespace RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that you have configured your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

ACS cannot allow for partial support of IETF; hence, adding a Cisco Airespace device (into the Network Config) will automatically enable IETF attributes just as adding a Cisco IOS device does.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco Airespace)**.

Step 5 In the Cisco Airespace RADIUS Attributes table, set the attributes to authorize for the group by checking the check box next to the attribute. Be certain to define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco Aironet RADIUS Settings for a User Group

The single Cisco Aironet RADIUS Vendor Specific Attribute (VSA), Cisco-Aironet-Session-Timeout, is a virtual VSA. It is a specialized implementation of the IETF RADIUS `Session-Timeout` attribute (27) that ACS uses only when it responds to a RADIUS request from a AAA client by using RADIUS (Cisco Aironet). You can, therefore, provide different timeout values for users accessing your network through wireless and wired access devices. By specifying a timeout value specifically for WLAN connections, you avoid the conflicts that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes).

Tip In ACS 3.3, you only enable and configure the `Cisco-Aironet-Session-Timeout` when some or all members of a group connect through wired or wireless access devices. If members of a group always connect with a Cisco Aironet Access Point (AP) or always connect only with a wired access device, you

do not need to use `Cisco-Aironet-Session-Timeout`; but you should instead configure RADIUS (IETF) attribute 27, Session-Timeout. In ACS 4.0, use a network-access profile to create a wireless-specific policy, which makes the Aironet timeout VSA obsolete. Existing configurations will not break because this VSA is supported for those configurations. RACs do not include support for this VSA.

Imagine a user group Cisco-Aironet-Session-Timeout set to 600 seconds (10 minutes) and that same user group IETF RADIUS Session-Timeout set to 3 hours. When a member of this group connects through a VPN concentrator, ACS uses three hours as the timeout value. However, if that same user connects via a Cisco Aironet AP, ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS Session-Timeout attribute. Thus, with the Cisco-Aironet-Session-Timeout attribute configured, different session timeout values can be sent depending on whether the end-user client is a wired access device or a Cisco Aironet AP.

The Cisco-Aironet-Session-Timeout VSA appears on the **Group Setup** page only when the following are true. You have configured:

- A AAA client to use **RADIUS (Cisco Aironet)** in **Network Configuration**.
- Group-level **RADIUS (Cisco Aironet)** attribute in **Interface Configuration > RADIUS (Cisco Aironet)**.

Note To hide or display the Cisco Aironet RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA that is applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients configured to use RADIUS (Cisco Aironet), the VSA settings do not appear in the group configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to apply as an authorization for each user in the current group:

Step 1 Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco Aironet)**.

Step 5 In the Cisco Aironet RADIUS Attributes table, check the **[5842\001] Cisco-Aironet-Session-Timeout** check box.

Step 6 In the **[5842\001] Cisco-Aironet-Session-Timeout** box, type the session timeout value (in seconds) that ACS is to send in the IETF RADIUS `Session-Timeout` (27) attribute when you configure the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.

For more information about the IETF RADIUS `Session-Timeout` (27) attribute, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 7 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 8 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Ascend RADIUS Settings for a User Group

The Ascend RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use RADIUS (Ascend) or RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Ascend) attributes in Interface Configuration: RADIUS (Ascend).

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting for RADIUS is `Ascend-Remote-Addr`.

Note To hide or display Ascend RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA that is applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Ascend RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that you configured your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Ascend)**.

Step 5 In the Ascend RADIUS Attributes table, determine the attributes to authorize for the group by checking the check box next to the attribute. Be certain to define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group

To control Microsoft Point-to-Point Encryption (MPPE) settings for users accessing the network through Cisco VPN 3000 concentrators, for example, use the `CVPN3000-PPTP-Encryption (VSA 20)` and `CVPN3000-L2TP-Encryption (VSA 21)` attributes. Settings for `CVPN3000-PPTP-Encryption (VSA 20)` and `CVPN3000-L2TP-Encryption (VSA 21)` override Microsoft MPPE RADIUS settings.

If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes; regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The VPN 3000/ASA/PIX v7.x+ RADIUS attribute configurations appear only if the following are true. You have configured:

- A AAA client to use RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) in Network Configuration.
- Group-level RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) attributes on the RADIUS (VPN 3000/ASA/PIX v7.x+) page of the Interface Configuration section.

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS represents only the Cisco VPN 3000/ASA/PIX v7.x+ VSAs. You must configure the IETF RADIUS and VPN 3000/ASA/PIX v7.x+ RADIUS attributes.

Note To hide or display VPN 3000/ASA/PIX v7.x+ RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable VPN 3000/ASA/PIX v7.x+VPN 3000/ASA/PIX v7.x+ RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that you configured your IETF RADIUS attributes properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 3000/ASA/PIX v7.x+)**.

Step 5 In the Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes table, determine the attributes to authorize for the group by checking the check box next to the attribute. Further define the authorization for that attribute in the field next to it.

For more information about attributes, see Appendix C, "RADIUS Attributes," or the documentation for network devices that are using RADIUS.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 5000 Concentrator RADIUS attribute configurations appear only when the following are true.You have configured:

- A network device to use RADIUS (Cisco VPN 5000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 5000) attributes on the RADIUS (Cisco VPN 5000) page of the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 5000)**.

Step 5 In the Cisco VPN 5000 Concentrator RADIUS Attributes table, choose the attributes that should be authorized for the group by checking the check box next to the attribute. Further define the authorization for each attribute in the field next to it.

For more information about attributes, see Appendix C, “RADIUS Attributes,” or the documentation for network devices that use RADIUS.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Microsoft RADIUS Settings for a User Group

Microsoft RADIUS provides VSAs that support MPPE, which encrypts PPP links. These PPP connections can be via a dial-in line or over a VPN tunnel.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, for example, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) attributes; regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only when the following are true. You have configured:

- A network device in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.
- Group-level Microsoft RADIUS attributes on the RADIUS (Microsoft) page of the Interface Configuration section.

The following ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX v7.x+
- Ascend
- Cisco Airespace

Microsoft RADIUS represents only the Microsoft VSA. You must configure the IETF RADIUS and Microsoft RADIUS attributes.

Note To hide or display Microsoft RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Microsoft RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Microsoft)**.

Step 5 In the Microsoft RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes," or the documentation for network devices by using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Nortel RADIUS Settings for a User Group

The Nortel RADIUS attribute configurations appear only when the following are true. You have configured:

- A network device in Network Configuration that uses a RADIUS protocol that supports the Nortel RADIUS VSA.
- Group-level Nortel RADIUS attributes on the RADIUS (Nortel) page of the Interface Configuration section.

Nortel RADIUS represents only the Nortel VSA. You must configure the IETF RADIUS and Nortel RADIUS attributes.

Note To hide or display Nortel RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Nortel RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Nortel)**.

Step 5 In the Nortel RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes," or the documentation for network devices that are using RADIUS.

Note ACS autogenerates the MS-CHAP-MPPE-Keys attribute value; there is no value to set in the web interface.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Juniper RADIUS Settings for a User Group

Juniper RADIUS represents only the Juniper VSA. You must configure the IETF RADIUS and Juniper RADIUS attributes.

Note To hide or display Juniper RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Juniper RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that you configured your IETF RADIUS attributes properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Juniper)**.

Step 5 In the Juniper RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes," or the documentation for network devices that are using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring BBSM RADIUS Settings for a User Group

BBSM RADIUS represents only the BBSM RADIUS VSA. You must configure the IETF RADIUS and BBSM RADIUS attributes.

Note To hide or display BBSM RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable BBSM RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that you configured your IETF RADIUS attributes properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (BBSM)**.

Step 5 In the BBSM RADIUS Attributes table, specify the attribute to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes," or the documentation for network devices that are using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Custom RADIUS VSA Settings for a User Group

User-defined, custom Radius VSA configurations appear only when all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-19.)
- You have configured a network device in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- You have configured group-level custom RADIUS attributes on the RADIUS (*Name*) page of the Interface Configuration section.

You must configure the IETF RADIUS and the custom RADIUS attributes.

To configure and enable custom RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Confirm that you configured your IETF RADIUS attributes properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-27.

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS** (*custom name*).

Step 5 In the RADIUS (*custom name*) Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes," or the documentation for network devices that are using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-41.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Group Setting Management

This section describes how to use the **Group Setup** section to perform a variety of managerial tasks.

This section contains the following topics:

- Listing Users in a User Group, page 6-40
- Resetting Usage Quota Counters for a User Group, page 6-40

- Renaming a User Group, page 6-40
- Saving Changes to User Group Settings, page 6-41

Listing Users in a User Group

To list all users in a specified group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, choose the group.

Step 3 Click **Users in Group**.

The User List page for the particular group that you selected opens in the display area.

Step 4 To open a user account (to view, modify, or delete a user), click the name of the user in the User List.

The User Setup page for the particular user account selected appears.

Resetting Usage Quota Counters for a User Group

You can reset the usage quota counters for all members of a group, before or after a quota has been exceeded.

To reset usage quota counters for all members of a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, choose the group and click **Edit Settings**.

Step 3 In the Usage Quotas section, check the **On submit reset all usage counters for all users of this group** check box.

Step 4 Click **Submit** at the bottom of the browser page.

The usage quota counters for all users in the group are reset. The Group Setup Select page appears.

Renaming a User Group

To rename a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, choose the group.

Step 3 Click **Rename Group**.

The Renaming Group: *Group Name* page appears.

Step 4 Type the new name in the **Group** field. Group names cannot contain angle brackets (< >).

Step 5 Click **Submit**.

Note The group remains in the same position in the list. The number value of the group is still associated with this group name. Some utilities, such as the database import utility, use the numeric value that is associated with the group.

The Select page opens with the new group name selected.

Saving Changes to User Group Settings

After you have completed configuration for a group, you must save your work.

To save the configuration for the current group:

Step 1 To save your changes and apply them immediately, click **Submit + Restart**. This action restarts ACS services and applies the changes.

You can click only the **Submit** button if you do not want to affect your network with a restart.

Step 2 To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

The group attributes are applied and services are restarted. The Edit page opens.

Note Restarting the service clears the Logged-in User Report and temporarily interrupts all ACS services. This action affects the Max Sessions counter.

Step 3 To verify that your changes were applied, choose the group and click **Edit Settings**. View the settings.

User Management

This chapter contains information about setting up and managing user accounts in Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains the following topics:

- About User Setup Features and Functions, page 7-1
- About User Databases, page 7-2
- Basic User Setup Options, page 7-2
- Advanced User Authentication Settings, page 7-15
- User Management, page 7-36

Caution Settings at the user level override settings that you configured at the group level.

Before you configure User Setup, you should understand how this section functions. ACS dynamically builds the User Setup section interface depending on the configuration of your Authentication, Authorization, and Accounting (AAA) client and the security protocols that you use. That is, what you see under User Setup is affected by settings in the Network Configuration and Interface Configuration sections.

About User Setup Features and Functions

The User Setup section of the ACS web interface is the centralized location for all operations regarding user account configuration and administration.

From within the User Setup section, you can:

- View a list of all users in the ACS internal database.
- Find a user.
- Add a user.
- Assign the user to a group, including Voice-over-IP (VoIP) groups.
- Edit user account information.
- Establish or change user authentication type.
- Configure callback information for the user.
- Set network-access restrictions (NARs) for the user.

- Configure Advanced Settings.
- Set the maximum number of concurrent sessions (Max Sessions) for the user.
- Disable or reenable the user account.
- Delete the user.

About User Databases

ACS authenticates users against one of several possible databases, including its ACS internal database. Regardless of which database that you configure ACS to use when authenticating a user, all users have accounts within the ACS internal database, and authorization of users is always performed against the user records in the ACS internal database. The following list details the basic user databases that are used and provides links to greater details on each:

- **ACS internal database**—Authenticates a user from the local ACS internal database. For more information, see ACS Internal Database, page 13-1.

Tip The following authentication types appear in the web interface only when the corresponding external user database has been configured in the Database Configuration area of the External User Databases section.

- **Windows Database**—Authenticates a user with an existing account in the Windows user database in the local domain or in domains that you configure in the Windows user database. For more information, see Windows User Database, page 13-5.
- **Generic LDAP**—Authenticates a user from a Generic Lightweight Directory Access Protocol (LDAP) external user database (including Network. Directory Services (NDS) users). For more information, see Generic LDAP, page 13-22.
- **ODBC Database**—Authenticates a user from an Open Database Connectivity-compliant database server. For more information, see ODBC Database, page 13-34.
- **LEAP Proxy RADIUS Server Database**—Authenticates a user from a Lightweight and Efficient Application Protocol (LEAP) Proxy Remote Access Dial-In User Service (RADIUS) server. For more information, see LEAP Proxy RADIUS Server Database, page 13-46.
- **Token Server**—Authenticates a user from a token server database. ACS supports the use of a variety of token servers for the increased security that one-time passwords provide. For more information, see Token Server User Databases, page 13-48.

Basic User Setup Options

This section presents the basic tasks that you perform when configuring a new user. At its most basic level, configuring a new user requires only three steps:

Step 1 Specify a name.

Step 2 Specify an external user database or a password.

Step 3 Submit the information.

The steps for editing user account settings are nearly identical to those used when adding a user account; but, to edit, you navigate directly to the field or fields to change. You cannot edit the name that is associated with a user account. To change a username, you must delete the user account and establish another.

What other procedures that you perform when setting up new user accounts is a function of the complexity of your network and of the granularity of control that you want.

This section contains the following topics:

- Adding a Basic User Account, page 7-3
- Setting Supplementary User Information, page 7-4
- Setting a Separate CHAP/MS-CHAP/ARAP Password, page 7-5
- Assigning a User to a Group, page 7-5
- Setting the User Callback Option, page 7-6
- Assigning a User to a Client IP Address, page 7-7
- Setting Network Access Restrictions for a User, page 7-8
- Setting Max Sessions Options for a User, page 7-11
- Options for Setting User Usage Quotas, page 7-12
- Setting Options for User Account Disablement, page 7-13
- Assigning a Downloadable IP ACL to a User, page 7-14

Adding a Basic User Account

This procedure details the minimum steps necessary to add a new user account to the ACS internal database.

To add a user account:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 Type a name in the **User** box.

Note The username can contain up to 64 characters. Names cannot contain the pound sign (#), the question mark (?), the quote ("), the asterisk (*), the right angle bracket (>), or the left angle bracket (<). Leading and trailing spaces are not allowed.

Step 3 Click **Add/Edit**.

The User Setup Edit page opens. The username that you are adding appears at the top of the page.

Step 4 Ensure that you uncheck the **Account Disabled** check box.

Note Alternatively, you can check the **Account Disabled** check box to create a user account that is disabled, and enable the account at another time.

Step 5 Under Password Authentication in the User Setup table, select the applicable authentication type from the list.

Tip The authentication types that appear reflect the databases that you have configured in the Database Configuration area of the External User Databases section.

Step 6 Enter a single ACS Password Authentication Protocol (PAP) password by typing it in the first set of **Password** and **Confirm Password** boxes.

Note Up to 32 characters are allowed each for the **Password** box and the **Confirm Password** box.

Tip The ACS PAP password is also used for CHAP/MS-CHAP/ARAP if you do not check the **Separate CHAP/MS-CHAP/ARAP** check box.

Tip You can configure the AAA client to ask for a PAP password first and then a Challenge Authentication Handshake Protocol (CHAP) or Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP) password; so that, when users dial in by using a PAP password, they will authenticate. For example, the following line in the AAA client configuration file causes the AAA client to enable CHAP after PAP: **ppp authentication pap chap**

Step 7 Do one:

- Finish configuring the user account options and establish the user account, click **Submit**.
- Continue to specify the user account options, perform other procedures in this chapter, as applicable.

Tip For lengthy account configurations, you can click **Submit** before continuing. This action will prevent loss of information that you already entered if an unforeseen problem occurs.

Setting Supplementary User Information

Supplementary User Information can contain up to five fields that you configure. The default configuration includes two fields: Real Name and Description.

For information about how to display and configure these optional fields, see User Data Configuration Options, page 3-4.

To enter optional information into the Supplementary User Information table:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Complete each box that appears in the Supplementary User Info table.

Note Up to 128 characters are allowed each for the **Real Name** and the **Description** boxes.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Setting a Separate CHAP/MS-CHAP/ARAP Password

Setting a separate CHAP/MS-CHAP/ARAP password adds more security to ACS authentication. However, you must have an AAA client configured to support the separate password.

To allow the user to authenticate by using a CHAP, MS-CHAP, or AppleTalk Remote Access Protocol (ARAP) password, instead of the PAP password in the ACS internal database:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Select the **Separate CHAP/MS-CHAP/ARAP** check box in the User Setup table.

Step 3 Enter the CHAP/MS-CHAP/ARAP password to use by typing it in each of the second set of **Password** or **Confirm** boxes under the **Separate (CHAP/MS-CHAP/ARAP)** check box.

Note Up to 32 characters are allowed each for the **Password** box and the **Confirm Password** box.

Note These **Password** and **Confirm Password** boxes are only required for authentication by the ACS database. Additionally, if you assign a user to a VoIP (null password) group, and the optional password is also included in the user profile, the password is not used until the user is remapped to a non-VoIP group.

Step 4 Do one:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Assigning a User to a Group

A user can only belong to one group in ACS. The user inherits the attributes and operations that are assigned to his or her group. However, in the case of conflicting settings, the settings at the user level override the settings that you configure at the group level.

By default, users are assigned to the Default Group. Users who authenticate via the Unknown User method and who are not mapped to an existing ACS group are also assigned to the Default Group.

Alternatively, you can choose not to map a user to a particular group; but instead, to have the group mapped by an external authenticator. For external user databases from which ACS can derive group information, you can associate the group memberships—defined for the users in the external user database—to specific ACS groups. For more information, see Chapter 17, "About User Group Mapping and Specification."

To assign a user to a group:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 From the Group to which user is assigned list in the User Setup table, select the group to which to assign the user.

Tip Alternatively, you can scroll up in the list to select the **Mapped By External Authenticator** option.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Setting the User Callback Option

Callback is a command string that is passed to the access server. You can use a callback string to initiate a modem to call the user back on a specific number for added security or reversal of line charges.

To set the user callback option:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Under Callback in the User Setup table, select the applicable option. Choices include:

- **Use group setting**—Click if you want this user to use the setting for the group.
- **No callback allowed**—Click to disable callback for this user.
- **Callback using this number**—Click and type the complete number, including area code if necessary, on which to always call back this user.

  Note The maximum length for the callback number is 199 characters.

- **Dialup client specifies callback number**—Click to enable the Windows dialup client to specify the callback number.
- **Use Windows Database callback settings**—Click to use the settings specified for Windows callback. If a Windows account for a user resides in a remote domain, the domain in which ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.

Note The dial-in user must have configured Windows software that supports callback.

Note If you enable the Windows Database callback settings, the Windows Callback feature must also be enabled in the Windows Database Configuration Settings. See Windows User Database Configuration Options, page 13-18.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Assigning a User to a Client IP Address

To assign a user to a client IP address:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Under **Client IP Address Assignment** in the User Setup table, select the applicable option. Choices include:

Note The IP address assignment in User Setup overrides the IP address assignment in Group Setup.

- **Use group settings**—Click this option to use the IP address group assignment.
- **No IP address assignment**—Click this option to override the group setting if you do not want an IP address returned by the client.
- **Assigned by dialup client**—Click this option to use the IP address dialup client assignment.
- **Assign static IP address**—Click this option and type the IP address in the box (up to 15 characters), if a specific IP address should be used for this user.

  Note If the IP address is being assigned from a pool of IP addresses or by the dialup client, leave the **Assign static IP address** box blank.

- **Assigned by AAA client pool**—Click this option and type the AAA client IP pool name in the box, if this user is to have the IP address assigned by an IP address pool that is configured on the AAA client.
- **Assigned from AAA pool**—Click this option and type the applicable pool name in the box, if this user is to have the IP address that is assigned by an IP address pool configured on the AAA server. Select the AAA server IP pool name from the **Available Pools** list, and then click **-->** (right arrow button) to move the name into the **Selected Pools** list. If the **Selected Pools** list contains more than one pool, the users in this group are assigned to the first available pool in the order listed. To move the position of a pool in the list, select the pool name, and click **Up** or **Down** until the pool is in the position that you want.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Network Access Restrictions for a User

You use the Network Access Restrictions table in the Advanced Settings area of User Setup to set NARs in three ways:

- Apply existing shared NARs by name.
- Define IP-based access restrictions to permit or deny user access to a specified AAA client or to specified ports on an AAA client when an IP connection has been established.
- Define calling line ID/Dialed Number Identification Service (CLI/DNIS)-based access restrictions to permit or deny user access based on the CLI/DNIS that is used.

Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see Network Access Restrictions, page 5-17.

Typically, you define (shared) NARs from within the Shared Components section so that you can apply these restrictions to more than one group or user. For more information, see Adding a Shared NAR, page 5-20. You must have selected the **User-Level Network Access Restrictions** check box on the Advanced Options page of the Interface Configuration section for this set of options to appear in the web interface.

However, you can also use ACS to define and apply a NAR for a single user from within the User Setup section. You must have enabled the **User-Level Network Access Restrictions** setting on the Advanced Options page of the Interface Configuration section for single user IP-based filter options and single user CLI/DNIS-based filter options to appear in the web interface.

Note When an authentication request is forwarded by proxy to an ACS, any NARs for Terminal Access Controller Access Control System (TACACS+) requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

When you create access restrictions on a per-user basis, ACS does not enforce limits to the number of access restrictions nor does it enforce a limit to the length of each access restriction; however, there are strict limits:

- The combination of fields for each line item cannot exceed 1024 characters in length.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

To set NARs for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 To apply a previously configured shared NAR to this user:

Note To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see Adding a Shared NAR, page 5-20.

a. Check the **Only Allow network access when** check box.

b. To specify whether one or all shared NARs must apply for the user to be permitted access, select one, as applicable:

   – All selected NARS result in permit.

   – Any one selected NAR results in permit.

c. Select a shared NAR name in the NARs list, and then click **-->** (right arrow button) to move the name into the Selected NARs list.

Tip To view the server details of the shared NARs you have selected to apply, you can click **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

Step 3 To define and apply a NAR, for this particular user, that permits or denies this user access based on IP address, or IP address and port:

Tip You should define most NARs from within the Shared Components section so that you can apply them to more than one group or user. For more information, see Adding a Shared NAR, page 5-20.

a. In the Network Access Restrictions table, under Per User Defined Network Access Restrictions, check the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select one:

   – **Permitted Calling/Point of Access Locations**

   – **Denied Calling/Point of Access Locations**

c. Select or enter the information in the following boxes:

   – **AAA Client**—Select **All AAA Clients**, or the name of a network device group (NDG), or the name of the individual AAA client, to which to permit or deny access.

   – **Port**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.

   – **Address**—Type the IP address or addresses to use when performing access restrictions. You can use the asterisk (*) as a wildcard.

Note The total number of characters in the AAA Client list, and the Port and Src IP Address boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **Enter**.

The specified AAA client, port, and address information appears in the table above the AAA Client list.

Step 4 To permit or deny this user access based on calling location or values other than an established IP address:

a. Check the **Define CLI/DNIS based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one:

- **Permitted Calling/Point of Access Locations**
- **Denied Calling/Point of Access Locations**

c. Complete the following boxes:

Note You must make an entry in each box. You can use the asterisk (*) as a wildcard for all or part of a value. The format that you use must match the format of the string that you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **AAA Client**—Select **All AAA Clients**, or the name of the NDG, or the name of the individual AAA client, to which to permit or deny access.
- **PORT**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.

Tip Use the CLI entry if you want to restrict access based on other values such as a Cisco Aironet client MAC address. For more information, see About Network Access Restrictions, page 5-18.

- **DNIS**—Type the DNIS number to which to permit or deny access. Use this entry to restrict access based on the number into which the user will be dialing. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.

Tip Use the DNIS selection if you want to restrict access based on other values such as a Cisco Aironet AP MAC address. For more information, see About Network Access Restrictions, page 5-18.

Note The total number of characters in the AAA Client list and the **Port**, **CLI**, and **DNIS** boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **enter**.

The information, specifying the AAA client, port, CLI, and DNIS, appears in the table above the AAA Client list.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Max Sessions Options for a User

You use the Max Sessions feature to set the maximum number of simultaneous connections permitted for this user. For ACS purposes, a session is considered any type of user connection RADIUS or TACACS+ supports, for example Point-to-Point Protocol (PPP), or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for ACS to be aware of a session. All session counts are based on user and group names only. ACS does not support any differentiation by type of session—all sessions are counted as the same. To illustrate, a user with a Max Session count of 1 who is dialed in to an AAA client with a PPP session will be refused a connection if that user then tries to Telnet to a location whose access is controlled by the same ACS.

Note Each ACS holds its own Max Sessions counts. There is no mechanism for ACS to share Max Sessions counts across multiple ACSs. Therefore, if two ACSs are set up as a mirror pair with the workload distributed between them, they will have completely independent views of the Max Sessions totals.

Tip If the Max Sessions table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Max Sessions** check box.

To set max sessions options for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 In the Max Sessions table, under Sessions available to user, select one:

- **Unlimited**—Select to allow this user an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- ***n***—Select and then type the maximum number of simultaneous sessions to allow this user.
- **Use group setting**—Select to use the Max Sessions value for the group.

Note The default setting is Use group setting.

Note User Max Sessions settings override the group Max Sessions settings. For example, if the group Sales has a Max Sessions value of only 10, but a user in the group Sales, John, has a User Max Sessions value of Unlimited, John is still allowed an unlimited number of sessions.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Options for Setting User Usage Quotas

You can define usage quotas for individual users. You can limit users by the:

- Duration of sessions for the period selected.
- Number of sessions for the period selected.

For ACS purposes, a session is considered any type of user connection the RADIUS or TACACS+ supports, for example PPP, or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for ACS to be aware of a session. If you make no selections in the Session Quotas section for an individual user, ACS applies the session quotas of the group to which the user is assigned.

Note If the User Usage Quotas feature does not appear, choose **Interface Configuration > Advanced Options**. Then check the **Usage Quotas** check box.

Tip The Current Usage table under the User Usage Quotas table on the User Setup Edit page displays usage statistics for the current user. The Current Usage table lists online time and sessions used by the user, with columns for daily, weekly, monthly, and total usage. The Current Usage table appears only on user accounts that you have established; that is, it does not appear during initial user setup.

For a user who has exceeded his quota, ACS denies him access on his next attempt to start a session. If a quota is exceeded during a session, ACS allows the session to continue. If a user account has been disabled because the user has exceeded usage quotas, the User Setup Edit page displays a message stating that the account has been disabled for this reason.

You can reset the session quota counters on the User Setup page for a user. For more information about resetting usage quota counters, see Resetting User Session Quota Counters, page 7-39.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off. If the AAA client through which the user is accessing your network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate, which means that a second channel will be accepted; even if the first channel has exhausted the quota that is allocated to the user.

To set usage quota options for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 In the Usage Quotas table, select **Use these settings**.

Step 3 To define a usage quota based on duration of sessions for a user:

a. Check the **Limit user to** *x* **hours of online time** check box.

b. Type the number of hours to which you want to limit the user in the **Limit user to *x* hours of online time** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal 10 hours and 30 minutes.

Note This field can contain up to 10 characters.

c. Select the period for which you want to enforce the time usage quota:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Absolute**—A continuous, open-ended count of hours.

Step 4 To define usage quotas based on the number of sessions for a user:

a. Check the **Limit user to *x* sessions** check box.

b. Type the number of sessions to which you want to limit the user in the **Limit user to *x* sessions** box.

Note Up to 10 characters are allowed for this field.

c. Select the period for which you want to enforce the session usage quota:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Absolute**—A continuous, open-ended count of hours.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Options for User Account Disablement

The Account Disable feature defines the circumstances under which a user account is disabled.

Note Do not confuse this feature with account expiration due to password aging. Password aging is defined for groups only, not for individual users. This feature is distinct from the **Account Disabled** check box. For instructions on how to disable a user account, see Disabling a User Account, page 7-38.

Note If the user is authenticated with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings configured in Windows.

To set options for user account disablement:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Do one:

a. Select the **Never** option to keep the user account always enabled.

Note This is the default setting.

b. Select the **Disable account if** option to disable the account under specific circumstances. Then, specify one or both of the circumstances under the following boxes:

- **Date exceeds**—Check the **Date exceeds** check box. Then select the month and type the date (two characters) and year (four characters) on which to disable the account.

Note The default is 30 days after the user is added.

- **Failed attempts exceed**—Check the **Failed attempts exceed** check box and then type the number of consecutive unsuccessful login attempts to allow before disabling the account.

Note The default is 5.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Assigning a Downloadable IP ACL to a User

You can use the Downloadable ACLs feature to assign an IP Access Control List (ACL) at the user level. You must configure one or more IP ACLs before you assign one. For instructions on how to configure a downloadable IP ACL by using the Shared Profile Components section of the ACS web interface, see Adding a Downloadable IP ACL, page 5-15.

Note The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration > Advanced Options**, and then check the **User-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a user account:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username being added and edited is at the top of the page.

Step 2 Under the Downloadable ACLs section, click the **Assign IP ACL:** check box.

Step 3 Select an IP ACL from the list.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Advanced User Authentication Settings

This section presents the activities that you perform to configure user-level TACACS+ and RADIUS enable parameters.

This section contains the following topics:

- TACACS+ Settings (User), page 7-16
  - Configuring TACACS+ Settings for a User, page 7-16
  - Configuring a Shell Command Authorization Set for a User, page 7-17
  - Configuring a PIX Command Authorization Set for a User, page 7-19
  - Configuring Device-Management Command Authorization for a User, page 7-20
  - Configuring the Unknown Service Setting for a User, page 7-21
- Advanced TACACS+ Settings for a User, page 7-22
  - Setting Enable Privilege Options for a User, page 7-22
  - Setting TACACS+ Enable Password Options for a User, page 7-23
  - Setting TACACS+ Outbound Password for a User, page 7-24
- RADIUS Attributes, page 7-24
  - Setting IETF RADIUS Parameters for a User, page 7-25
  - Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User, page 7-26
  - Setting Cisco Airespace RADIUS Parameters for a User, page 7-27
  - Setting Cisco Aironet RADIUS Parameters for a User, page 7-28
  - Setting Ascend RADIUS Parameters for a User, page 7-29
  - Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User, page 7-30
  - Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 7-31
  - Setting Microsoft RADIUS Parameters for a User, page 7-32
  - Setting Nortel RADIUS Parameters for a User, page 7-33
  - Setting Juniper RADIUS Parameters for a User, page 7-34
  - Setting BBSM RADIUS Parameters for a User, page 7-35
  - Setting Custom RADIUS Attributes for a User, page 7-35

TACACS+ Settings (User)

You can use TACACS+ Settings section to enable and configure the service and protocol parameters to apply for the authorization of a user.

This section contains the following topics:

- Configuring TACACS+ Settings for a User, page 7-16
- Configuring a Shell Command Authorization Set for a User, page 7-17
- Configuring a PIX Command Authorization Set for a User, page 7-19
- Configuring Device-Management Command Authorization for a User, page 7-20
- Configuring the Unknown Service Setting for a User, page 7-21

Configuring TACACS+ Settings for a User

You can use this procedure to configure TACACS+ settings at the user level for the following services and protocols:

- PPP IP
- PPP IPX
- PPP Multilink
- PPP Apple Talk
- PPP VPDN
- PPP LCP
- ARAP
- Shell (exec)
- Project Information Exchange (PIX) PIX Shell (pixShell)
- Serial Line Internet Protocol (SLIP)

You can also enable any *new* TACACS+ services that you configure. Because having all service/protocol settings appear within the User Setup section would be cumbersome, you choose what settings to hide or display at the user level when you configure the interface. For more information about setting up new or existing TACACS+ services in the ACS web interface, see Protocol Configuration Options for TACACS+, page 3-7.

If you have configured ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about ACS interaction with device-management applications, see Support for Cisco Device-Management Applications, page 1-13.

For more information about attributes, see Appendix B, "TACACS+ AV Pairs," or your AAA client documentation. For information on assigning an IP ACL, see Assigning a Downloadable IP ACL to a User, page 7-14.

Before You Begin

- For the TACACS+ service/protocol configuration to appear, you must configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.

To configure TACACS+ settings for a user:

Step 1 Click **Interface Configuration > TACACS+ (Cisco IOS)**. In the TACACS+ Services table, under the heading User, ensure that the check box is selected for each service/protocol that you want to configure.

Step 2 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 3 Scroll down to the TACACS+ Settings table and select the bold service name check box to enable that protocol; for example **PPP IP**.

Step 4 To enable specific parameters within the selected service, Check the check box next to a specific parameter and then do one of the following, as applicable:

- Check the **Enabled** check box.
- Enter a value in the corresponding attribute box.

  To specify ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. Leave the box blank if the default (as defined on the AAA client) should be used. For more information about attributes, see Appendix B, "TACACS+ AV Pairs," or your AAA client documentation. For information on assigning a IP ACL, see Assigning a Downloadable IP ACL to a User, page 7-14.

Tip An ACL is a list of Cisco IOS commands that you use to restrict access to or from other devices and users on the network.

Step 5 To employ custom attributes for a particular service, check the **Custom attributes** check box under that service, and then enter the attribute and value in the box below the check box.

Step 6 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 7 If you are finished configuring the user account options, click **Submit** to record the options.

Configuring a Shell Command Authorization Set for a User

Use this procedure to specify the shell command-authorization set parameters for a user. You can choose:

- **None**—No authorization for shell commands.
- **Group**—The group-level shell command-authorization set applies for this user.
- **Assign a Shell Command Authorization Set for any network device**—One shell command-authorization set is assigned, and it applies all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Particular shell command-authorization sets will be effective on particular NDGs. When you select this option, you create the table that lists what NDG associates with what shell command-authorization set.
- **Per User Command Authorization**—Permits or denies specific Cisco IOS commands and arguments at the user level.

Before You Begin

- Ensure that you configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, ensure that the Shell (exec) option is selected in the User column.
- Ensure that you have already configured one or more shell command-authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-28.

To specify shell command-authorization set parameters for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Scroll down to the TACACS+ Settings table and to the Shell Command Authorization Set feature area within it.

Step 3 To prevent the application of any shell command-authorization set, click (or accept the default of) the **None** option.

Step 4 To assign the shell command-authorization set at the group level, select the **As Group** option.

Step 5 To assign a particular shell command-authorization set to be effective on any configured network device:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, select the shell command-authorization set that you want to apply to this user.

Step 6 To create associations that assign a particular shell command-authorization set to be effective on a particular NDG, for each association:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

Tip You can also select which command set applies to network device groups that are not listed simply by associating that command set with the NDG <*default*> listing.

The NDG or NDGs and associated shell command-authorization set or sets are paired in the table.

Step 7 To define the specific Cisco IOS commands and arguments to permit or deny for this user:

Caution This step configures a powerful, advanced feature. Only an administrator who is skilled with Cisco IOS commands should use this feature. Correct syntax is the responsibility of the administrator. For information on how ACS uses pattern matching in command arguments, see About Pattern Matching, page 5-27.

a. Select the **Per User Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select **Permit** or **Deny**.

If you select **Permit**, the user can issue all commands that are not specifically listed. If you select **Deny**, the user can issue only those commands that are listed.h

c. To list particular commands to permit or deny, check the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments are to be permitted or denied.

Tip To enter several commands, you must click **Submit** after entering a command. A new command entry box appears below the box that you just completed.

Step 8 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 9 If you are finished configuring the user account options, click **Submit** to record the options.

Configuring a PIX Command Authorization Set for a User

Use this procedure to specify the PIX command-authorization set parameters for a user. The four options are:

- **None**—No authorization for PIX commands.
- **Group**—The group-level PIX command-authorization set applies for this user.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command-authorization set is assigned, and it applies to all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command-authorization sets will be effective on particular NDGs.

Before You Begin

- Ensure that you configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In **Interface Configuration > TACACS+ (Cisco)**, ensure that the **PIX Shell (pixShell)** option is selected in the User column.
- Ensure that you have configured one or more PIX command-authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-28.

To specify PIX command-authorization set parameters for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Scroll down to the TACACS+ Settings table and to the PIX Command Authorization Set feature area within it.

Step 3 To prevent the application of any PIX command-authorization set, select (or accept the default of) the **None** option.

Step 4 To assign the PIX command-authorization set at the group level, select the **As Group** option.

Step 5 To assign a particular PIX command-authorization set to be effective on any configured network device:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, select the PIX command-authorization set that you want to apply to this user.

Step 6 To create associations that assign a particular PIX command-authorization set to be effective on a particular NDG, for each association:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

The associated NDG and PIX command-authorization sets appear in the table.

Step 7 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 8 If you are finished configuring the user account options, click **Submit** to record the options.

Configuring Device-Management Command Authorization for a User

Use this procedure to specify the device-management command-authorization set parameters for a user. Device-management command-authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use ACS for authorization. You can choose:

- **None**—No authorization is performed for commands that are issued in the applicable Cisco device-management application.
- **Group**—For this user, the group-level command-authorization set applies for the applicable device-management application.
- **Assign a** <*device-management application*> for any network device—For the applicable device-management application, one command-authorization set is assigned, and it applies to management tasks on all network devices.
- **Assign a** <*device-management application*> on a per Network Device Group Basis—For the applicable device-management application, you use this option to apply command-authorization sets to specific NDGs, so that it affects all management tasks on the network devices that belong to the NDG.

Before You Begin

- Ensure that an AAA client is configured to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In **Interface Configuration > TACACS+ (Cisco)**, ensure that the new TACACS+ service corresponding to the applicable device-management application is selected under **New Services** in the User column.
- If you want to apply command-authorization sets, be certain that you have configured one or more device-management command-authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-28.

To specify device-management application command authorization for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Scroll down to the TACACS+ Settings table and to the applicable device-management command-authorization feature area within it.

Step 3 To prevent the application of any command authorization for actions that are performed in the applicable device-management application, select (or accept the default of) the **None** option.

Step 4 To assign command authorization for the applicable device-management application at the group level, select the **As Group** option.

Step 5 To assign a particular command-authorization set that affects device-management application actions on any network device:

a. Select the **Assign a** <*device-management application*> for any network device option.

b. Then, from the list directly below that option, select the command-authorization set that you want to apply to this user.

Step 6 To create associations that assign a particular command-authorization set that affects device-management application actions on a particular NDG, for each association:

a. Select the **Assign a** <*device-management application*> on a per Network Device Group Basis option.

b. Select a **Device Group** and an associated <*device-management application*>.

c. Click **Add Association**.

The associated NDG and command-authorization sets appear in the table.

Step 7 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 8 If you are finished configuring the user account options, click **Submit** to record the options.

Configuring the Unknown Service Setting for a User

If you want TACACS+ AAA clients to permit unknown services, you can check the Default (Undefined) Services check box. Checking this option will PERMIT all UNKNOWN Services.

To configure the Unknown Service setting for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Scroll down to the table under the heading PERMIT all UNKNOWN Services.

Step 3 To allow TACACS+ AAA clients to permit unknown services for this user, select the **Default (Undefined) Services** check box.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Advanced TACACS+ Settings for a User

The information in this section applies when you have configured an AAA client with TACACS+.

Tip If the Advanced TACACS+ Settings (User) table does not appear, choose **Interface Configuration > TACACS+ (Cisco IOS)**. Then, choose **Advanced TACACS+ Features**.

This section contains the following topics:

- Setting Enable Privilege Options for a User, page 7-22
- Setting TACACS+ Enable Password Options for a User, page 7-23
- Setting TACACS+ Outbound Password for a User, page 7-24

Setting Enable Privilege Options for a User

You use a TACACS+ Enable Control with Exec session to control administrator access. Typically, you use it for router-management control. Select and specify the user privilege level:

- **Use Group Level Setting**—Sets the privileges for this user identical to the privileges configured at the group level.
- **No Enable Privilege**—Disallows enable privileges for this user.

Note No Enable Privilege is the default setting.

- **Max Privilege for any AAA Client**—You can select from a list the maximum privilege level that will apply to this user on any AAA client on which this user is authorized.
- **Define Max Privilege on a per-Network Device Group Basis**—You can associate maximum privilege levels for this user in one or more NDGs.

Note For information about privilege levels, refer to your AAA client documentation.

Tip You must configure NDGs from within Interface Configuration before you can assign user privilege levels to them.

To select and specify the privilege level for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Under TACACS+ Enable Control in the Advanced TACACS+ Settings table, select one of the four privilege options:

- **Use Group Level Setting**
- **No Enable Privilege**

Note **No Enable Privilege** is the default setting; when setting up an new user account, this privilege should already be selected.

- **Max Privilege for Any Access Server**
- **Define Max Privilege on a per-Network Device Group Basis**

Step 3 If you selected **Max Privilege for Any Access Server** in Step 2, select the appropriate privilege level from the corresponding list.

Step 4 If you selected **Define Max Privilege on a per-Network Device Group Basis** in Step 2, perform the following steps to define the privilege levels on each NDG, as applicable:

a. From the Device Group list, select a device group.

Note You must have already configured a device group for it to be listed.

b. From the Privilege list, select a privilege level to associate with the selected device group.

c. Click **Add Association**.

An entry appears in the table, which associates the device group with a particular privilege level.

d. Repeat Step a through Step c for each device group that you want to associate to this user.

Tip To delete an entry, select the entry and then click **Remove Associate**.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting TACACS+ Enable Password Options for a User

When setting the TACACS+ Enable Password Options for a user, you can use:

- **ACS PAP password**.
- **External database password**.
- **A separate password**.

To set the options for the TACACS+ Enable password:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Select a password option:

- To use the information that is configured in the Password Authentication section, select **Use Cisco Secure PAP password**.

Note For information about basic password setup, see Adding a Basic User Account, page 7-3.

- To use an external database password, select **Use external database password**, and then choose the database that authenticates the enable password for this user.

Note The list of databases displays only the databases that you have configured. For more information, see About External User Databases, page 13-3.

- To use a separate password, click **Use separate password**, and then type and retype to confirm a control password for this user. This password is used in addition to the regular authentication.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Setting TACACS+ Outbound Password for a User

The TACACS+ outbound password enables an AAA client to authenticate itself to another AAA client via outbound authentication. The outbound authentication can be PAP, CHAP, MS-CHAP, or ARAP, and results in the ACS password being given out. By default, the user ASCII/PAP or CHAP/MS-CHAP/ARAP password is used. To avoid compromising inbound passwords, you can configure a separate SENDAUTH password.

Caution Use an outbound password only if you are familiar with the use of a TACACS+ SendAuth/OutBound password.

To set a TACACS+ outbound password for a user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Type and retype to confirm a TACACS+ outbound password for this user.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

RADIUS Attributes

You can configure user attributes for RADIUS authentication generally, at the Internet Engineering Task Force (IETF) level, or for vendor-specific attributes (VSAs) on a vendor-by-vendor basis. For general attributes, see Setting IETF RADIUS Parameters for a User, page 7-25. ACS ships with many popular VSAs already loaded and available to configure and apply. For information about creating additional, custom RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-19.

Caution If you are using Shared Radius Authorization Components (SRACs), you should be aware of issues regarding attribute merging and overwriting RADIUS attributes on a user or group level. You should not assign RADIUS attributes to an individual user (only as a last resort). Use group or SRACs to assign RADIUS attributes in the user's group or profile levels.

This section contains the following topics:

- Setting IETF RADIUS Parameters for a User, page 7-25
- Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User, page 7-26
- Setting Cisco Aironet RADIUS Parameters for a User, page 7-28
- Setting Ascend RADIUS Parameters for a User, page 7-29
- Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User, page 7-30
- Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 7-31
- Setting Microsoft RADIUS Parameters for a User, page 7-32
- Setting Nortel RADIUS Parameters for a User, page 7-33
- Setting Juniper RADIUS Parameters for a User, page 7-34
- Setting BBSM RADIUS Parameters for a User, page 7-35
- Setting Custom RADIUS Attributes for a User, page 7-35

Setting IETF RADIUS Parameters for a User

RADIUS attributes are sent as a profile for the user from ACS to the requesting AAA client.

These parameters appear only if:

- AAA clients (one or more) are configured to use one of the RADIUS protocols in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level IETF RADIUS attributes are enabled under **Interface Configuration > RADIUS (IETF)**.

Note To display or hide any of these attributes in the web interface, see Protocol Configuration Options for RADIUS, page 3-9.

Note For a list and explanation of RADIUS attributes, see Appendix C, "RADIUS Attributes," or the documentation for your particular network device that is using RADIUS.

To configure IETF RADIUS attribute settings to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 In the IETF RADIUS table, for each attribute that you need to authorize for the current user, check the check box next to the attribute and then further define the authorization for the attribute in the box or boxes next to it, as applicable.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User

The Cisco IOS RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco IOS/PIX 6.0)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco IOS/PIX 6.0)** attributes are enabled under **Interface Configuration > RADIUS (Cisco IOS/PIX 6.0)**.

Note To hide or display the Cisco IOS RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

Cisco IOS RADIUS represents only the Cisco IOS VSAs. You must configure the IETF RADIUS and Cisco IOS RADIUS attributes.

To configure and enable Cisco IOS RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Cisco IOS RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 If you want to use the [009\001] `cisco-av-pair` attribute to specify authorizations, check the check box next to the attribute and then type the attribute-value pairs in the text box. Separate each attribute-value pair by pressing **enter**.

For example, if the current user profile corresponds to a Network Admission Control (NAC) client to which ACS always assigns a `status-query-timeout` attribute value that must be different than a value that any applicable group profile contains, you could specify the value as:

```
status-query-timeout=1200
```

Step 4 If you want to use other Cisco IOS/PIX 6.0 RADIUS attributes, select the corresponding check box and specify the required values in the adjacent text box.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Cisco Airespace RADIUS Parameters for a User

The Cisco Airespace RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco Airespace)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco Airespace)** attributes that you want to apply are enabled under **Interface Configuration> RADIUS (Cisco Airespace)**.

Cisco Airespace RADIUS represents only the Cisco Airespace proprietary attributes. You must configure IETF RADIUS and Cisco Airespace RADIUS attributes that you want to use.

Note To hide or display Cisco Airespace RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco Airespace RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Cisco Airespace RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Cisco Airespace RADIUS Attributes table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 Do one:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Cisco Aironet RADIUS Parameters for a User

The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a virtual VSA. This VSA acts as a specialized implementation (that is, a remapping) of the IETF RADIUS Session-Timeout attribute (27) to respond to a request from a Cisco Aironet Access Point.Use the Cisco-Aironet-Session-Timeout attribute to provide a different timeout value when a user must be able to connect via wireless and wired devices. This capability to provide a second timeout value specifically for WLAN connections avoids the difficulties that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes). You do not need to use Cisco-Aironet-Session-Timeout if the particular user will always connect only with a Cisco Aironet Access Point. Rather, use this setting when a user may connect via wired or wireless clients.

For example, imagine a user's **Cisco-Aironet-Session-Timeout** set to 600 seconds (10 minutes) and that same user's IETF RADIUS Session-Timeout set to 3 hours. When the user connects via a VPN, ACS uses 3 hours as the timeout value. However, if that same user connects via a Cisco Aironet Access Point, ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS **Session-Timeout** attribute. Thus, with the **Cisco-Aironet-Session-Timeout** attribute configured, different session-timeout values can be sent depending on whether the end-user client is a wired device or a Cisco Aironet Access Point.

The Cisco Aironet RADIUS parameters appear on the User Setup page only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco Aironet)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco Aironet)** attribute is enabled under RADIUS (Cisco Aironet) in the **Interface Configuration > RADIUS (Cisco Aironet)**.

Note To hide or display the Cisco Aironet RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Cisco Aironet RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Cisco Aironet RADIUS Attributes table, select the **[5842\001] Cisco-Aironet-Session-Timeout** check box.

Step 4 In the **[5842\001] Cisco-Aironet-Session-Timeout** box, type the session-timeout value (in seconds) that ACS is to send in the IETF RADIUS Session-Timeout (27) attribute when the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.

For more information about the IETF RADIUS Session-Timeout attribute, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Ascend RADIUS Parameters for a User

The Ascend RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Ascend)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Ascend)** attributes that you want to apply are enabled under in the **Interface Configuration > RADIUS (Ascend)**.

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting that appears for RADIUS is `Ascend-Remote-Addr`.

Note To hide or display Ascend RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA that is applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Ascend RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Ascend RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Ascend RADIUS Attributes table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User

To control Microsoft Point-to-Point Encryption (MPPE) settings for users who access the network through a Cisco VPN 3000-series concentrator, an Adaptive Security Appliance (ASA), or PIX Security Appliance version 7.x+, use the **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) attributes. Settings for **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) attributes; regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attribute configurations appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.

Cisco VPN 3000/ASA/PIX 7.x+ RADIUS represents only the Cisco VPN 3000/ASA/PIX 7.x+ VSA. You must configure the IETF RADIUS and Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes.

Note To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Cisco VPN 3000/ASA/PIX 7.x+ Attribute table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User

The Cisco VPN 5000 Concentrator RADIUS attribute configurations appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco VPN 5000)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level RADIUS (Cisco VPN 5000) attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Cisco VPN 5000)**.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Cisco VPN 5000 Concentrator RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Cisco VPN 5000 Concentrator Attribute table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Microsoft RADIUS Parameters for a User

Microsoft RADIUS provides VSAs supporting Microsoft Point-to-Point Encryption (MPPE), which is an encryption technology developed by Microsoft to encrypt point-to-point (PPP) links. These PPP connections can be via a dial-in line, or over a Virtual Private Network (VPN) tunnel.

To control Microsoft MPPE settings for users who access the network through a Cisco VPN 3000-series concentrator, use the **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) attributes. Settings for **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the **RADIUS (Cisco VPN 3000)** attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only if the following are true:

- AAA clients (one or more) are configured in **Network Configuration** that use a RADIUS protocol that supports the Microsoft RADIUS VSA.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Microsoft)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Microsoft)**.

The following ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+
- Cisco VPN 5000
- Ascend
- Cisco Airespace

Microsoft RADIUS represents only the Microsoft VSA. You must configure the IETF RADIUS and Microsoft RADIUS attributes.

Note To hide or display Microsoft RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Microsoft RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Cisco IOS RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Microsoft RADIUS Attributes table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Note The **MS-CHAP-MPPE-Keys** attribute value is autogenerated by ACS; there is no value to set in the web interface.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Nortel RADIUS Parameters for a User

The Nortel RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Nortel)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Nortel)** attributes that you want to apply are enabled under in the **Interface Configuration > RADIUS (Nortel)**.

Nortel RADIUS represents only the Nortel proprietary attributes. You must configure the Internet Engineering Task Force (IETF) RADIUS and Nortel RADIUS attributes. Proprietary attributes override IETF attributes.

Note To hide or display Nortel RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA that is applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Nortel RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Nortel RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Nortel RADIUS Attributes table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Juniper RADIUS Parameters for a User

The Juniper RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Juniper)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Juniper)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Juniper)**.

Juniper RADIUS represents only the Juniper proprietary attributes. You must configure the IETF RADIUS and Juniper RADIUS attributes. Proprietary attributes override IETF attributes.

Note To hide or display Juniper RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Juniper RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Juniper RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the Juniper RADIUS Attributes table, to specify the attributes to authorize for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting BBSM RADIUS Parameters for a User

The Building Broadband Services Manager (BBSM) RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (BBSM)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (BBSM)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (BBSM)**.

BBSM RADIUS represents only the BBSM proprietary attributes. You must configure the IETF RADIUS and BBSM RADIUS attributes. Proprietary attributes override IETF attributes.

Note To hide or display BBSM RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable BBSM RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring BBSM RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the BBSM RADIUS Attributes table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Custom RADIUS Attributes for a User

Custom RADIUS parameters appear only if all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-19.)
- AAA clients (one or more) are configured in **Network Configuration** that use a RADIUS protocol that supports the custom VSA.

- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level RADIUS (*custom name*) attributes that you want to apply are enabled under RADIUS (*custom name*) in the **Interface Configuration** section.

You must configure the IETF RADIUS and the custom RADIUS attributes. Proprietary attributes override IETF attributes.

To configure and enable custom RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-3.

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring custom RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-25.

Step 3 In the RADIUS *custom name* Attributes table, to specify the attributes that should be authorized for the user:

a. Check the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it, as required.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes," or your AAA client documentation.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

User Management

This section describes how to use the User Setup section to perform a variety of user account-management tasks.

This section contains the following topics:

- Listing All Users, page 7-37
- Finding a User, page 7-37
- Disabling a User Account, page 7-38
- Deleting a User Account, page 7-38
- Resetting User Session Quota Counters, page 7-39
- Resetting a User Account after Login Failure, page 7-39
- Removing Dynamic Users, page 7-40
- Saving User Settings, page 7-41

Listing All Users

The User List displays all user accounts (enabled and disabled). The list includes, for each user, the username, status, and the group to which the user belongs.

Usernames appear in the order in which they were entered into the database. This list cannot be sorted.

To view a list of all user accounts:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 Click **List All Users**.

In the display area on the right, the User List appears.

Step 3 To view or edit the information for an individual user, click the username in the right window.

The user account information appears.

Finding a User

To find a user:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 Type the name in the **User** box, and then click **Find**.

Tip You can use an asterisk (*) as a wildcard in this box.

Tip To display a list of usernames that begin with a particular letter or number, click the letter or number in the alphanumeric list. A list of users, whose names begin with that letter or number, opens in the display area on the right.

The username, status (enabled or disabled), and group to which the user belongs appear in the display area on the right.

Step 3 To view or edit the information for the user, click the username in the display area on the right.

The user account information appears.

Disabling a User Account

To manually disable a user account in the ACS internal database:

Note To configure the conditions by which a user account will automatically be disabled, see Setting Options for User Account Disablement, page 7-13.

Note Do not confuse this procedure with account expiration due to password aging. Password aging is defined for groups only, not for individual users.

To disable a user account:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 In the **User** box, type the name of the user whose account is to be disabled.

Step 3 Click **Add/Edit**.

The User Setup Edit page opens. The username being edited is at the top of the page.

Step 4 Select the **Account Disabled** check box.

Step 5 Click **Submit** at the bottom of the page.

The specified user account is disabled.

Deleting a User Account

You can delete user accounts one at a time by using the web interface.

Note If you are by authenticating using the Unknown User policy and you want deny a user access by deleting the user account, you must also delete the user account from the external user database. This action prevents the username from being automatically added to the ACS internal database the next time the user attempts to log in.

Tip For deleting batches of user accounts, use the Relational Database Management System (RDBMS) Synchronization feature with action code 101 (see RDBMS Synchronization, page 9-17, for more information.).

To delete a user account:

Step 1 Click **User Setup**.

The User Setup Select page of the web interface opens.

Step 2 In the **User** box, type the complete username to be deleted.

Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 At the bottom of the User Setup page, click **Delete**.

Note The Delete button appears only when you are editing user information, not when you are adding a username.

A popup window appears and prompts you to confirm the user deletion.

Step 5 Click **OK**.

The user account is removed from the ACS internal database.

Resetting User Session Quota Counters

You can reset the session quota counters for a user before or after the user exceeds a quota.

To reset user usage quota counters:

Step 1 Click **User Setup**.

The Select page of the web interface opens.

Step 2 In the **User** box, type the complete username of the user whose session quota counters that you are going to reset.

Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the Session Quotas section, select the **Reset All Counters on submit** check box.

Step 5 Click **Submit** at the bottom of the browser page.

The session quota counters are reset for this user. The User Setup Select page appears.

Resetting a User Account after Login Failure

Perform this procedure when an account is disabled because the failed attempts count has been exceeded during an unsuccessful user attempt to log in.

To reset a user account after login failure:

Step 1 Click **User Setup**.

The User Setup Select page of the web interface opens.

Step 2 In the **User** box, type the complete username of the account to be reset.

Note Alternatively, you can click List All Users and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the Account Disable table, select the **Reset current failed attempts count on submit** check box, and then click **Submit**.

The **Failed attempts since last successful login**: counter resets to zero (0) and the system reenables the account.

Note This counter shows the number of unsuccessful login attempts since the last time this user logged in successfully.

Note If the user authenticates with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings that you configured in Windows.

Removing Dynamic Users

External sources can manage dynamic users, their identities and other related properties. Dynamic users are created in the ACS internal database after they are successfully authenticated against the external sources.

Users that are dynamically mapped will keep on being dynamically mapped even when their group mapping settings are modified to a group which is set to **Disable caching of dynamically mapped users**.

You can remove dynamic users in user groups that are cached.

Note All CSAuth activities will be suspended while dynamic users are being removed from the database.

To remove dynamic users:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page appears.

Step 2 Click **Remove Dynamic Users.**

A message appears in the right pane, indicating the number of dynamic users removed or whether any errors occurred.

Note Dynamically mapped users *are not* saved when you perform replication, upgrade or overinstall ACS. Dynamically mapped users *are* saved when you back up or restore ACS.

Saving User Settings

After you have completed configuration for a user you must save your work.

To save the configuration for the current user:

Step 1 To save the user account configuration, click **Submit**.

Step 2 To verify that your changes were applied, type the username in the **User** box and click **Add/Edit**, and then review the settings.

System Configuration: Basic

This chapter addresses the basic features in the System Configuration section of the web interface for Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains the following topics:

- Service Control, page 8-1
- Logging, page 8-3
- Date Format Control, page 8-3
- Local Password Management, page 8-4
- ACS Backup, page 8-7
- ACS System Restore, page 8-11
- ACS Active Service Management, page 8-13
- VoIP Accounting Configuration, page 8-15

Service Control

ACS uses several services. The Service Control page provides basic status information about the services. You use this page to configure the service log files, and to stop or restart the services. For more information about ACS services, see Chapter 1, "Overview."

Tip You can configure ACS service logs. For more information, see Configuring Service Logs, page 11-24.

This section contains the following topics:

- Determining the Status of ACS Services, page 8-2
- Stopping, Starting, or Restarting Services, page 8-2
- Setting Service Log File Parameters, page 8-3

Determining the Status of ACS Services

You can determine whether ACS services are running or stopped by accessing the Service Control page.

To determine the status of ACS services:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the ACS.

Stopping, Starting, or Restarting Services

You can stop, start, or restart ACS services as needed. Stopping, starting, or restarting ACS services from within the interface achieves the same result as starting and stopping ACS services from within Windows Control panel. This procedure stops, starts, or restarts the ACS services except for CSAdmin, which is responsible for the web interface.

Note If you need to restart the CSAdmin service, you can use the Control Panel Services applet; however, you should just let ACS handle the services, due to the dependencies in the order which the services are started.

To stop, start, or restart ACS services:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the ACS.

If the services are running, the Restart and Stop buttons appear at the bottom of the page.

If the services are stopped, the Start button appears at the bottom of the page.

Step 3 Click **Stop**, **Start**, or **Restart**, as applicable.

The status of ACS services changes to the state according to which button that you clicked.

Setting Service Log File Parameters

To configure the parameters for the service log file and directory management, use this page. For detailed option descriptions, see Configuring Service Logs, page 11-24.

Step 1 Complete the following:

Field	From the List, Select:
Level of detail	The level of detail.
Generate new file	The schedule to generate log files.
Manage directory	How long to keep log files.

Step 2 Click **Restart**.

ACS restarts its services and implements the service log settings that you specified.

Note Ensure that you have enough disk space in which to store your log files. Consult the logs if any problems occur.

Logging

You can configure ACS to generate logs for administrative and accounting events, depending on the protocols and options that you enable. Log files are stored in the *drive:\install_dir\service_name\Logs* directory. For example, in C:*CiscoSecureACS\CSAuth\Logs*. For details on service logs and gathering information for troubleshooting, see Service Logs, page 11-23.

Date Format Control

ACS supports two possible date formats in its logs, reports, and administrative interface. You can choose a month/day/year format or a day/month/year format.

Tip Using a comma-separated value (CSV) file might not work well in different countries; for example, when imported into programs such as Word or Excel. You might need to replace the commas(,) with semicolons (;) if necessary.

Setting the Date Format

Note If you have reports that were generated before you changed the date format, you must move or rename them to avoid conflicts. For example, if you are using the month/day/year format, ACS assigns the name *2001-07-12.csv* to a report that was generated on July 12, 2001. If you subsequently change to the day/month/year format, on December 7, 2001, ACS creates a file also named *2001-07-12.csv* and overwrites the existing file.

To set the date format:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Date Format Control**.

ACS displays the Date Format Selection table.

Step 3 Select a date format option.

Step 4 Click **Submit & Restart**.

ACS restarts its services and implements the date format that you selected.

Note For the new date format to be seen in the web interface reports, you must restart the connection to the ACS. Click the **X** in the upper-right corner of the browser window to close it.

Local Password Management

Use the Local Password Management page to configure settings that manage user passwords that were in the ACS internal database.

Note Validation options do not apply to the ACS **admin** password. ACS administrator accounts have no correlation with ACS user accounts, or username and password authentication. ACS stores accounts that were created for authentication of network service requests and those that were created for ACS administrative access in separate internal databases.

The Local Password Management page contains these sections:

- **Password Validation Options**—You use these settings to configure validation parameters for user passwords. ACS enforces these rules when an administrator changes a user password in the ACS internal database and when a user attempts to change passwords by using the Authentication Agent applet.

  Note Password validation options apply only to user passwords that are stored in the ACS internal database. They do not apply to passwords in user records in external user databases; nor do they apply to enable or **admin** passwords for Cisco IOS network devices.

The password validation options are:

- **Password length between *X* and *Y* characters**—Enforces that password lengths adhere to the values specified in the *X* and *Y* boxes, inclusive. ACS supports passwords up to 32 characters long.
- **Password may not contain the username**—Requires that a user password does not contain the username.
- **Password is different from the previous value**—Requires that a new user password to be different from the previous password.
- **Password must be alphanumeric**—Requires that a user password contain letters and numbers.

- **Remote Change Password**—You use these settings to configure whether a Telnet password change is enabled and, if so, whether ACS immediately sends the updated user data to its replication partners.

  The remote change password options are:

  - **Disable TELNET Change Password against this ACS and return the following message to the users telnet session**—When selected, this option disables the ability to perform password changes during a Telnet session that a Terminal Access Controller Access Control System (TACACS+) Authentication, Authorization, and Accounting (AAA) client hosts. Users who submit a password change receive the text message that you type in the corresponding box.
  - **Upon remote user password change, immediately propagate the change to selected replication partners**—This setting determines whether ACS sends its replication partners any passwords that are changed during a Telnet session that is hosted by a TACACS+ AAA client, the Authentication Agent, or the User-Changeable Passwords web interface. The ACSs that were configured as the replication partners of this ACS appear below this check box.

    This feature depends on the Database Replication feature being configured properly; however, replication scheduling does not apply to propagation of changed password information. ACS sends changed password information immediately, regardless of replication scheduling.

    Changed password information is replicated only to ACSs that are properly configured to receive replication data from this ACS. The automatically triggered cascade setting for the Database Replication feature does not cause ACSs that receive changed password information to send it to their replication partners.

    For more information about Database Replication, see ACS Internal Database Replication, page 9-1.

- **Password Change Log File Management**—You use these settings to configure how ACS handles log files that are generated for the User Password Change report. For more information about this report, see ACS System Logs, page 11-8.

  The log file management options for the User Password Changes Log are:

  - **Generate New File**—You can specify the frequency at which ACS creates a *User Password Changes Log* file: daily, weekly, monthly; or, after the log reaches a size in kilobytes that you specify.
  - **Manage Directory**—You can specify whether ACS controls the retention of log files. You can use this feature to specify the maximum number of files to retain or the maximum age of files to retain. If the maximum number of files is exceeded, ACS deletes the oldest log file. If the maximum age of a file is exceeded, ACS deletes the file.

Configuring Local Password Management

To configure password validation options for user account passwords:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Local Password Management**.

The Local Password Management page appears.

Step 3 Under Password Validation Options:

a. In **Password length between *X* and *Y* characters**, type the *minimum* valid number of characters for a password in the *X* box. While the *X* box accepts two characters, passwords can only be between 1 and 32 characters in length.

b. In **Password length between *X* and *Y* characters**, type the *maximum* valid number of characters for a password in the *Y* box. While the *Y* box accepts two characters, passwords can only be between 1 and 32 characters in length.

c. If you want to disallow passwords that contain the username, check the **Password may not contain the username** check box.

d. If you want to require that a user password be different than the previous user password, check the **Password is different from the previous value** check box.

e. If you want to require that passwords must contain letters and numbers, check the **Password must be alphanumeric** check box.

Step 4 Under Remote Change Password:

a. If you want to *enable* user password changes in Telnet sessions, clear the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box.

b. If you want to *disable* user password changes in Telnet sessions, check the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box.

c. In the box below the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box, type a message that users should see when attempting to change a password in a Telnet session and when the Telnet password change feature has been disabled (Step b).

d. If you want ACS to send changed password information immediately after a user has changed a password, check the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

Tip The ACSs that receive the changed password information appear below the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

Step 5 If you want ACS to generate a new User Password Changes log file at a regular interval, select one:

- **Every day**—ACS generates a new User Password Changes log file at the start of each day.
- **Every week**—ACS generates a new User Password Changes log file at the start of each week.
- **Every month**—ACS generates a new User Password Changes log file at the start of each month.

Step 6 If you want ACS to generate a new *User Password Changes* log file when the current file reaches a specific size, select the **When size is greater than** *X* **KB** option and type the file size threshold, in kilobytes, in the *X* box.

Step 7 If you want to manage which *User Password Changes* log files that ACS keeps:

a. Check the **Manage Directory** check box.

b. If you want to limit the number of User Password Changes log files that ACS retains, select the **Keep only the last** *X* **files** option and type the number of files that you want ACS to retain in the *X* box.

c. If you want to limit the age of User Password Changes log files that ACS retains, select the **Delete files older than** *X* **days** option and type the number of days for which ACS should retain a User Password Changes log file before deleting it.

Step 8 Click **Submit**.

ACS restarts its services and implements the settings that you specified.

ACS Backup

This section provides information about the ACS Backup feature, including procedures for implementing this feature.

Caution As with previous versions of ACS, you must not perform backups, restores, or replication between different versions of ACS.

This section contains the following topics:

- About ACS Backup, page 8-7
- Backup File Locations, page 8-8
- Directory Management, page 8-8
- Components Backed Up, page 8-8
- Reports of ACS Backups, page 8-8
- Backup Options, page 8-9
- Performing a Manual ACS Backup, page 8-9
- Scheduling ACS Backups, page 8-9
- Disabling Scheduled ACS Backups, page 8-10

About ACS Backup

The ACS Backup feature provides the option to back up your user and group databases, and your ACS system configuration information to a file on the local hard drive. You can manually back up the ACS system. You can also establish automated backups that occur at regular intervals, or at selected days of the week and times. Maintaining backup files can minimize downtime if system information becomes corrupt or is misconfigured. We recommend copying the files to the hard drive on another system in case the hardware fails on the primary system.

For information about using a backup file to restore ACS, see ACS System Restore, page 8-11.

Note The backup and restore features between different ACS versions are not supported.

Backup File Locations

The default directory for backup files is:

drive:*path*\CSAuth\System Backups

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory. For example, if you installed ACS version 4.0 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v4.0\CSAuth\System Backups
```

ACS determines the filename that is assigned to a backup. For more information about filenames that ACS assigns to backup files, see Backup Filenames and Locations, page 8-11.

Directory Management

You can configure the number of backup files to keep and the number of days after which backup files are deleted. The more complex your configuration and the more often you back up the system, the more diligent you should be about clearing out old databases from the ACS hard drive.

Components Backed Up

The ACS System Backup feature backs up the ACS user database that is relevant to ACS. The user database backup includes all user information, such as username, password, and other authentication information, including server certificates and the certificate trust list.

If your ACS for Windows logs information to a remote ACS server, both ACS versions must have identical release, build, and patch numbers; or the logging might fail.

As with previous versions of ACS, you must not perform backups, restores, or replication between different versions of ACS.

Reports of ACS Backups

When a system backup occurs, whether it was manually generated or scheduled, the event is logged in the Administration Audit report, and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of ACS.

For more information about ACS reports, see Chapter 1, “Overview”.

Backup Options

The ACS System Backup Setup page contains:

- **Manually**—ACS does not perform automatic backups. When this option is selected, you can only perform a backup by following the steps in Performing a Manual ACS Backup, page 8-9.
- **Every *X* minutes**—ACS performs automatic backups on a set frequency. The unit of measurement is minutes, with a default backup frequency of 60 minutes.
- **At specific times**—ACS performs automatic backups at the time that is specified in the day-and-hour graph. The minimum interval is one hour, and the backup occurs on the hour that you selected.
- **Directory**—The directory where ACS writes the backup file. You must specify the directory by its full path on the Windows server that runs ACS, such as `c:\acs-bups`.
- **Manage Directory**—Defines whether ACS deletes older backup files. Using the following options, you can specify how ACS determines which log files to delete:
  - **Keep only the last *X* files**—ACS retains the most recent backup files, up to the number of files that you specified. When the number of files that you specified is exceeded, ACS deletes the oldest files.
  - **Delete files older than *X* days**—ACS deletes backup files that are older than the number of days that you specified. When a backup file grows older than the number of days that you specified, ACS deletes it.

Performing a Manual ACS Backup

You can back up ACS whenever you want, without scheduling the backup.

To perform an immediate backup of ACS:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

The ACS System Backup Setup page appears.

Step 3 In the **Directory** box under Backup Location, type the drive and path to the directory on a local hard drive where you want the backup file to be written.

Step 4 Click **Backup Now**.

ACS immediately begins a backup.

Scheduling ACS Backups

You can schedule ACS backups to occur at regular intervals, or on selected days of the week and times.

To schedule the times at which ACS performs a backup:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

The ACS System Backup Setup page appears.

Step 3 To schedule backups at regular intervals, under ACS Backup Scheduling, select the **Every** *X* **minutes** option and, in the ***X*** box, type the length of the interval at which ACS should perform backups.

Note Because ACS is momentarily shut down during backup, if the backup interval is too frequent, users might be unable to authenticate.

Step 4 To schedule backups at specific times:

a. Under ACS Backup Scheduling, select the **At specific times** option.

b. In the day-and-hour graph, click the times at which you want ACS to perform a backup.

Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 5 To change the location where ACS writes backup files, type the drive letter and path in the **Directory** box.

Step 6 To manage which backup files ACS keeps:

a. Check the **Manage Directory** check box.

b. To limit the number of backup files that ACS retains, select the **Keep only the last** *X* **files** option and type in the ***X*** box the number of files that you want ACS to retain.

c. To limit the age of backup files that ACS retains, select the **Delete files older than** *X* **days** option and type the number of days for which ACS should retain a backup file before deleting it.

Step 7 Click **Submit**.

ACS implements the backup schedule that you configured.

Disabling Scheduled ACS Backups

You can disable scheduled ACS backups without losing the schedule itself. You can use this method to end scheduled backups and resume them later without having to recreate the schedule.

To disable a scheduled backup:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

The ACS System Backup Setup page appears.

Step 3 Under ACS Backup Scheduling, select the **Manual** option.

Step 4 Click **Submit**.

ACS does not continue any scheduled backups. You can still perform manual backups as needed.

ACS System Restore

This section provides information about the ACS System Restore feature, including procedures for restoring your ACS from a backup file.

Caution As with previous versions of ACS, you must not perform backups, restores, or replication between different versions of ACS.

This section contains the following topics:

- About ACS System Restore, page 8-11
- Backup Filenames and Locations, page 8-11
- Components Restored, page 8-12
- Reports of ACS Restorations, page 8-12
- Restoring ACS from a Backup File, page 8-12

About ACS System Restore

You use the ACS System Restore feature to restore your user and group databases, and your ACS system configuration information from backup files that the ACS Backup feature generates. This feature helps you to minimize downtime if ACS system information becomes corrupted or is misconfigured.

The ACS System Restore feature only works with backup files that ACS generates when running an identical ACS version and patch level.

If you restore onto a physically different server, it must have the same IP address as the original server; otherwise, replication will not work correctly because the network configuration has a hidden record that contains details of the ACS server.

Backup Filenames and Locations

The ACS System Restore feature restores the ACS user database and ACS Windows Registry information from a file that the ACS Backup feature created. ACS writes backup files only on the local hard drive. You can restore from any backup file that you select. For example, you can restore from the latest backup file; or, if you suspect that the latest backup was incorrect, you can select an earlier backup file to restore.

The backup directory is selected when you schedule backups or perform a manual backup. The default directory for backup files is:

drive`:\`*path*`\CSAuth\System Backups`

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory. For example, if you installed ACS version 3.0 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v3.0\CSAuth\System Backups
```

ACS creates backup files by using the date and time format:

dd-mmm-yyyy hh-nn-ss`.dmp`

where:

- *dd* is the date the backup started
- *mmm* is the month, abbreviated in alphabetic characters
- *yyyy* is the year
- *hh* is the hour, in 24-hour format
- *nn* is the minute
- *ss* is the second at which the backup started

For example, if ACS started a backup on October 13, 1999, 11:41:35 a.m., ACS would generate a backup file named:

```
13-Oct-1999 11-41-35.dmp
```

If you are uncertain of the location of the latest backup file, check your scheduled backup configuration on the ACS Backup page.

Components Restored

You can select the components to restore: user and group databases, system configuration, or both.

Reports of ACS Restorations

When an ACS system restoration occurs, the event is logged in the Administration Audit report, and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of ACS.

For more information about ACS reports, see Chapter 1, "Overview".

Restoring ACS from a Backup File

You can perform a system restoration of ACS whenever needed.

Note Using the ACS System Restore feature restarts all ACS services and logs out all administrators.

To restore ACS from a backup file that the ACS Backup feature generated:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Restore**.

The ACS System Restore Setup page appears.

The Directory box displays the drive and path to the backup directory most recently configured in the Directory box on the ACS Backup page.

Beneath the Directory box, ACS displays the backup files in the current backup directory. If no backup files exist, `<No Matching Files>` appears in place of filenames.

Step 3 To change the backup directory, type the new drive and path to the backup directory in the **Directory** box, and then click **OK**.

ACS displays the backup files, if any, in the backup directory that you specified.

Step 4 In the list below the **Directory** box, select the backup file that you want to use to restore ACS.

Step 5 To restore user and group database information, select the **User and Group Database** check box.

Step 6 To restore system configuration information, select the **ACS System Configuration** check box.

Step 7 Click **Restore Now**.

ACS displays a confirmation dialog box indicating that performing the restoration will restart ACS services and log out all administrators.

Step 8 To continue with the restoration, click **OK**.

ACS restores the system components that you specified by using the backup file that you selected. The restoration should require several minutes to finish, depending on the components that you selected to restore and the size of your database.

When the restoration is complete, you can log in to ACS again.

ACS Active Service Management

ACS Active Service Management is an application-specific service-monitoring tool that is tightly integrated with ACS. The two features that comprise ACS Active Service Management are described in this section.

This section contains the following topics:

- System Monitoring, page 8-13
- Event Logging, page 8-15

System Monitoring

You use ACS system monitoring to determine how often ACS tests its authentication and accounting processes, and to determine what automated actions to take if the tests detect a failure of these processes. ACS performs system monitoring with the CSMon service. For more information about the CSMon service, see CSMon, page G-4.

System Monitoring Options

The options for configuring system monitoring are:

- **Test login process every *X* minutes**—Controls whether ACS tests its login process. The value in the X box defines, in minutes, how often ACS tests its login process. The default frequency is once per minute, which is also the most frequent testing interval possible.

  When you enable this option, at the interval defined, ACS tests authentication and accounting. If the test fails, after four unsuccessful retries ACS performs the action identified in the If no successful authentications are recorded list and logs the event.

- **If no successful authentications are recorded**—Specifies what action ACS takes if it detects that its test login process failed. This list contains several built-in actions and actions that you define. The items beginning with asterisks (*) are predefined actions:

  - ***Restart All**—Restart all ACS services.

- ***Restart RADIUS/TACACS+**—Restart only the Proxy Remote Access Dial-In User Service (RADIUS) and TACACS+ services.
- ***Reboot**—Reboot ACS.
- **Custom actions**—You can define other actions for ACS to take if failure of the login process occurs. ACS can execute a batch file or executable on the failure of the login process. To make a batch or executable file available in the on failure list, place the file in:

  drive:*path*\CSMon\Scripts

  where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory.

Tip Restart CSAdmin to see the new batch file or executable in the list.

- **Take No Action**—Leave ACS operating as is.

- **Generate event when an attempt is made to log in to a disabled account**—Specifies whether ACS generates a log entry when a user attempts to log in to your network by using a disabled account.
- **Log all events to the NT Event log**—Specifies whether ACS generates a Windows event log entry for each exception event.
- **Email notification of event**—Specifies whether ACS sends an e-mail notification for each event.
  - **To**—The e-mail address to which a notification e-mail is sent; for example, *joeadmin@company.com*.
  - **SMTP Mail Server**—The simple mail transfer protocol (SMTP) server that ACS should use to send notification e-mail. You can identify the SMTP server by its hostname or IP address.

Setting Up System Monitoring

To set up ACS System Monitoring:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Service Management**.

The ACS Active Service Management Setup page appears.

Step 3 To have ACS test the login process:

a. Select the **Test login process every** *X* **minutes** check box.

b. Type in the ***X*** box the number of minutes (up to 3 characters) that should pass between each login process test.

c. From the **If no successful authentications are recorded** list, select the action that ACS should take when the login test fails five successive times.

Step 4 To generate a Windows event when a user tries to log in to your network by using a disabled account, select the **Generate event when an attempt is made to log in to a disabled account** check box.

Step 5 If you want to set up event logging, see Setting Up Event Logging, page 8-15.

Step 6 If you are finished setting up ACS Service Management, click **Submit**.

ACS implements the service-management settings that you made.

Event Logging

You use the Event Logging feature to configure whether ACS logs events to the Windows event log and ACS generates an e-mail when an event occurs. ACS uses the System Monitoring feature to detect the events to be logged. For more information about system monitoring, see System Monitoring Options, page 8-13.

Setting Up Event Logging

To view the Windows event log, choose **Start > Programs > Administrative Tools > Event Viewer**. For more information about the Windows event log or Event Viewer, refer to your Microsoft Windows documentation.

To set up ACS event logging:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Service Management**.

The ACS Active Service Management Setup page appears.

Step 3 To have ACS send all events to the Windows event log, select **Log all events to the Windows Event log**.

Step 4 To have ACS send an e-mail when an event occurs:

a. Select the **Email notification of event** check box.

b. In the **To** box, type the e-mail address (up to 200 characters) to which ACS should send event notification e-mail.

Note Do not use underscores (_) in the e-mail addresses that you type in this box.

c. In the **SMTP Mail Server** box, type the hostname (up to 200 characters) of the sending e-mail server.

Note The SMTP mail server must be operational and must be available from the ACS.

Step 5 If you want to set up system monitoring, see Setting Up System Monitoring, page 8-14.

Step 6 If you are finished setting up ACS Service Management, click **Submit**.

ACS implements the service-management settings that you made.

VoIP Accounting Configuration

You use the voice over IP (VoIP) Accounting Configuration feature to specify which accounting logs receive VoIP accounting data. The options for VoIP accounting are:

- **Send to RADIUS and VoIP Accounting Log Targets**—ACS appends VoIP accounting data to the RADIUS accounting data and logs it separately to a CSV file. To view the data, you can use RADIUS Accounting or VoIP Accounting under **Reports** and **Activity**.

- **Send only to VoIP Accounting Log Targets**—ACS only logs VoIP accounting data to a CSV file. To view the data, you can use VoIP Accounting under Reports and Activity.
- **Send only to RADIUS Accounting Log Targets**—ACS only appends VoIP accounting data to the RADIUS accounting data. To view the data, you can use RADIUS Accounting under Reports and Activity.

Configuring VoIP Accounting

Note The VoIP Accounting Configuration feature does not enable VoIP accounting. To enable VoIP accounting, see Chapter 1, "Overview".

To configure VoIP accounting:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **VoIP Accounting Configuration**.

Note If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Voice-over-IP (VoIP) Accounting Configuration** check box.

The VoIP Accounting Configuration page appears. The Voice-over-IP (VoIP) Accounting Configuration table displays the options for VoIP accounting.

Step 3 Select the VoIP accounting option that you want.

Step 4 Click **Submit**.

ACS implements the VoIP accounting configuration that you specified.

System Configuration: Advanced

This chapter addresses the ACS internal database replication and RDBMS synchronization features in the System Configuration section of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains the following sections:

- ACS Internal Database Replication, page 9-1
- RDBMS Synchronization, page 9-17
- IP Pools Server, page 9-28
- IP Pools Address Recovery, page 9-33

ACS Internal Database Replication

This section provides information about the ACS internal database replication feature, including procedures for implementing this feature and configuring the ACSs involved.

Note ACS does not support distributed deployments in a NAT environment. If a Primary or Secondary address is NATed, the database replication file will indicate shared secret mismatch.

This section contains the following topics:

- About ACS Internal Database Replication, page 9-2
  - Replication Process, page 9-3
  - Replication Frequency, page 9-5
- Important Implementation Considerations, page 9-5
- Database Replication Versus Database Backup, page 9-6
- Database Replication Logging, page 9-7
- Replication Options, page 9-7
  - Replication Components Options, page 9-7
  - Outbound Replication Options, page 9-9
  - Inbound Replication Options, page 9-10
- Implementing Primary and Secondary Replication Setups on ACSs, page 9-10

- Configuring a Secondary ACS, page 9-11
- Replicating Immediately, page 9-12
- Scheduling Replication, page 9-14
- Disabling ACS Database Replication, page 9-15
- Configuring Automatic Change Password Replication, page 9-16
- Database Replication Event Errors, page 9-16

About ACS Internal Database Replication

Database replication creates mirror systems of ACSs by duplicating parts of the primary ACS setup to one or more secondary ACSs. You can configure your AAA clients to use these secondary ACSs if the primary ACS fails or is unreachable. With a secondary ACS whose ACS internal database is a replica of the ACS internal database on the primary ACS, if the primary ACS goes out of service, incoming requests are authenticated without network downtime, provided that your AAA clients are configured to fail over to the secondary ACS.

You can use database replication to:

- Select the parts of the primary ACS configuration to be replicated.
- Control the timing of the replication process, including creating schedules.
- Export selected configuration items from the primary ACS.
- Securely transport selected configuration data from the primary ACS to one or more secondary ACSs.
- Update the secondary ACSs to create matching configurations.

The following items cannot be replicated:

- IP pool definitions (for more information, see About IP Pools Server, page 9-28).
- ACS certificate and private key files.
- Unknown user group mapping configuration.
- Dynamically-mapped users.
- Settings on the ACS Service Management page in the System Configuration section.
- RDBMS Synchronization settings.
- Third-party software, such as Novell Requestor or RSA ACE client software.

Tip For a list of the various components and what database replication encompasses, see Replication Components Options, page 9-7.

With regard to database replication, we make the following distinctions about ACSs:

- **Primary ACS**—An ACS that sends replicated ACS internal database components to other ACSs.
- **Secondary ACS**—An ACS that receives replicated ACS internal database components from a primary ACS. In the web interface, these are identified as replication partners.

An ACS can be a primary ACS and a secondary ACS, provided that it is not configured to be a secondary ACS to an ACS for which it performs as a primary ACS.

Note Bidirectional replication, wherein an ACS sends database components to and receives database components from the same remote ACS, is not supported. Replication fails if an ACS is configured to replicate to and from the same ACS.

Note All ACSs that are involved in replication must run the same release of the ACS software. For example, if the primary ACS is running ACS version 3.2, all secondary ACSs should be running ACS version 3.2. Because patch releases can introduce significant changes to the ACS internal database, we strongly recommend that ACSs involved in replication use the same patch level.

Replication Process

This topic describes the process of database replication, including the interaction between a primary ACS and each of its secondary ACSs. The following steps occur in database replication:

1. The primary ACS determines if its database has changed since the last successful replication. If it has, replication proceeds. If it has not, replication is aborted. No attempt is made to compare the databases of the primary and secondary ACSs.

Tip You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

2. The primary ACS contacts the secondary ACS. In this initial connection, the following four events occur:
   a. The two ACSs perform mutual authentication based on the shared secret of the primary ACS. If authentication fails, replication fails.

      Note On the secondary ACS, the AAA Servers table entry for the primary ACS must have the same shared secret that the primary ACS has for itself in its own AAA Servers table entry. The shared secret of the secondary ACS is irrelevant.

   b. The secondary ACS verifies that it is not configured to replicate to the primary ACS. If it is, replication is aborted. ACS does not support bidirectional replication, wherein an ACS can act as a primary and a secondary ACS to the same remote ACS.
   c. The primary ACS verifies that the version of ACS that the secondary ACS is running is the same as its own version of ACS. If not, replication fails.
   d. The primary ACS compares the list of database components that it is configured to send with the list of database components that the secondary ACS is configured to receive. If the secondary ACS is not configured to receive any of the components that the primary ACS is configured to send, the database replication fails.
3. After the primary ACS has determined which components to send to the secondary ACS, the replication process continues on the primary ACS:
   a. The primary ACS stops its authentication and creates a copy of the ACS internal database components that it is configured to replicate. During this step, if AAA clients are configured properly, those that usually use the primary ACS fail over to another ACS.

b. The primary ACS resumes its authentication service. It also compresses and encrypts the copy of its database components for transmission to the secondary ACS.

c. The primary ACS transmits the compressed, encrypted copy of its database components to the secondary ACS. This transmission occurs over a TCP connection by using port 2000. The TCP session uses a 128-bit encrypted, Cisco-proprietary protocol.

4. After the preceding events on the primary ACS, the database replication process continues on the secondary ACS:

   a. The secondary ACS receives the compressed, encrypted copy of the ACS internal database components from the primary ACS. After transmission of the database components is complete, the secondary ACS decompresses the database components.

   b. The secondary ACS stops its authentication service and replaces its database components with the database components that it received from the primary ACS. During this step, if AAA clients are configured properly, those that usually use the secondary ACS fail over to another ACS.

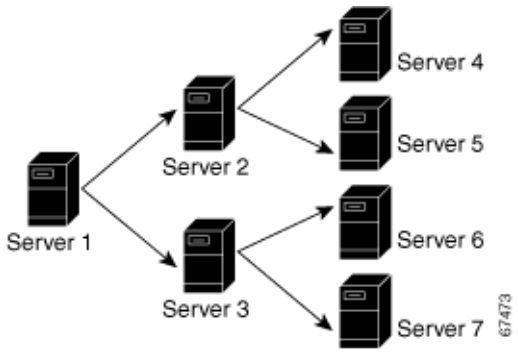
   c. The secondary ACS resumes its authentication service.

ACS can act as a primary ACS and a secondary ACS. Figure 9-1 shows a cascading replication scenario. Server 1 acts only as a primary ACS, replicating to servers 2 and 3, which act as secondary ACSs. After replication from server 1 to server 2 has completed, server 2 acts as a primary ACS while replicating to servers 4 and 5. Similarly, server 3 acts as a primary ACS while replicating to servers 6 and 7.

Note If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. In Figure 9-1, server 1 must have an entry in its AAA Servers table for each of the other six ACSs. If this is not done, after replication, servers 2 and 3 do not have servers 4 through 7 in their AAA Servers tables and replication will fail.

If server 2 were configured to replicate to server 1 in addition to receiving replication from server 1, replication to server 2 would fail. ACS cannot support such a configuration, known as bidirectional replication. To safeguard against this, a secondary ACS aborts replication when its primary ACS appears on its Replication list.

Figure 9-1 Cascading Database Replication



Replication Frequency

The frequency with which your ACSs replicate can have important implications for overall AAA performance. With shorter replication frequencies, a secondary ACS is more up to date with the primary ACS. This frequency produces a more current secondary ACS if the primary ACS fails.

Frequent replicaations incur a cost. The more frequent the replication, the higher the load on a multi-ACS architecture and your network environment. If you schedule frequent replications, network traffic is much higher. Also, processing load on the replicating systems is increased. Replication consumes system resources and briefly interrupts authentication; thus the more often replication occurs, the greater the impact on the AAA performance of the ACS. And because service is momentarily interrupted on both servers, NAS failovers can occur.

Note Regardless of how frequently replication is scheduled to occur, it only occurs when the database of the primary ACS has changed since the last successful replication.

This issue is more apparent with databases that are large or frequently change. Database replication is a nonincremental, destructive backup. In other words, it completely replaces the database and configuration on the secondary ACS every time it runs. Therefore, a large database results in substantial amounts of data being transferred, and the processing overhead can also be large.

Important Implementation Considerations

Several important points to consider when you implement the ACS Database Replication feature are:

- ACS only supports database replication to other ACSs. All ACSs participating in ACS internal database replication must run the same version of ACS. We strongly recommend that ACSs that are involved in replication use the same patch level, too.
- You must ensure correct configuration of the AAA Servers table in all ACSs that are involved in replication.
  - In its AAA Servers table, a primary ACS must have an accurately configured entry for each secondary ACS.

    Note If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from that primary ACS. For example, if the primary ACS replicates to two secondary ACSs, which, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.

  - In its AAA Servers table, a secondary ACS must have an accurately configured entry for each of its primary ACSs.
  - On a primary ACS and all its secondary ACSs, the AAA Servers table entries for the primary ACS must have identical shared secrets.
- Only suitably configured, valid ACSs can be secondary ACSs. To configure a secondary ACS for database replication, see Configuring a Secondary ACS, page 9-11.

- Replication only occurs when the database of the primary ACS has changed since the last successful replication, regardless of how frequently replication is scheduled to occur. When a scheduled or manually started replication begins, the primary ACS automatically aborts replication if its database has not changed since the last successful replication.

Tip You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

- Replication to secondary ACSs occurs sequentially in the order listed in the Replication list under Replication Partners on the ACS Database Replication page.
- You must configure a secondary ACS that is receiving replicated components to accept database replication from the primary ACS. To configure a secondary ACS for database replication, see Configuring a Secondary ACS, page 9-11.
- ACS does not support bidirectional database replication. The secondary ACS that receives the replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.
- For all components (except for Network Access Profiles), if you replicate user accounts, encusre that you name external database configurations identically on primary and secondary ACSs. A replicated user account retains its association with the database that is assigned to provide authentication or posture validation service, regardless of whether a database configuration of the same name exists on the secondary ACS. For example, if user account is associated with a database named **WestCoast LDAP**; on the primary ACS, the replicated user account on all secondary ACSs remains associated with an external user database named **WestCoast LDAP** even if you have not configured an LDAP database instance of that name.
- For all components (except for Network Access Profiles), in order to replicate user and group settings that use user-defined RADIUS vendor and VSAs, you must manually add the user-defined RADIUS vendor and VSA definitions on primary and secondary ACSs, ensuring that the RADIUS vendor slots that the user-defined RADIUS vendors occupy are identical on each ACS. After you have done so, replication of settings by using user-defined RADIUS vendors and VSAs is supported. For more information about user-defined RADIUS vendors and VSAs, see Custom RADIUS Vendors and VSAs, page 9-19.

Database Replication Versus Database Backup

Do not confuse database replication with system backup. Database replication does *not* replace System Backup. While both features protect against partial or complete server loss, each feature addresses the issue in a different way:

- System Backup archives data into a format that you can later use to restore the configuration if the system fails or the data becomes corrupted. The backup data is stored on the local hard drive, and can be copied and removed from the system for long-term storage. You can store several generations of database backup files.
- You use ACS Database Replication to copy various components of the ACS internal database to other ACSs. This method can help you plan a failover AAA architecture, and reduce the complexity of your configuration and maintenance tasks. While unlikely, it is possible that ACS Database Replication can propagate a corrupted database to the ACSs that generate your backup files.

Caution Because the possibility of replicating a corrupted database always exists, we strongly recommend that you implement a backup plan, especially in mission-critical environments. For more information about backing up the ACS internal database, see ACS Backup, page 8-7 and Appendix D, "CSUtil Database Utility".

Database Replication Logging

ACS logs all replication events—regardless of whether they are successful—in two files. The:

- Windows Event Log
- Database Replication report

To view the Windows Event Log, use the Windows administration utilities. You can view recent reports in the Reports and Activity section of ACS.

For more information about ACS reports, see Chapter 1, "Overview".

Replication Options

The ACS web interface provides three sets of options for configuring ACS Database Replication.

This section contains the following topics:

- Replication Components Options, page 9-7
- Outbound Replication Options, page 9-9
- Inbound Replication Options, page 9-10

Replication Components Options

You can specify the ACS internal database components that an ACS sends as a primary ACS and the components that it receives as a secondary ACS.

For increased security, you might want to have one ACS always be the sender and the other ACSs always be the receivers. You can use this method to ensure that all your ACSs are configured identically.

Note The ACS internal database components that a secondary ACS receives *overwrite* the ACS internal database components on the secondary ACS. Any information that is unique to the overwritten database component is lost. For example, if the Receive checkbox is selected for the User and Group Database, any existing user or group records are lost on replication when the new ACS internal database is received.

Table 9-1 describes the Replication Components table on the ACS Database Replication page and describes the component options that are replicated.

Table 9-1 Replication Component Descriptions

Component	What Gets Replicated?
User and group database	Groups and users. Using this option excludes the use of the Group database only option.
Group database only	Groups, but not for users. Using this option excludes the use of the User and group database option.
Network Configuration Device tables[1]	AAA Servers tables and the AAA Clients tables in the Network Configuration section. This also controls whether Network Device Groups (NDG) are replicated.
Distribution table	Proxy Distribution Table in the Network Configuration section.
Interface configuration	Advanced Options settings, RADIUS settings, and TACACS+ settings from the Interface Configuration section.
Interface security settings	Administrators and security information for the ACS web interface.
Password validation settings	Password validation settings.
EAP-FAST master keys and policies	Active and retired master keys and policies for EAP-FAST.
Network Access Profiles[2]	A collaboration of configuration settings. These include: Network Access Profiles, Posture Validation settings, AAA clients and hosts, external user database configuration, global authentication configuration, NDGs, user-defined RADIUS dictionaries, shared profile components and additional logging attributes.

1. If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. For example, if the primary ACS replicates to two secondary ACSs that, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.
2. Replication of Network Access Profiles contradicts the replication of Network Configuration Device tables, therefore do not check both of these components at the same time. NAP settings will override all other settings. Dynamically-mapped users are not replicated, only statically-added users are replicated.

If mirroring the entire database might send confidential information to the secondary ACS, such as the Proxy Distribution Table, you can configure the primary ACS to send only a specific category of database information.

Outbound Replication Options

In the Outbound Replication table on the ACS Database Replication page, you can schedule outbound replication and specify the secondary ACSs for this primary ACS.

Table 9-2 Outbound Replication Options

Option	Description
Scheduling Options	
Manually	ACS does not perform automatic database replication.
Automatically Triggered Cascade[1]	ACS performs database replication to the configured list of secondary ACSs when database replication from a primary ACS completes. You use this option to build a propagation hierarchy of ACS, relieving a primary ACS from the burden of propagating the replicated components to every other ACS. For an illustration of cascade replication, see Figure 9-1.
Every X minutes	ACS performs, on a set frequency, database replication to the configured list of secondary ACSs. The unit of measurement is minutes, with a default update frequency of 60 minutes.
At specific times	ACS performs, at the time that is specified in the day and hour graph, database replication to the configured list of secondary ACSs. The minimum interval is one hour, and the replication occurs on the hour selected.
Partner Options	You can specify the secondary ACSs for this primary ACS. The options that control the secondary ACSs to which a primary ACS replicates appear in the Partners section of the Outbound Replication table.
AAA Server	Represents the secondary ACSs that this primary ACS *does not* send replicated components to.
Replication	Represents the secondary ACSs that this primary ACS *does* send replicated components to.
Replication Timeout	Specifies the number of minutes that this primary ACS continues replicating to a secondary ACS. When the timeout value is exceeded, ACS terminates replication to the secondary ACS is was attempting to replicate to and then it restarts the CSAuth service. The replication timeout feature helps prevent loss of AAA services due to stalled replication communication, which can occur when the network connection between the primary and secondary ACS is abnormally slow or when a fault occurs within either ACS. The default value is five minutes.

1. If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. For example, if the primary ACS replicates to two secondary ACSs which, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.

The items in the AAA Server and Replication lists reflect the AAA servers configured in the AAA Servers table in Network Configuration. To make a particular ACS available as a secondary ACS, you must first add that ACS to the AAA Servers table of the primary ACS.

Tip The size of the components replicated affects the time required for replication. For example, replicating a user database containing 80,000 user profiles takes more time than replicating a user database containing 500 user profiles. You may need to monitor successful replication events to determine a reasonable timeout value for your implementation.

ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.

Inbound Replication Options

You can specify the primary ACSs from which a secondary ACS accepts replication. This option appears in the Inbound Replication table on the ACS Database Replication page.

The **Accept replication from** list controls which ACSs the current ACS does accept replicated components from. The list contains:

- **Any Known ACS Server**—If this option is selected, ACS accepts replicated components from any ACS configured in the AAA Servers table in Network Configuration.
- **Other AAA servers**—The list displays all the AAA servers configured in the AAA Servers table in Network Configuration. If a specific AAA server name is selected, ACS accepts replicated components only from the ACS specified.

Note ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.

For more information about the AAA Servers table in Network Configuration, see AAA Server Configuration, page 4-15.

Implementing Primary and Secondary Replication Setups on ACSs

If you implement a replication scheme that uses cascading replication, the ACS configured to replicate only when it has received replicated components from another ACS acts as a primary ACS and as a secondary ACS. First, it acts as a secondary ACS while it receives replicated components, and then it acts as a primary ACS while it replicates components to other ACSs. For an illustration of cascade replication, see Figure 9-1.

To implement primary and secondary replication setups on ACSs:

Step 1 On each secondary ACS:

a. In the Network Configuration section, add the primary ACS to the AAA Servers table.

   For more information about adding entries to the AAA Servers table, see AAA Server Configuration, page 4-15.

b. Configure the secondary ACS to receive replicated components. For instructions, see Configuring a Secondary ACS, page 9-11.

Step 2 On the primary ACS:

a. In the Network Configuration section, add each secondary ACS to the AAA Servers table.

Note If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. For example, if the primary ACS replicates to two secondary ACSs which, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.

For more information about adding entries to the AAA Servers table, see AAA Server Configuration, page 4-15.

b. If you want to replicate according to a schedule, at intervals, or whenever the primary ACS has received replicated components from another ACS, see Scheduling Replication, page 9-14.

c. If you want to initiate replication immediately, see Replicating Immediately, page 9-12.

Configuring a Secondary ACS

Note If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **ACS Database Replication** check box. Check the **Distributed System Settings** check box if not already selected.

The ACS Database Replication feature requires that you configure specific ACSs to act as secondary ACSs. The components that a secondary ACS is to receive must be explicitly specified, as must be its primary ACS.

Replication is always initiated by the primary ACS. For more information about sending replication components, see Replicating Immediately, page 9-12 or Scheduling Replication, page 9-14.

Caution The ACS internal database components received by a secondary ACS *overwrite* the ACS internal database components on the secondary ACS. Any information unique to the overwritten database component is lost.

Before You Begin

Ensure correct configuration of the AAA Servers table in the secondary ACS. This secondary ACS must have an entry in its AAA Servers table for each of its primary ACSs. Also, the AAA Servers table entry for each primary ACS must have the same shared secret that the primary ACS has for its own entry in its AAA Servers table. For more information about the AAA Servers table, see AAA Server Configuration, page 4-15.

To configure an ACS to be a secondary ACS:

Step 1 Log in to the web interface on the secondary ACS.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **Database Replication**.

The Database Replication Setup page appears.

Step 4 In the Replication Components table, select the **Receive** check box for each database component to be received from a primary ACS.

For more information about replication components, see Replication Components Options, page 9-7.

Step 5 Make sure that no ACS that the secondary ACS is to receive replicated components from is included in the Replication list. If so, select the primary ACS in the Replication list and click the **<--** (left arrow) to move it to the AAA Servers list.

Note ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it aborts replication.

Step 6 If the secondary ACS is to receive replication components from *only one* primary ACS, from the Accept replication from list, select the name of the primary ACS.

The primary ACSs available in the Accept replication from list are determined by the AAA Servers table in the Network Configuration section. For more information about the AAA Servers table, see AAA Server Configuration, page 4-15.

Note On the primary ACS and all secondary ACSs, the AAA Servers table entries for the primary ACS must have identical shared secrets.

Step 7 If the secondary ACS is to receive replication components from *more than one* primary ACS, from the Accept replication from list, select **Any Known ACS Server**.

The Any Known ACS Server option is limited to the ACSs listed in the AAA Servers table in Network Configuration.

Note For each primary ACS for this secondary ACS, on the primary and secondary ACS, the AAA Servers table entries for the primary ACS must have identical shared secrets.

Step 8 Click **Submit**.

ACS saves the replication configuration, and at the frequency or times that you specified, ACS begins accepting the replicated components from the other ACSs you specified.

Replicating Immediately

You can manually start database replication.

Note Replication cannot occur until you have configured at least one secondary ACS. For more information about configuring a secondary ACS, see Configuring a Secondary ACS, page 9-11.

Before You Begin

Ensure correct configuration of the primary and secondary ACSs. For detailed steps, see Implementing Primary and Secondary Replication Setups on ACSs, page 9-10.

For each secondary ACS that this ACS is to send replicated components to, make sure that you have completed the steps in Configuring a Secondary ACS, page 9-11.

To initiate database replication immediately:

Step 1 Log in to the web interface on the primary ACS.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **Database Replication**.

Note If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **ACS Database Replication** check box. Check the **Distributed System Settings** check box if not already selected.

The Database Replication Setup page appears.

Step 4 For each ACS internal database component you want to replicate to a secondary ACS, under Replication Components, select the corresponding **Send** check box.

Step 5 For each secondary ACS that you want the primary ACS to replicate its select components to, select the secondary ACS from the AAA Servers list, and then click **-->** (right arrow button).

Tip If you want to remove a secondary ACSs from the Replication list, select the secondary ACS in the Replication list, and then click **<--** (left arrow button).

Note ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.

Step 6 In the **Replication timeout** text box, specify how long this ACS will perform replication to each of its secondary ACS before terminating the replication attempt and restarting the CSAuth service.

Step 7 At the bottom of the browser window, click **Replicate Now**.

ACS saves the replication configuration. ACS immediately begins sending replicated database components to the secondary ACSs you specified.

Note Replication only occurs when the database of the primary ACS has changed since the last successful replication. You can force replication to occur by making one change to a user or group profile, such as changing a password or RADIUS attribute.

Scheduling Replication

You can schedule when a primary ACS sends its replicated database components to a secondary ACS. For more information about replication scheduling options, see Outbound Replication Options, page 9-9.

Note Replication cannot occur until the secondary ACSs are configured properly. For more information, see Configuring a Secondary ACS, page 9-11.

Before You Begin

Ensure correct configuration of the primary and secondary ACSs. For detailed steps, see Implementing Primary and Secondary Replication Setups on ACSs, page 9-10.

For each secondary ACS of this primary ACS, ensure that you have completed the steps in Configuring a Secondary ACS, page 9-11.

To schedule when a primary ACS replicates to its secondary ACSs:

Step 1 Log in to the web interface on the primary ACS.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **ACS Database Replication**.

Note If this feature does not appear, choose **Interface Configuration > click Advanced Options**. Then, check the **ACS Database Replication** check box. Check the **Distributed System Settings** check box if not already selected.

The Database Replication Setup page appears.

Step 4 To specify which ACS internal database components the primary ACS should send to its secondary ACSs, under Replication Components, select the corresponding **Send** check box for each database component to be sent.

For more information about replicated database components, see Replication Components Options, page 9-7.

Step 5 To have the primary ACS send replicated database components to its secondary ACSs at regular intervals, under Replication Scheduling, select the **Every** *X* **minutes** option and in the *X* box type the length of the interval at which ACS should perform replication (up to 7 characters).

Note Because ACS is momentarily shut down during replication, a short replication interval may cause frequent failover of your AAA clients to other ACSs. If AAA clients are not configured to failover to other ACSs, the brief interruption in authentication service may prevent users from authenticating. For more information, see Replication Frequency, page 9-5.

Step 6 If you want to schedule times at which the primary ACS sends its replicated database components to its secondary ACSs:

a. In the Outbound Replication table, select the **At specific times** option.

b. In the day and hour graph, click the times at which you want ACS to perform replication.

Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 7 If you want to have this ACS send replicated database components immediately on receiving replicated database components from another ACS, select the **Automatically triggered cascade** option.

Note If you specify the Automatically triggered cascade option, you must configure another ACS to act as a primary ACS to this ACS; otherwise, this ACS never replicates to its secondary ACSs.

Step 8 You must specify the secondary ACSs that this ACS should replicate to. To do so:

Note ACS does not support bidirectional database replication. A secondary ACS receiving replicated database components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated database components. If so, it rejects the components. For more information about replication partners, see Inbound Replication Options, page 9-10.

a. In the Outbound Replication table, from the AAA Servers list, select the name of a secondary ACS to which you want the primary ACS to send its selected replicated database components.

Note The AAA Servers table in Network Configuration determines which secondary ACSs are available in the AAA Servers list. For more information about the AAA Servers table, see AAA Server Configuration, page 4-15.

b. Click **-->** (right arrow button).

The selected secondary ACS moves to the Replication list.

c. Repeat Step a and Step b for each secondary ACS to which you want the primary ACS to send its selected replicated database components.

Step 9 In the **Replication timeout** text box, specify how long this ACS will perform replication to each of its secondary ACS before terminating the replication attempt and restarting the CSAuth service.

Step 10 Click **Submit**.

ACS saves the replication configuration you created.

Disabling ACS Database Replication

You can disable scheduled ACS database replications without losing the schedule itself. This allows you to cease scheduled replications temporarily and later resume them without having to re-enter the schedule information.

To disable ACS database replication:

Step 1 Log in to the web interface on the primary ACS.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **Database Replication**.

The Database Replication Setup page appears.

Step 4 In the Replication Components table, clear all check boxes.

Step 5 In the Outbound Replication table, select the **Manually** option.

Step 6 Click **Submit**.

ACS does not permit any replication to or from this ACS server.

Configuring Automatic Change Password Replication

To configure automatic change password replication and other local password management options:

Step 1 Log in to the web interface on the primary ACS.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **Local Password Management**.

Step 4 Select the options to configure:

Field	Description
Password Validation Options	• Character length • May not contain username • Different from previous value • Alphanumeric
Remote Change Password	• Disable Telnet password on this ACS and return desired message to users Telnet session. • Upon remote password change, immediately propagate the change to selected replication partners.
Password Change Log File Management	• Set frequency to generate new password change log file • Set log file deletion based on selected options

Step 5 Click **Submit**.

Database Replication Event Errors

The Database Replication report contains messages indicating errors that occur during replication. For more information about the Database Replication report, see ACS System Logs, page 11-8.

Tip Brief descriptions of errors are reported to the replication report, however sometimes more detailed errors are written to the CSAuth service log file, auth.log.

RDBMS Synchronization

This section provides information about the RDBMS Synchronization feature, including procedures for implementing this feature, within ACS and the external data source involved.

This section contains the following topics:

- About RDBMS Synchronization, page 9-17
  - Users, page 9-18
  - User Groups, page 9-18
  - Network Configuration, page 9-19
  - Custom RADIUS Vendors and VSAs, page 9-19
- RDBMS Synchronization Components, page 9-19
  - About CSDBSync, page 9-20
  - About the accountActions Table, page 9-20
- ACS Database Recovery Using the accountActions Table, page 9-21
- Reports and Event (Error) Handling, page 9-22
- Preparing to Use RDBMS Synchronization, page 9-22
- Configuring a System Data Source Name for RDBMS Synchronization, page 9-23
- RDBMS Synchronization Options, page 9-24
  - RDBMS Setup Options, page 9-24
  - Synchronization Scheduling Options, page 9-25
  - Synchronization Partners Options, page 9-25
- Performing RDBMS Synchronization Immediately, page 9-25
- Scheduling RDBMS Synchronization, page 9-26
- Disabling Scheduled RDBMS Synchronizations, page 9-28

About RDBMS Synchronization

The RDBMS Synchronization feature enables you to update the ACS internal database with information from an ODBC-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, ACS reads the file or database via the ODBC connection. You can also regard RDBMS Synchronization as an API—much of what you can configure for a user, group, or device through the ACS web interface, you can alternatively maintain through this feature. RDBMS Synchronization supports addition, modification, and deletion for all data items it can access.

You can configure synchronization to occur on a regular schedule. You can also perform synchronizations manually, updating the ACS internal database on demand.

Synchronization performed by a single ACS can update the internal databases of other ACSs, so that you only need configure RDBMS Synchronization on one ACS. ACSs listen on TCP port 2000 for synchronization data. RDBMS Synchronization communication between ACSs is encrypted using 128-bit encrypted, proprietary algorithm.

The topics in this section provide an overview of the kinds of configuration that RDBMS Synchronization can automate. You specify the actions in a relational database table or text file named accountActions. For more information about accountActions, see About the accountActions Table, page 9-20. For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

Users

Among the user-related configuration actions that RDBMS Synchronization can perform are:

- Adding users.
- Deleting users.
- Setting passwords.
- Setting user group memberships.
- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.
- Assigning IP addresses.
- Specifying outbound RADIUS attribute values.
- Specifying outbound TACACS+ attribute values.

Note For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

User Groups

Among the group-related configuration actions that RDBMS Synchronization can perform are:

- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.
- Specifying outbound RADIUS attribute values.
- Specifying outbound TACACS+ attribute values.

Note For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

Network Configuration

Among the network device-related configuration actions that RDBMS Synchronization can perform are:

- Adding AAA clients.
- Deleting AAA clients.
- Setting AAA client configuration details.
- Adding AAA servers.
- Deleting AAA servers.
- Setting AAA server configuration details.
- Adding and configuring Proxy Distribution Table entries.

Note For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

Custom RADIUS Vendors and VSAs

RDBMS Synchronization enables you to configure custom RADIUS vendors and VSAs. In addition to supporting a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), ACS supports RADIUS vendors and VSAs that you define. Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26.

You can define up to ten custom RADIUS vendors. ACS allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and by the vendor name.

Note If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary ACSs, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see ACS Internal Database Replication, page 9-1.

For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

RDBMS Synchronization Components

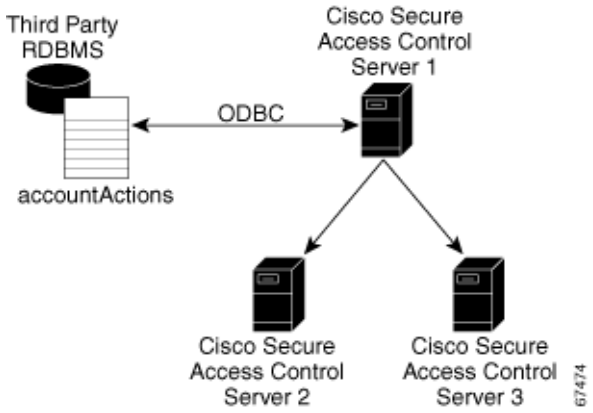
The RDBMS Synchronization feature comprises two components:

- **CSDBSync**—A dedicated Windows service that performs automated user and group account management services for ACS.
- **accountActions Table**—The data object that holds information used by CSDBSync to update the ACS internal database.

About CSDBSync

The CSDBSync service uses an ODBC system data source name (DSN) to access the accountActions table. See Figure 9-2. This service looks specifically for a table named **accountActions**. Synchronization events fail if CSDBSync cannot access the accountActions table.

Figure 9-2 RDBMS Synchronization



CSDBSync reads each record from the accountActions table and updates the ACS internal database as specified by the action code in the record. For example, a record could instruct CSDBSync to add a user or change a user password. In a distributed environment, a single ACS, known as the senior synchronization partner, accesses the accountActions table and sends synchronization commands to its synchronization partners. In Figure 9-2, Access Control Server 1 is the senior synchronization partner and the other two ACSs are its synchronization partners.

Note The senior synchronization partner must have AAA configurations for each ACS that is a synchronization partners. In turn, each of the synchronization partners must have a AAA server configuration for the senior partner. Synchronization commands from the senior partner are ignored if the ACS receiving the synchronization commands does not have a AAA server configuration for the senior partner.

CSDBSync reads and writes (deletes records) in the accountActions table. After CSDBSync processes each record, it deletes the record from the table. This requires that the database user account that you configure the system DSN to use must have read and write privileges.

For more information about CSDBSync or other Windows services used by ACS, see Chapter 1, "Overview".

About the accountActions Table

The accountActions table contains a set of rows that define actions CSDBSync is to perform in the ACS internal database. Each row in the accountActions table holds user, user group, or AAA client information. Each row also contains an action field and several other fields. These fields provide CSDBSync with the information it needs to update the ACS internal database. For full details of the accountActions table format and available actions, see Appendix F, "RDBMS Synchronization Import Definitions".

The database containing the accountActions table must support a multi-user ODBC driver. This is required to prevent problems if ACS and the third-party system attempt to access the accountActions table simultaneously.

ACS includes files to help you create your accountActions table for several common formats. You can find these files on the ACS in the following location, assuming a default installation of ACS:

C:\Program Files\CiscoSecure ACS vx.x\CSDBSync\Databases

The Databases directory contains the following subdirectories:

- **Access**—Contains the file `CiscoSecure Transactions.mdb`.

  The `CiscoSecure Transactions.mdb` database contains a preconfigured accountActions table. When you install ACS, the installation routine creates a system DSN named CiscoSecure DBSync. This system DSN is configured to communicate with `CiscoSecure Transactions.mdb`.

  Note By default, the username and password for the CiscoSecure Transactions.mdb database are set to null. To increase the security of RDBMS synchronizations performed using this database, change the username and password, in the CiscoSecure Transactions.mdb database and in ACS. Any other processes that access the CiscoSecure Transactions.mdb database should be changed to use the new username and password, too.

- **CSV**—Contains the files `accountactions` and `schema.ini`.

  The `accountactions` file is the accountActions table in a comma-separated value file. The `schema.ini` file provides the Microsoft ODBC text file driver with the information it needs to access the accountactions file.

- **Oracle 7**—Contains the files `accountActions.sql` and `testData.sql`.

  The `accountActions.sql` file contains the Oracle 7 SQL procedure needed to generate an accountActions table. The `testData.sql` file contains Oracle 7 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

- **Oracle 8**—Contains the files `accountActions.sql` and `testData.sql`.

  The `accountActions.sql` file contains the Oracle 8 SQL procedure needed to generate an accountActions table. The `testData.sql` file contains Oracle 8 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

- **SQL Server 6.5**—Contains the files `accountActions.sql` and `testData.sql`.

  The `accountActions.sql` file contains the Microsoft SQL Server 6.5 SQL procedure needed to generate an accountActions table. The `testData.sql` file contains Microsoft SQL Server 6.5 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

ACS Database Recovery Using the accountActions Table

Because the RDBMS Synchronization feature deletes each record in the accountActions table after processing the record, the accountActions table can be considered a transaction queue. The RDBMS Synchronization feature does not maintain a transaction log/audit trail. If a log is required, the external system that adds records to the accountActions table must create it. Unless the external system can recreate the entire transaction history in the accountActions table, we recommend that you construct a transaction log file for recovery purposes. To do this, create a second table that is stored in a safe location and backed up regularly. In that second table, mirror all the additions and updates to records in the accountActions table.

If the database is large, it is not practical to replay all transaction logs to synchronize the ACS internal database with the third-party system. Instead, you should create regular backups of the ACS internal database and replay the transaction logs from the time of most recent backup to resynchronize the ACS internal database with the third-party system. For information on creating backup files, see ACS Backup, page 8-7.

Replaying transaction logs that slightly predate the checkpoint does not damage the ACS internal database, although some transactions might be invalid and reported as errors. As long as the entire transaction log is replayed, the ACS internal database is consistent with the database of the external RDBMS application.

Reports and Event (Error) Handling

The CSDBSync service provides event and error logging. For more information about the RDBMS Synchronization log, see ACS System Logs, page 11-8. For more information about the CSDBSync service log, see Service Logs, page 11-23.

During manual synchronizations, ACS provides visual alerts to notify you of problems that occurred during synchronization.

Preparing to Use RDBMS Synchronization

Synchronizing the ACS internal database by using data from the accountActions table requires that you complete several steps that are external to ACS before you configure the RDBMS Synchronization feature within ACS. If you are planning to use a CSV file as your accountActions table, also see Configuring a System Data Source Name for RDBMS Synchronization, page 9-23.

Note The `schema.ini`. file must be located in the same folder as the `accountactions.csv` file.

To prepare to use RDBMS Synchronization:

Step 1 Determine where you want to create the accountActions table and in what format. For more information about the accountActions table, see About the accountActions Table, page 9-20. For details on the format and content of the accountActions table, see Appendix F, "RDBMS Synchronization Import Definitions".

Step 2 Create your accountActions table.

Step 3 Configure your third-party system to generate records and update the accountActions table with them. This effort will most likely involve creating stored procedures that write to the accountActions table at a triggered event; however, the mechanism for maintaining your accountActions table is unique to your implementation. If the third-party system that you are using to update the accountActions table is a commercial product, for assistance, refer to the documentation from your third-party system vendor.

For information about the format and content of the accountActions table, see Appendix F, "RDBMS Synchronization Import Definitions".

Step 4 Validate that your third-party system updates the accountActions table properly. Rows that are generated in the accountActions table must be valid. For details on the format and content of the accountActions table, see Appendix F, "RDBMS Synchronization Import Definitions".

Note After testing that the third-party system updates the accountActions table properly, discontinue updating the accountActions table until after you have completed Step 6 and Step 7.

Step 5 If you have a distributed AAA environment and want to synchronize multiple ACSs:

a. Determine which ACS you want to use to communicate with the third-party system. This ACS is the senior synchronization partner, which you will later configure to send synchronization data to its synchronization partners, which are the other ACSs needing synchronization.

b. On the senior synchronization partner, verify that there is a AAA server configuration for each synchronization partner. Add a AAA server configuration for each missing synchronization partner. For detailed steps about adding a AAA server, see Adding AAA Servers, page 4-16.

c. On all the other synchronization partners, verify that a AAA server configuration exists for the senior synchronization partner. If no AAA server configuration for the senior synchronization partner exists, create one. For detailed steps about adding a AAA server, see Adding AAA Servers, page 4-16.

Synchronization between the senior synchronization partner and the other synchronization partners is enabled.

Step 6 Set up a system DSN on the senior synchronization partner (the ACS that will communicate with the third-party system). For steps, see Configuring a System Data Source Name for RDBMS Synchronization, page 9-23.

Step 7 Schedule RDBMS synchronization on the senior synchronization partner. For steps, see Scheduling RDBMS Synchronization, page 9-26.

Step 8 Configure your third-party system to begin updating the accountActions table with information that will imported into the ACS internal database.

Step 9 Confirm that RDBMS synchronization is operating properly by monitoring the RDBMS Synchronization report in the Reports and Activity section. For more information about the RDBMS Synchronization log, see ACS System Logs, page 11-8.

Also, monitor the CSDBSync service log. For more information about the CSDBSync service log, see Service Logs, page 11-23.

Configuring a System Data Source Name for RDBMS Synchronization

On the ACS, a system DSN must exist for ACS to access the accountActions table. If you plan to use the `CiscoSecure Transactions.mdb` Microsoft Access database that is provided with ACS, you can use the `CiscoSecure DBSync` system DSN, rather than create one.

Tip Everything ACS does with ODBC requires System DSNs. User DSNs will not work. Confusing the two DSNs is an easy mistake to make when configuring the datasources in the ODBC control panel applet. Ensure your System DSN is set properly.

For more information about the `CiscoSecure Transactions.mdb` file, see Preparing to Use RDBMS Synchronization, page 9-22.

To create a system DSN for use with RDBMS synchronization:

Step 1 From Windows Control Panel, open the ODBC Data Source Administrator window.

Tip In Windows 2000 and new Microsoft operating systems, the ODBC Data Sources icon is located in the Administrative Tools folder.

Step 2 In the ODBC Data Source Administrator window, click the **System DSN** tab.

Step 3 Click **Add**.

Step 4 Select the driver to use with your new DSN, and then click **Finish**.

A dialog box displays fields requiring information that is specific to the selected ODBC driver.

Step 5 In the **Data Source Name** box, type a descriptive name for the DSN.

Step 6 Complete the other fields that the selected ODBC. These fields may include information such as the IP address of the server on which the ODBC-compliant database runs.

Step 7 Click **OK**.

The name that you assigned to the DSN appears in the System Data Sources list.

Step 8 Close the **ODBC** window and **Windows Control Panel**.

On your ACS, you create the system that ACS uses to access your accountActions table.

RDBMS Synchronization Options

The RDBMS Synchronization Setup page, which is available from System Configuration, provides control of the RDBMS Synchronization feature. It contains three tables whose options are described in this section.

This section contains the following topics:

- RDBMS Setup Options, page 9-24
- Synchronization Scheduling Options, page 9-25
- Synchronization Partners Options, page 9-25

RDBMS Setup Options

The RDBMS Setup table defines how ACS accesses the accountActions table. It contains:

- **Data Source**—Specifies which of all the system DSNs that are available on the ACS is used to access the accountActions table.
- **Username**—Specifies the username that ACS should use to access the database that contains the accountActions table.

Note The database user account that the username specifies must have sufficient privileges to read and write to the accountActions table.

- **Password**—Specifies the password that ACS uses to access the database that contains the accountActions table.

Synchronization Scheduling Options

The Synchronization Scheduling table defines when synchronization occurs. It contains:

- **Manually**—ACS does not perform automatic RDBMS synchronization.
- **Every *X* minutes**—ACS performs synchronization on a set frequency. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times**—ACS performs synchronization at the time that is specified in the day and hour graph. The minimum interval is one hour, and the synchronization occurs on the hour that you selected.

Synchronization Partners Options

The Synchronization Partners table defines which ACSs are synchronized with data from the accountActions table. It provides:

- **AAA Server**—This list represents the AAA servers that are configured in the AAA Servers table in Network Configuration for which the ACS *does not* perform RDBMS synchronization.
- **Synchronize**—This list represents the AAA servers that are configured in the AAA Servers table in Network Configuration for which the ACS *does* perform RDBMS synchronization. The AAA servers on this list are the synchronization partners of this ACS. During synchronization, communication between this ACS and its synchronization partners is 128-bit encrypted with a Cisco-proprietary protocol. The synchronization partners receive synchronization data on TCP port 2000.

Note Each synchronization partner *must* have a AAA server configuration in its Network Configuration section that corresponds to this ACS; otherwise, the synchronization commands this ACS sends to it are ignored.

For more information about the AAA Servers table in Network Configuration, see AAA Server Configuration, page 4-15.

Performing RDBMS Synchronization Immediately

You can manually start an RDBMS synchronization event.

To perform manual RDBMS synchronization:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

Note If this feature does not appear, click **Interface Configuration > Advanced Options**, then check **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

Step 3 To specify options in the RDBMS Setup table:

Note For more information about RDBMS setup, see RDBMS Setup Options, page 9-24.

a. From the Data Source list, select the system DSN that you configured to communicate with the database that contains your accountActions table.

   For more information about configuring a system DSN for use with RDBMS Synchronization, see Configuring a System Data Source Name for RDBMS Synchronization, page 9-23.

b. In the **Username** box, type the username for a database user account that has read-write access to the accountActions table.

c. In the **Password** box, type the password for the username that was specified in the Step b.

ACS has the information with which to access the accountActions table.

Note You do *not* have to select Manually under Replication Scheduling. For more information, see Disabling Scheduled RDBMS Synchronizations, page 9-28.

Step 4 For each ACS that you want this ACS to update with data from the accountActions table, select the ACS in the AAA Servers list, and then click **-->** (right arrow button).

The selected ACS appears in the Synchronize list.

Step 5 To remove ACSs from the Synchronize list, select the ACS in the Synchronize list, and then click **<--** (left arrow button).

The selected ACS appears in the AAA Servers list.

Step 6 At the bottom of the browser window, click **Synchronize Now**.

ACS immediately begins a synchronization event. To check the status of the synchronization, view the RDBMS Synchronization report in Reports and Activity.

Scheduling RDBMS Synchronization

You can schedule when an ACS performs RDBMS synchronization.

To schedule when an ACS performs RDBMS synchronization:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

Note If this feature does not appear, click **Interface Configuration > Advanced Options**, then click **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

Step 3 To specify options in the RDBMS Setup table:

Note For more information about RDBMS setup, see RDBMS Setup Options, page 9-24.

a. From the Data Source list, select the system DSN that you configured to communicate with the database that contains your accountActions table.

   For more information about configuring a system DSN for use with RDBMS Synchronization, see Configuring a System Data Source Name for RDBMS Synchronization, page 9-23.

b. In the **Username** box, type the username for a database user account that has read-write access to the accountActions table.

c. In the **Password** box, type the password for the username that was specified in the Step b.

Step 4 To have this ACS perform RDBMS synchronization at regular intervals, under Synchronization Scheduling, select the **Every *X* minutes** option and in the ***X*** box type the length of the interval in minutes at which ACS should perform synchronization (up to 7 characters).

Step 5 To schedule times at which this ACS performs RDBMS synchronization:

a. Under Synchronization Scheduling, select the **At specific times** option.

b. In the day and hour graph, click the times at which you want ACS to perform replication.

Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 6 For each ACS that you want to synchronize with data from the accountActions table:

Note For more information about synchronization targets, see Inbound Replication Options, page 9-10.

a. In the Synchronization Partners table, from the AAA Servers list, select the name of an ACS that you want this ACS to update with data from the accountActions table.

Note The AAA Servers table in Network Configuration determines which ACSs are available in the AAA Servers list, with the addition of the name of the current ACS server. For more information about the AAA Servers table, see AAA Server Configuration, page 4-15.

b. Click **-->** (right arrow button).

   The selected ACS moves to the Synchronize list.

Note At least one ACS must be in the Synchronize list. This includes the server on which you are configuring RDBMS Synchronization. RDBMS Synchronization does not automatically include the internal database of the current server.

Step 7 Click **Submit**.

ACS saves the RDBMS synchronization schedule that you created.

Disabling Scheduled RDBMS Synchronizations

You can disable scheduled RDBMS synchronization events without losing the schedule itself. You can use this ability to end scheduled synchronizations and resume them later without having to recreate the schedule.

To disable scheduled RDBMS synchronizations:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

Step 3 Under Synchronization Scheduling, select the **Manually** option.

Step 4 Click **Submit**.

ACS does not perform scheduled RDBMS synchronizations.

IP Pools Server

This section provides information about the IP Pools feature, including procedures for creating and maintaining IP pools.

This section contains the following topics:

- About IP Pools Server, page 9-28
- Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges, page 9-29
- Refreshing the AAA Server IP Pools Table, page 9-30
- Adding a New IP Pool, page 9-30
- Editing an IP Pool Definition, page 9-31
- Resetting an IP Pool, page 9-32
- Deleting an IP Pool, page 9-32

About IP Pools Server

If you are using VPNs you may have to overlap IP address assignments; that is, it may be advantageous for a PPTP tunnel client within a given tunnel to use the same IP address that another PPTP tunnel client in a different tunnel is using. You can use the IP Pools Server feature to assign the same IP address to multiple users, provided that the users are being tunnelled to different home gateways for routing beyond the boundaries of your own network. You can, therefore, conserve your IP address space without having

to resort to using illegal addresses. When you enable this feature, ACS dynamically issues IP addresses from the IP pools that you have defined by number or name. You can configure up to 999 IP pools, for approximately 255,000 users.

If you are using IP pooling and proxy, all accounting packets are proxied so that the ACS that is assigning the IP addresses can confirm whether an IP address is already in use.

Note The CiscoSecure Database Replication feature does not replicate IP pool definitions; however, user and group assignments to IP pools are replicated. By not replicating IP pool definitions, ACS avoids inadvertently assigning an IP address that a replication partner has already assigned to a different workstation. To support IP pools in a AAA environment that uses replication, you must manually configure each secondary ACS to have IP pools with names that are identical to the IP pools that are defined on the primary ACS.

To use IP pools, the AAA client must have network authorization (in IOS, **aaa authorization network**) and accounting (in IOS, **aaa accounting**) enabled.

Note To use the IP Pools feature, you must set up your AAA client to perform authentication and accounting by using the same protocol; TACACS+ or RADIUS.

For information on assigning a group or user to an IP pool, see Setting IP Address Assignment Method for a User Group, page 6-21 or Assigning a User to a Client IP Address, page 7-7.

Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges

ACS provides automated detection of overlapping pools.

Note To use overlapping pools, you must be using RADIUS with VPN, and you cannot be using the Dynamic Host Configuration Protocol (DHCP).

You can determine whether overlapping IP pools are allowed by checking which button appears below the AAA Server IP Pools table:

- **Allow Overlapping Pool Address Ranges**—Overlapping IP pool address ranges are *not allowed*. Clicking this button allows IP address ranges to overlap between pools.
- **Force Unique Pool Address Range**—Overlapping IP pool address ranges are *allowed*. Clicking this button prevents IP address ranges from overlapping between pools.

To allow overlapping IP pools or to force unique pool address ranges:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

Note If this feature does not appear, click **Interface Configuration > Advanced Options**, then click **IP Pools**.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 To allow overlapping IP pool address ranges:

a. If the **Allow Overlapping Pool Address Ranges** button appears, click it.

ACS allows overlapping IP pool address ranges.

b. If the **Force Unique Pool Address Range** button appears, do nothing.

ACS already allows overlapping IP pool address ranges.

Step 4 To deny overlapping IP pool address ranges:

a. If the **Allow Overlapping Pool Address Ranges** button appears, do nothing.

ACS already does not permit overlapping IP pool address ranges.

b. If the **Force Unique Pool Address Range** button appears, click it.

ACS does not permit overlapping IP pool address ranges.

Refreshing the AAA Server IP Pools Table

You can refresh the AAA Server IP Pools table to get the latest usage statistics for your IP pools.

To refresh the AAA Server IP Pools table:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click **Refresh**.

ACS updates the percentages of pooled addresses in use.

Adding a New IP Pool

You can define up to 999 IP address pools.

To add an IP pool:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools that you have already configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click **Add Entry**.

The New Pool table appears.

Step 4 In the **Name** box, type the name (up to 31 characters) to assign to the new IP pool.

Step 5 In the **Start Address** box, type the lowest IP address (up to 15 characters) of the range of addresses for the new pool.

Note All addresses in an IP pool must be on the same Class C network; so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.

Step 6 In the **End Address** box, type the highest IP address (up to 15 characters) of the range of addresses for the new pool.

Step 7 Click **Submit**.

The new IP pool appears in the AAA Server IP Pools table.

Editing an IP Pool Definition

To edit an IP pool definition:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click the name of the IP pool to edit.

The *name* pool table appears, where *name* is the name of the IP pool that you selected. The In Use field displays how many IP addresses in this pool are allocated to a user. The Available field displays how many IP addresses are unallocated to users.

Step 4 To change the name of the pool, in the **Name** box, type the name (up to 31 characters) to which to change the IP pool.

Step 5 To change the starting address of the pool range of IP addresses, in the **Start Address** box, type the lowest IP address (up to 15 characters) of the new range of addresses for the pool.

Note All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.

Step 6 To change the ending address of the pool range of IP addresses, in the **End Address** box, type the highest IP address (up to 15 characters) of the new range of addresses for the pool.

Step 7 Click **Submit**.

The edited IP pool appears in the AAA Server IP Pools table.

Resetting an IP Pool

The Reset function recovers IP addresses within an IP pool when there are dangling connections. A dangling connection occurs when a user disconnects and ACS does not receive an accounting stop packet from the applicable AAA client. If the Failed Attempts log in Reports and Activity shows a large number of `Failed to Allocate IP Address For User` messages, consider using the Reset function to reclaim all allocated addresses in this IP pool.

Note Using the Reset function to reclaim all allocated IP addresses in a pool can result in users being assigned addresses that are already in use.

To reset an IP pool and reclaim all its IP addresses:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click the name of the IP pool to reset.

The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays how many IP addresses in this pool are assigned to a user. The Available field displays how many IP addresses are not assigned to users.

Step 4 Click **Reset**.

ACS displays a dialog box indicating the possibility of assigning user addresses that are already in use.

Step 5 To continue resetting the IP pool, click **OK**.

The IP pool is reset. All its IP addresses are reclaimed. In the In Use column of the AAA Server IP Pools table, zero percent of the IP pool addresses are assigned to users.

Deleting an IP Pool

Note If you delete an IP pool that has users assigned to it, those users cannot authenticate until you edit the user profile and change their IP assignment settings. Alternatively, if the users receive their IP assignment based on group membership, you can edit the user group profile and change the IP assignment settings for the group.

To delete an IP pool:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click the name of the IP pool to delete.

The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use column displays how many IP addresses in this pool are assigned to a user. The Available column displays how many IP addresses are not assigned to users.

Step 4 Click **Delete**.

ACS displays a dialog box to confirm that you want to delete the IP pool.

Step 5 To delete the IP pool, click **OK**.

The IP pool is deleted. The AAA Server IP Pools table does not list the deleted IP pool.

IP Pools Address Recovery

You use the IP Pools Address Recovery feature to recover assigned IP addresses that have not been used for a specified period of time. You must configure an accounting network on the AAA client for ACS to reclaim the IP addresses correctly.

Enabling IP Pool Address Recovery

To enable IP pool address recovery:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Address Recovery**.

Note If this feature does not appear, click **Interface Configuration > Advanced Options**, then click **IP Pools**.

The IP Address Recovery page appears.

Step 3 Select the **Release address if allocated for longer than *X* hours** check box and in the ***X*** box type the number of hours (up to 4 characters) after which ACS should recover assigned, unused IP addresses.

Step 4 Click **Submit**.

ACS implements the IP pools address recovery settings you made.

CHAPTER 10

System Configuration: Authentication and Certificates

This chapter addresses authentication and certification features in the System Configuration section of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains the following topics:

- About Certification and EAP Protocols, page 10-1
- Global Authentication Setup, page 10-19
- ACS Certificate Setup, page 10-25

About Certification and EAP Protocols

ACS uses Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST), and Protected Extensible Authentication Protocol (PEAP) authentication protocols in combination with digital certification to ensure the protection and validity of authentication information. Digital certification, EAP-TLS, PEAP, EAP-FAST, and machine authentication are described in the topics that follow.

This section contains the following topics:

- Digital Certificates, page 10-1
- EAP-TLS Authentication, page 10-2
- PEAP Authentication, page 10-5
- EAP-FAST Authentication, page 10-8

Digital Certificates

You use the ACS Certificate Setup pages to install digital certificates to support EAP-TLS, EAP-FAST, and PEAP authentication, as well as to support Secure HyperText Transfer Protocol (HTTPS) protocol for secure access to the ACS web interface. ACS uses the X.509 v3 digital certificate standard. Certificate files must be in Base64-encoded X.509 format or Distinguished Encoding Rules (DER)-encoded binary X.509 format. Also, ACS supports manual certificate enrollment and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRL).

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 certification authority (CA) or, if you choose, may be a self-signed certificate. For more information, see Installing an ACS Server Certificate, page 10-25, and Using Self-Signed Certificates, page 10-32.

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.

EAP-TLS Authentication

This section contains the following topics:

- About the EAP-TLS Protocol, page 10-2
- EAP-TLS and ACS, page 10-3
- EAP-TLS Limitations, page 10-4
- Enabling EAP-TLS Authentication, page 10-4

About the EAP-TLS Protocol

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. The EAP-TLS authentication protocol uses the certificates of ACS and of the end-user client, enforcing mutual authentication of the client and ACS. For more detailed information on EAP, TLS, and EAP-TLS, refer to the following IETF RFCs: PPP Extensible Authentication Protocol (EAP) RFC 2284, The TLS Protocol RFC 2246, and PPP EAP TLS Authentication Protocol RFC 2716.

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 About Self-Signed Certificates, page 10-33.

EAP-TLS requires support from the end client and the Authentication, Authorization, and Accounting (AAA) client. An example of an EAP-TLS client includes the Microsoft Windows XP operating system.

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.

EAP-TLS and ACS

ACS supports EAP-TLS with any end-user client that supports EAP-TLS, such as Windows XP. To learn which user databases support EAP-TLS, see Authentication Protocol-Database Compatibility, page 1-7. For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a008009256b.shtml

ACS can use EAP-TLS to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol for user authentication to the same protocol that is used for machine authentication; that is, use of EAP-TLS for machine authentication may require the use of EAP-TLS for user authentication. For more information about machine authentication, see Machine Authentication, page 13-11.

ACS supports domain stripping for EAP-TLS authentication by using Windows Active Directory. For more information, see EAP-TLS Domain Stripping, page 13-10.

ACS also supports three methods of certificate comparison and a session resume feature. This topic discusses these features.

To permit user access to the network or computer authenticating with EAP-TLS, ACS must verify that the claimed identity (presented in the EAP Identity response) corresponds to the certificate that the user presents. ACS can accomplish this verification in three ways:

- **Certificate SAN Comparison**—Based on the name in the Subject Alternative Name field in the user certificate.
- **Certificate CN Comparison**—Based on the name in the Subject Common Name field in the user certificate.
- **Certificate Binary Comparison**—Based on a binary comparison between the user certificate in the user object in the LDAP server or Active Directory and the certificate that the user presents during EAP-TLS authentication. This comparison method cannot be used to authenticate users who are in an ODBC external user database.

Note If you use certificate binary comparison, the user certificate must be stored in a binary format. Also, for generic LDAP and Active Directory, the attribute that stores the certificate must be the standard LDAP attribute named **usercertificate**.

When you set up EAP-TLS, you can select the criterion (one, two, or all) that ACS uses. For more information, see Configuring Authentication Options, page 10-19.

ACS supports a session resume feature for EAP-TLS-authenticated user sessions, which is a particularly useful feature for WLANs, wherein a user may move the client computer to set a different wireless access point. When this feature is enabled, ACS caches the TLS session that is created during EAP-TLS authentication, provided that the user successfully authenticates. If a user needs to reconnect and the

original EAP-TLS session has not timed out, ACS uses the cached TLS session, resulting in faster EAP-TLS performance and lessened AAA server load. When ACS resumes an EAP-TLS session, the user reauthenticates by a secure sockets layer (SSL) handshake only, without a certificate comparison.

In effect, enabling an EAP-TLS session resume allows ACS to trust a user based on the cached TLS session from the original EAP-TLS authentication. Because ACS only caches a TLS session when a new EAP-TLS authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated in the number of minutes that the EAP-TLS session timeout option specified.

Note Session timeout is based on the time of the initial, full authentication of the session. It does not depend on an accounting start message.

The Session resume feature does not enforce changes to the group assignment in an external user database; because group mapping does not occur when a user session is resumed. Instead, the user is mapped to the same ACS group to which the user was mapped at the beginning of the session. At the start of a new session, group mapping enforces the new group assignment.

To force an EAP-TLS session to end before the session timeout is reached, you can restart the CSAuth service or delete the user from the ACS user database. Disabling or deleting the user in an external user database has no effect because the session resume feature does not involve the use of external user databases.

You can enable the EAP-TLS session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see Global Authentication Setup, page 10-19.

EAP-TLS Limitations

The limitations in the ACS implementation of EAP-TLS are:

- **Server and CA certificate file format**—If you install the ACS server and CA certificates from files, rather than from certificate storage, server and CA certificate files must be in Base64-encoded X.509 format or DER-encoded binary X.509 format.
- **LDAP attribute for binary comparison**—If you configure ACS to perform binary comparison of user certificates, the user certificate must be stored in the Active Directory or an LDAP server by using a binary format. Also, the attribute storing the certificate must be named **usercertificate**.
- **Windows server type**—If you want to use Active Directory to authenticate users with EAP-TLS when ACS runs on a member server, additional configuration is required. For more information, including steps for the additional configuration, see the *Installation Guide for Cisco Secure ACS for Windows*.

Enabling EAP-TLS Authentication

This explains the procedures that are required to configure ACS to support EAP-TLS authentication.

Note You must configure end-user client computers to support EAP-TLS. This procedure is specific to the configuration of ACS only. For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.htm.

Before You Begin

For EAP-TLS machine authentication, if you have configured a Microsoft certification authority server on the domain controller, you can configure a policy in Active Directory to produce a client certificate automatically when a computer is added to the domain. For more information, seethe Microsoft Knowledge Base.

To enable EAP-TLS authentication, follow these steps:

Step 1 Install a server certificate in ACS. EAP-TLS requires a server certificate. For detailed steps, see Installing an ACS Server Certificate, page 10-25.

Note If you have previously installed a certificate to support EAP-TLS, or PEAP user authentication, or to support HTTPS protection of remote ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based ACS services and remote administration; however, EAP-TLS, EAP-FAST and PEAP require that the certificate be suitable for server authentication purposes.

Step 2 Edit the certification trust list so that the CA issuing end-user client certificates is trusted. If you do not perform this step, ACS only trusts user certificates that were issued by the same CA that issued the certificate that is installed in ACS. For detailed steps, see Editing the Certificate Trust List, page 10-27.

Step 3 Establish a certificate revocation list (CRL) for each CA and certificate type in the certificate trust list (CTL). As part of EAP-TLS authentication, ACS validates the status of the certificate presented by the user against the cached CRL to ensure that it has not been revoked. For detailed steps, see Editing the Certificate Trust List, page 10-27.

Step 4 Enable EAP-TLS on the Global Authentication Setup page. In ACS, you complete this step only after you have successfully completed Step 1. For detailed steps, see Configuring Authentication Options, page 10-19.

Step 5 Configure a user database. To determine which user databases support EAP-TLS authentication, see Authentication Protocol-Database Compatibility, page 1-7.

ACS is ready to perform EAP-TLS authentication.

PEAP Authentication

This section contains the following topics:

- About the PEAP Protocol, page 10-5
- PEAP and ACS, page 10-6
- PEAP and the Unknown User Policy, page 10-7
- Enabling PEAP Authentication, page 10-7

About the PEAP Protocol

The PEAP protocol is a client-server security architecture that you use to encrypt EAP transactions; thereby protecting the contents of EAP authentications. lRSA, Cisco, and Microsoft have posted a PEAP IETF Internet Draft that is available at:

http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-05.txt.

PEAP authentications always involve two phases:

- In the first phase, 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.

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 phase one protects the EAP authentication. The authentication type that is negotiated during the second conversation may be any valid EAP type, such as EAP-GTC (for Generic Token Card). Because PEAP can support any EAP authentication protocol, individual combinations of PEAP and EAP protocols are denoted with the EAP protocol in parentheses, such as PEAP (EAP-GTC). For the authentication protocols that ACS supports in phase two of PEAP, see Authentication Protocol-Database Compatibility, page 1-7.

One improvement in security that PEAP offers is identity protection. This improvement is the potential of 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 Cisco Aironet PEAP client sends user identity through the SSL tunnel only. The initial identity, used in phase one and which is sent in the clear, is the MAC address of the end-user client with **PEAP_** as a prefix. The Microsoft PEAP client does not provide identity protection; the Microsoft PEAP client sends the username in clear text in phase one of PEAP authentication.

PEAP and ACS

ACS supports PEAP authentication by using the Cisco Aironet PEAP client or the Microsoft PEAP client that is included with Microsoft Windows XP Service Pack 1. ACS can support the Cisco Aironet PEAP client with PEAP(EAP-GTC) only. For the Microsoft PEAP client in the Windows XP Service Pack 1, ACS supports only PEAP(EAP-MS-CHAPv2). For information about which user databases support PEAP protocols, see Authentication Protocol-Database Compatibility, page 1-7.

When the end-user client is the Cisco Aironet PEAP client, and PEAP(EAP-GTC) and PEAP(EAP-MS-CHAPv2) are enabled on the Global Authentication Setup page, ACS first attempts PEAP(EAP-GTC) authentication with the end-user client. If the client rejects this protocol (by sending an EAP NAK message), ACS attempts authentication with PEAP(EAP-MS-CHAPv2). For more information about enabling EAP protocols that PEAP supports, see Global Authentication Setup, page 10-19.

ACS can use PEAP(EAP-MS-CHAPv2) to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol that is used for user authentication to the same protocol that is used for machine authentication; that is, use of PEAP for machine authentication requires the use of PEAP for user authentication. For more information about machine authentication, see Machine Authentication, page 13-11.

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 lessened AAA server load.

Note Session timeout is based on the time that authentication succeeds. It does not depend on accounting.

You can enable the PEAP session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see Global Authentication Setup, page 10-19.

ACS also supports a fast reconnect feature. When the session resume feature is enabled, the fast reconnect feature causes ACS to allow a PEAP session to resume without checking user credentials. In effect, ACS can trust a user based on the cached TLS session from the original PEAP authentication when this feature is enabled. Because ACS only caches a TLS session when phase two of PEAP authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated in the number of minutes that the PEAP session timeout option specifies.

The session resume feature does not enforce changes to group assignment in an external user database; group mapping does not occur when the session resume feature extends a user session. Instead, the user is mapped to the same ACS group that the user was mapped to at the beginning of the session. At the start of a new session, group mapping enforces the new group assignment.

The fast reconnect feature is particularly useful for wireless LANs, wherein a user may move the client computer so that a different wireless access point is in use. When ACS resumes a PEAP session, the user reauthenticates without entering a password, provided that the session has not timed out. If the end-user client is restarted, the user must enter a password; even if the session timeout interval has not ended.

You can enable the PEAP fast reconnect feature on the Global Authentication Setup page. For more information about enabling this feature, see Global Authentication Setup, page 10-19.

PEAP and the Unknown User Policy

During PEAP authentication, ACS might not know the real username to be authenticated until phase two of authentication. While the Microsoft PEAP client does reveal the actual username during phase one, the Cisco PEAP client does not; therefore, ACS does not attempt to look up the username that is presented during phase one and the use of the Unknown User Policy is irrelevant during phase one, regardless of the PEAP client used.

When phase two of PEAP authentication occurs and the username that the PEAP client presents is unknown to ACS, ACS processes the username in the same way that it processes usernames that are presented in other authentication protocols. If the username is unknown and the Unknown User Policy is disabled, authentication fails. If the username is unknown and the Unknown User Policy is enabled, ACS attempts to authenticate the PEAP user with unknown user processing.

For more information about unknown user processing, see About Unknown User Authentication, page 16-3.

Enabling PEAP Authentication

This procedure provides an overview of the detailed procedures that are required to configure ACS to support PEAP authentication.

Note You must configure end-user client computers to support PEAP. This procedure is specific to configuration of ACS only.

To enable PEAP authentication:

Step 1 Install a server certificate in ACS. PEAP requires a server certificate. For detailed steps, see Installing an ACS Server Certificate, page 10-25.

Note If you have previously installed a certificate to support EAP-TLS or PEAP user authentication, or to support HTTPS protection of remote ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based ACS services and remote administration; however, EAP-TLS and PEAP require that the certificate be suitable for server authentication purposes.

Step 2 Enable PEAP on the Global Authentication Setup page. You use ACS to complete this step only after you have successfully completed Step 1. For detailed steps, see Configuring Authentication Options, page 10-19.

Step 3 Configure a user database. To determine which user databases support PEAP authentication, see Authentication Protocol-Database Compatibility, page 1-7.

ACS is ready to perform PEAP authentication for most users. For more information, see PEAP and the Unknown User Policy, page 10-7.

Step 4 Consider enabling the Unknown User Policy to simplify PEAP authentication. For more information, see PEAP and the Unknown User Policy, page 10-7. For detailed steps, see Configuring the Unknown User Policy, page 16-8.

EAP-FAST Authentication

This section contains the following topics:

- About EAP-FAST, page 10-8
- About Master Keys, page 10-10
- About PACs, page 10-11
  - Automatic PAC Provisioning, page 10-13
  - Manual PAC Provisioning, page 10-14
- Master Key and PAC TTLs, page 10-15
- Replication and EAP-FAST, page 10-15
- Enabling EAP-FAST, page 10-17

About EAP-FAST

The EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol 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 significantly faster of the two solutions that provide encrypted EAP transactions. 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 PAC Provisioning, page 10-13.) 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. If EAP-MS-CHAPv2 authentication succeeds, ACS provides the user with a PAC. To determine which databases support EAP-FAST phase zero, see Authentication Protocol-Database Compatibility, page 1-7.

  Note Phase zero is optional and PACs can be manually provided to end-user clients. (See Manual PAC Provisioning, page 10-14.) You control whether ACS supports phase zero by checking the Allow automatic PAC provisioning check box in the Global Authentication Configuration page.

  The Allow anonymous in-band PAC provisioning option provisions an end-user client with a PAC by using EAP-FAST phase zero. If this check box is selected, 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-MS-CHAP will be used as inner method only.)

  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 and a trusted root CA on ACS.

  By default, ACS supports TLS server-side authentication; however, if the client sends the user certificate to ACS, mutual TLS authentication is performed and inner methods are bypassed.

  Phase zero of EAP-FAST does not enable a network service; therefore, even a successful EAP-FAST phase zero transaction is recorded in the ACS Failed Attempts log.

  If the Accept client on authenticated provisioning option is selected, ACS always sends an Access-Reject at the end of the provisioning phase (phase zero), forcing the client to reauthenticate by using the tunnel PAC. This option sends an Access-Accept to the client and can be enabled only when you check the Allow authenticated in-band PAC provisioning check box.

- **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 based on a master key that has not expired. The means by which PAC provisioning has occurred is irrelevant; you can use automatic or manual provisioning.

  No network service is enabled by phase one of EAP-FAST.

- **Phase two**—In phase two, ACS authenticates the user credentials with EAP-GTC, which is protected by the TLS tunnel that was created in phase one. TLS and MS-CHAP are supported as inner methods. No other EAP types are supported for EAP-FAST. To determine which databases support EAP-FAST phase two, see Authentication Protocol-Database Compatibility, page 1-7.

  ACS authorizes network service with a successful user authentication in phase two of EAP-FAST and logs the authentication in the Passed Authentications log, if it is enabled. Also, if necessary, ACS may refresh the end-user client PAC, which creates a second entry in the Passed Authentication log for the same phase two transaction.

Note This version of ACS supports EAP-FAST phase two for NAC phase two and is for wired clients only.

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. The Cisco Aironet EAP-FAST client protects the username in phase one by sending `FAST_`*MAC address* in place of the username. 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. For more information about password aging for Windows user databases, see Enabling Password Aging for Users in Windows Databases, page 6-19.

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 10-11.
- **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: the active master key or a retired master key.

To increase the security of EAP-FAST, ACS changes the master key that it uses to generate PACs. ACS uses time-to-live (TTL) values that you define to determine when it generates a new master key and the age of all master keys. Based on TTL values, ACS assigns master keys one of the these states:

- **Active**—An active master key is the master key used by ACS to generate PACs. The master key TTL setting determines the duration that a master key remains active. At any time, only one master key is active. When you define TTLs for master keys and PACs, ACS permits only a PAC TTL that is shorter than the active master key TTL. This limitation ensures that a PAC is refreshed at least once before the expiration of the master key used to generate the PAC, provided that EAP-FAST users log in to the network at least once before the master key expires. For more information about how TTL values determine whether PAC refreshing or provisioning is required, see Master Key and PAC TTLs, page 10-15.

  When you configure ACS to receive replicated EAP-FAST policies and master keys, a backup master key is among the master keys received. The backup master key is used only if the active master key retires before the next successful master key replication. If the backup master key also retires before the next successful master key replication, EAP-FAST authentication fails for all users requesting network access with EAP-FAST.

Tip If EAP-FAST authentication fails because the active and backup master keys have retired and ACS has not received new master keys in replication, you can force ACS to generate its own master keys by checking the **EAP-FAST Master Server** check box and clicking **Submit**.

  ACS records the generation of master keys in the logs for the CSAuth service.

- **Retired**—When a master key becomes older than the master key TTL settings, it is considered retired for the duration that the Retired master key TTL settings specify. ACS can store up to 255 retired master keys. While a retired master key is not used to generate new PACs, ACS needs it to authenticate PACs that were generated by using it. When you define TTLs for master keys and retired master keys, ACS permits only TTL settings that require storing 255 or fewer retired master

keys. For example, if the master key TTL is one hour and the retired master key TTL is four weeks, this would require storing up to 671 retired master keys; therefore, an error message appears and ACS does not allow these settings.

When a user gains network access by using a PAC that is generated with a retired master key, ACS provides the end-user client with a new PAC that the active master key generated. For more information about ACS master keys and PACs, see Master Key and PAC TTLs, page 10-15.

- **Expired**—When a master key becomes older than the sum of the master key TTL and retired master TTL settings, it is considered expired and ACS deletes it from its records of master keys. For example, if the master key TTL is one hour and the retired master key TTL is one week, a master key expires when it becomes greater than one week and one hour old.

  PACs that an expired master key cannot be used to access your network. An end-user client presenting a PAC that generated an expired master key requires a new PAC by using automatic or manual provisioning before phase one of EAP-FAST can succeed.

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 server's identify 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. ACS determines whether the PAC was generated using one of the master keys it is aware of: active or retired. (A PAC that is generated by using a master key that has since expired can never be used to gain network access.) When an end-user client has a PAC that is generated with an expired master key, the end-user client must receive a new PAC before EAP-FAST phase one can succeed. The means of providing PACs to end-user clients, known as PAC provisioning, are discussed in Automatic PAC Provisioning, page 10-13 and Manual PAC Provisioning, page 10-14.

After end-user clients are provided PACs, ACS refreshes them as that master key and PAC TTL values specify. ACS generates and sends a new PAC as needed at the end of phase two of EAP-FAST; however, if you shorten the master key TTL, you might require that PAC provisioning occur. For more information about how master key and PAC states determine whether ACS sends a new PAC to the end-user client at the end of phase two, see Master Key and PAC TTLs, page 10-15.

Regardless of the master key TTL values that you define, a user will require PAC provisioning when the user does not use EAP-FAST to access the network before the master key that generated the user's PAC has expired. For example, if the master key TTL is one week old and the retired master key TTL is one week old, each EAP-FAST end-user client used by someone who goes on vacation for two weeks will require PAC provisioning.

Provisioning Modes

ACS supports out-of-band and in-band provisioning modes. The in-band provisioning mode operates inside an Authenticated Diffie-HellmanKey Agreement Protocol (ADHP) tunnel before the peer authenticates the ACS server.

Since an unauthenticated server is provisioned, it is not possible to use a plain text password; so only MS-CHAP credentials can be used inside the tunnel. MS-CHAPv2 is used to prove the peer's identity and receives a PAC for further authentication sessions. This method minimizes the risk of exposing the user's credentials.

EAP-FAST has been enhanced to support an authenticated tunnel (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.

Since the server is authenticated as part of setting up the tunnel, weaker EAP methods, such EAP-GTC can be used inside the tunnel to provide supplicant authentication.

At the end of a provisioning session that uses an authenticated tunnel, network access can be granted; since the server and user have authenticated each other.

ACS supports the following EAP types inside the tunnel for provisioning:

- EAP-GTC
- EAP-MS-CHAPv2
- EAP-TLS

Types of PACs

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 PAC that have a wider contextual use.

The following types of PACs are provisioned to ACS, as per server policies:

- **Tunnel (Shared Secret) PAC, user or machine**—Distributed shared secret between the peer and ACS that is used to establish a secure tunnel and convey the policy of what must and can occur in the tunnel. The policy can include EAP methods, TLV exchanges, and identities that are allowed in the tunnel. It is up to the server policy to include what's necessary in PAC to enforce the policy in subsequent authentications that use the PAC. For example, in EAP-FAST Protocol Version 1, user identity I-ID is included as the part of the server policy. It limits the inner EAP methods to be carried only on the user identity that is provisioned. Other types of information can also be included, such as which EAP method and which cipher suite is allowed, for example. If the server policy is not included in the PAC, then no validation or limitation on the inner EAP methods or user identities inside the tunnel established by use of this PAC. The PAC user of machine contains a type field. The format for the machine will be **host/name of machine**.
- **User Authorization PAC**—Distributed user authentication and authorization result based on a previous authentication. You can use it a with combination of the Tunnel PAC to bypass subsequent user authentication. This result is intended to be short-lived and also controlled by the peer. If any state of the user has changed that will affect the user authentication result (for example, user has logged on or off), the peer should discard it and not use it again. You can use the User Authorization PACs in combination of Tunnel PAC to allow a stateless server session resume as described in Stateless Session Server Resume, page 10-18.

- **Posture PAC**—Distributed posture checking and authorization result based on a previous posture validation. You can use a posture PAC to optimize posture validation in the case of frequent revalidations. This result is specific to the posture validation application and may be used outside the contents of EAP-FAST.

The various means by which an end-user client can receive PACs are:

- **PAC provisioning**—Required when an end-user client has no PAC or has a PAC that is based on an expired master key. For more information about how master key and PAC states determine whether PAC provisioning is required, see Master Key and PAC TTLs, page 10-15.

  The two supported means of PAC provisioning are:

  - **Automatic provision**—Sends a PAC by using a secure network connection. For more information, see Automatic PAC Provisioning, page 10-13.
  - **Manual provision**—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 10-14.

- **PAC refresh**—Occurs automatically when EAP-FAST phase two authentication has succeeded, and master key and PAC TTLs dictate that the PAC must be refreshed. For more information about how master key and PAC states determine whether a PAC is refreshed, see Master Key and PAC TTLs, page 10-15.

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, provided that the master key that was used to generate it has not expired. Regardless of whether a PAC is active, if it is based on an expired master key, PAC provisioning must occur before EAP-FAST phase one can succeed.
- **Expired**—A PAC that is older than the PAC TTL is considered expired. Provided that the master key used to generate the PAC has not expired, an expired PAC can be used to complete EAP-FAST phase one and, at the end of EAP-FAST phase two, ACS will generate a new PAC for the user and provide it to the end-user client.

Automatic PAC Provisioning

Automatic PAC provisioning sends a new PAC to an end-user client over a secured network connection. Automatic PAC provisioning requires no intervention of the network user or a ACS administrator, provided that you configure ACS and the end-user client to support automatic provisioning.

EAP-FAST phase zero requires EAP-MS-CHAPv2 authentication of the user. At successful user authentication, ACS establishes a Diffie-Hellman tunnel with the end-user client. ACS generates a PAC for the user and sends it to the end-user client in this tunnel, along with the Authority ID and Authority ID information about this ACS.

Note Because EAP-FAST phase zero and phase two use different authentication methods (EAP-MS-CHAPv2 in phase zero versus EAP-GTC in phase two), some databases that support phase two cannot support phase zero. Given that ACS associates each user with a single user database, the use of automatic PAC provisioning requires that EAP-FAST users are authenticated with a database 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-Database Compatibility, page 1-7.

No network service is enabled by phase zero of EAP-FAST; therefore, ACS logs a EAP-FAST phase zero transaction in the Failed Attempts log, including an entry that PAC provisioning occurred. After the end-user client has received a PAC through a successful phase zero, it sends a new EAP-FAST request to begin phase one.

Note Because transmission of PACs in phase zero is secured by MS-CHAPv2 authentication and MS-CHAPv2 is vulnerable to dictionary attacks, we recommend that you limit use of automatic provisioning to initial deployment of EAP-FAST. After a large EAP-FAST deployment, PAC provisioning should be performed manually to ensure the highest security for PACs. For more information about manual PAC provisioning, see Manual PAC Provisioning, page 10-14.

To control whether ACS performs automatic PAC provisioning, you use the options on the Global Authentication Setup page in the System Configuration section. For more information, see Global Authentication Setup Page, page 10-20.

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. For example, if your EAP-FAST end-user client is the Cisco Aironet Client Utility (ACU), configuring the ACU to support EAP-FAST requires that you import a PAC file. For more information about configuring a Cisco ACU, see the applicable configuration guide for your ACU.

You can use manual PAC provisioning to control who can use EAP-FAST to access your network. If you disable automatic PAC provisioning, any EAP-FAST user denied a PAC cannot access the network. If your ACS deployment includes network segmentation, wherein access to each network segment is controlled by a separate ACS, 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.

Note Replicating EAP-FAST master keys and policies affects the ability to require different PACs per ACS. For more information, see Table 10-2.

While the administrative overhead of manual PAC provisioning is much greater than automatic PAC provisioning, it does not include the risk of sending the PAC over the network. When you first deploy EAP-FAST, using manual PAC provisioning would require a lot of manual configuration of end-user clients; however, this type of provisioning is the most secure means for distributing PACs. We recommend that, after a large EAP-FAST deployment, you should manually perform PAC provisioning to ensure the highest security for PACs.

You can generate PAC files for specific usernames, groups of users, lists of usernames, or all users. When you generate PAC files for groups of users or all users, the users must be known or discovered users and cannot be unknown users. ACS for Windows Server supports the generation of PAC files with `CSUtil.exe`. For more information about generating PACs with `CSUtil.exe`, see PAC File Generation, page D-25.

Master Key and PAC TTLs

The TTL values for master keys and PACs determine their states, as described in About Master Keys, page 10-10 and About PACs, page 10-11. master key and PAC states determine whether someone requesting network access with EAP-FAST requires PAC provisioning or PAC refreshing.

Table 10-1 summarizes ACS behavior with respect to PAC and master key states.

Table 10-1 Master Key versus PAC States

Master key state	PAC active	PAC expired
Master key active	Phase one succeeds. PAC is *not* refreshed at end of phase two.	Phase one succeeds. PAC is refreshed at end of phase two.
Master key retired	Phase one succeeds. PAC is refreshed at end of phase two.	Phase one succeeds. PAC is refreshed at end of phase two.
Master key expired	PAC provisioning is required. If automatic provisioning is *enabled*, phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC. If automatic provisioning is *disabled*, phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC.	PAC provisioning is required. If automatic provisioning is *enabled*, phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC. If automatic provisioning is *disabled*, phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC.

Replication and EAP-FAST

The Database Replication feature supports the replication of EAP-FAST settings, Authority ID, and master keys. Replication of EAP-FAST data occurs only if on the:

- Database Replication Setup page of the primary ACS, under Send, you have checked the EAP-FAST master keys and policies check box.
- Global Authentication Setup page of the primary ACS, you have enabled EAP-FAST and checked the EAP-FAST master server check box.
- Database Replication Setup page of the secondary ACS, under Receive, you have checked the EAP-FAST master keys and policies check box.
- Global Authentication Setup page of the secondary ACS, you have enabled EAP-FAST and unchecked the EAP-FAST master server check box.

EAP-FAST-related replication occurs for three events:

- **Generation of master keys**—A primary ACS sends newly generated active and backup master keys to secondary ACSs. This event occurs immediately after master key generation, provided that you configure the replication properly and it is not affected by replication scheduling on the Database Replication Setup page.
- **Manual replication**—All EAP-FAST components that can be replicated are replicated if you click **Replicate Now** on the Database Replication Setup page of the primary ACS. Some of the replicated components are configurable in the web interface. Table 10-2 shows whether an EAP-FAST component is replicated or configurable.

Note EAP-FAST replication is not included in scheduled replication events.

- **Changes to EAP-FAST settings**—If, on a primary ACS, you change any EAP-FAST configurable components that are replicated, ACS begins EAP-FAST replication. Whether an EAP-FAST component is replicated or configurable is detailed in Table 10-2.

The Database Replication log on the primary ACS records replication of master keys. Entries related to master key replication contain the text `MKEYReplicate`.

Table 10-2 EAP-FAST Components and Replication

EAP-FAST Component	Replicated?	Configurable?
EAP-FAST Enable	No	Yes, on the Global Authentication Setup page.
Master key TTL	Yes	Yes, on the Global Authentication Setup page.
Retired master key TTL	Yes	Yes, on the Global Authentication Setup page.
PAC TTL	Yes	Yes, on the Global Authentication Setup page.
Authority ID	Yes	No, generated by ACS.
Authority ID info	Yes	Yes, on the Global Authentication Setup page.
Client initial message	Yes	Yes, on the Global Authentication Setup page.
Master keys	Yes	No, generated by ACS when TTL settings dictate.
EAP-FAST master server	No	Yes, on the Global Authentication Setup page.
Actual EAP-FAST server status	No	No, determined by ACS.

The EAP-FAST master server setting has a significant effect on EAP-FAST authentication and replication:

- **Enabled**—When you check the EAP-FAST master server check box, the `Actual EAP-FAST server status` is `Master` and ACS ignores the EAP-FAST settings, Authority ID, and master keys it receives from a primary ACS during replication, preferring instead to use master keys that it generates, its unique Authority ID, and the EAP-FAST settings that are configured in its web interface.

  Enabling the EAP-FAST master server setting requires providing a PAC from the primary ACS that is different than the PAC from the secondary ACS for the end-user client. Because the primary and secondary ACSs send different Authority IDs at the beginning of the EAP-FAST transaction, the end-user client must have a PAC for each Authority ID. A PAC that the primary ACS generates is not accepted by the secondary ACS in a replication scheme where the EAP-FAST master server setting is enabled on the secondary ACS.

Tip In a replicated ACS environment, use the EAP-FAST master server feature in conjunction with disallowing automatic PAC provisioning to control EAP-FAST access to different segments of your network. Without automatic PAC provisioning, users must request PACs for each network segment.

- **Disabled**—When you do not check the EAP-FAST master server check box, ACS continues to operate as an EAP-FAST master server until the first time it receives replicated EAP-FAST components from the primary ACS. When `Actual EAP-FAST server status` displays the text `Slave`, ACS uses the EAP-FAST settings, Authority ID, and master keys that it receives from a primary ACS during replication; rather than using the master keys that it generates and its unique Authority ID.

Note When you uncheck the EAP-FAST master server check box, the `Actual EAP-FAST server status` remains `Master` until ACS receives replicated EAP-FAST components and then the `Actual EAP-FAST server status` changes to `Slave`. Until `Actual EAP-FAST server status` changes to `Slave`, ACS acts as a master EAP-FAST server by using master keys that it generates, its unique Authority ID, and the EAP-FAST settings that are configured in its web interface.

Disabling the EAP-FAST master server setting eliminates the need for providing a different PAC from the primary and secondary ACSs. This elimination occurs because the primary and secondary ACSs send the end-user client the same Authority ID at the beginning of the EAP-FAST transaction; therefore, the end-user client uses the same PAC in its response to either ACS. Also, a PAC that one ACS generated for a user in a replication scheme where the EAP-FAST master server setting is disabled is accepted by all other ACSs in the same replication scheme.

For more information about replication, see ACS Internal Database Replication, page 9-1.

Enabling EAP-FAST

This section explains the procedures to configure ACS to support EAP-FAST authentication.

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 PAC provisioning places different limits on user database support.

To enable ACS to perform EAP-FAST authentication:

Step 1 Configure a user database that supports EAP-FAST authentication. To determine which user databases support EAP-FAST authentication, see Authentication Protocol-Database Compatibility, page 1-7. For user database configuration, see Chapter 13, "User Databases."

Note User database support differs for EAP-FAST phase zero and phase two.

ACS supports use of the Unknown User Policy and group mapping with EAP-FAST, as well as password aging with Windows external user databases.

Step 2 Determine master key and PAC TTL values. While changing keys and PACs more frequently could be considered more secure, it also increases the likelihood that PAC provisioning will be needed for machines left offline so long that the PACs on them are based on expired master keys.

Also, if you reduce the TTL values with which you initially deploy EAP-FAST, you may force PAC provisioning to occur because users would be more likely to have PACs based on expired master keys.

For information about how master key and PAC TTL values determine whether PAC provisioning or PAC refreshing is required, see Master Key and PAC TTLs, page 10-15.

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 PAC Provisioning, page 10-13, and Manual PAC Provisioning, page 10-14.

Note We recommend that you limit the use of automatic PAC provisioning to initial deployments of EAP-FAST, followed by using 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 and Step 3, enable EAP-FAST on the Global Authentication Setup page. For detailed steps, see Configuring Authentication Options, page 10-19.

ACS is ready to perform EAP-FAST authentication.

Stateless Session Server Resume

To provide better support for server performance, load balancing and peer roaming to different servers, EAP-FAST supports the stateless-server session resume by using the short-lived Authorization PACs. Once a peer establishes a TLS session and is authenticated, the EAP server can provision it with a Tunnel PAC. The tunnel PAC can be used to establish a TLS session much more quickly than a normal TLS handshake. With the normal TLS session resume, the EAP server must maintain the TLS session cache, as well as the peer's authentication and authorization result. This storage requirement often hinders the server's performance, as well as introduces difficulties with server load balancing and peer roaming to different servers. The use of Tunnel PAC eliminates the server's need to maintain a TLS session cache. The TLS session can be quickly established in a fast and secure way; however, the server still has to cache the peer's previous authentication and authorization state for a quick session resume.

You can further optimize by using the User Authorization PAC in combination with the Tunnel PAC. The server generated key protects User Authorization PACs which store previous authentication and authorization states on the peer. If the peer has the authorization PACs corresponding to the EAP server connected (by matching A-ID), and detects no state change affecting the peer, the peer can piggyback the opaque part of these PACs in the PAC-TLV with Client TLS Finished as TLS application data, which the TLS cipher suite that is negotiated protects. This method prevents attackers from snooping the authorization PACs without introducing an extra round trip. Once the EAP server receives and decrypt the authorization PAC, the EAP server can recreate its previous state information based on the peer's authentication and authorization result. If the state information in these PACs is still valid, based on a server side policy, it might bypass one or all of the inner EAP method authentications. In case inner methods are bypassed, the EAP Server sends the Result TLV only without the Crypto-binding TLV, and the peer responds with Result TLV with Success. The EAP-Server may start a full sequence of EAP authentication or a partial sequence if one or all of the PACs are not present or accepted.

ACS supports the following inner methods and TLV exchange support combinations:

- EAP-MS-CHAP Authentication + Posture Validation TLV exchange
- EAP-GTC Authentication + Posture Validation TLV exchange
- EAP-TLS Authentication + Posture Validation TLV exchange
- Posture Validation TLV exchange without authentication

Global Authentication Setup

You use the Global Authentication Setup page to enable or disable some of the authentication protocols that ACS supports. You can also configure other options for some of the protocols on the Global Authentication Setup page.

This section contains the following topics:

- Configuring Authentication Options, page 10-19
- Global Authentication Setup Page, page 10-20

Caution Network Access Profile settings override the global authentication settings.

Configuring Authentication Options

Use this procedure to select and configure how ACS handles options for authentication. In particular, use this procedure to specify and configure the varieties of EAP that you allow, and to specify whether you allow MS-CHAP Version 1, MS-CHAP Version 2, or both.

For more information on the EAP-TLS Protocol, see EAP-TLS Authentication, page 10-2. For more information on the PEAP protocol, see PEAP Authentication, page 10-5. For more information on the PEAP protocol, see EAP-FAST Authentication, page 10-8. For details about how various databases support various password protocols, see Authentication Protocol-Database Compatibility, page 1-7.

You use the Global Authentication Setup Page to set up authentication configuration options.

Note If users access your network by using a AAA client that is defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, you must enable one or more of the LEAP, EAP-TLS, or EAP-FAST protocols on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

Before You Begin

For information about the options see the Global Authentication Setup Page, page 10-20.

To configure authentication options:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Global Authentication Setup**.

The Global Authentications page appears.

Step 3 Configure options, as applicable. For more information about the significance of the options, see Global Authentication Setup Page, page 10-20.

Step 4 If you want to immediately implement the settings that you have made, click **Submit + Restart**.

ACS restarts its services and implements the authentication configuration options that you selected.

Step 5 If you want to save the settings that you have made but implement them later, click **Submit**.

Tip You can restart ACS services at any time by using the Service Control page in the System Configuration section.

ACS saves the authentication configuration options that you selected.

Global Authentication Setup Page

This page contains:

Field	Description
PEAP	You can configure the following options for PEAP: • **Allow EAP-MSCHAPv2**—Whether ACS attempts EAP-MS-CHAPv2 authentication with PEAP clients. • **Allow EAP-GTC**—Whether ACS attempts EAP-GTC authentication with PEAP clients. **Note** If you check the Allow EAP-MS-CHAPv2 and the Allow EAP-GTC check boxes, ACS negotiates the EAP type with the end-user PEAP client. • **Allow Posture Validation**—To enable use of PEAP for posture validation of Network Admission Control (NAC) clients, check this check box. • **Cisco client initial message**—The message that you want to appear during PEAP authentication. The message that the PEAP client initially displays is the first challenge that a user of a Cisco Aironet PEAP client sees when attempting authentication. It should direct the user what to do next; for example, `Enter your message`. The message is limited to 40 characters. • **PEAP session timeout (minutes)**—The maximum PEAP session length to allow users, in minutes. A session timeout value that is greater than zero (0) enables the PEAP session resume feature, which caches the TLS session that was created in phase one of PEAP authentication. When a PEAP client reconnects, ACS uses the cached TLS session to restore the session, which improves PEAP performance. ACS deletes cached TLS sessions when they time out. The default timeout value is 120 minutes. To disable the session resume feature, set the timeout value to zero (0). • **Enable Fast Reconnect**—This option is related to MS CHAP only, and does not apply to EAP-GTC. If you want ACS to resume sessions for MS PEAP clients without performing phase two of MS PEAP authentication, check this check box. Unchecking this check box causes ACS to perform phase two of MS PEAP authentication, even when the PEAP session has not timed out. Fast recondition can occur only when ACS allows the session to resume because the session has not timed out. If you disable the PEAP session resume feature by entering zero (0) in the PEAP session timeout (minutes) box, checking the Enable Fast Reconnect check box has no effect on PEAP authentication and phase two of PEAP authentication always occurs.
EAP-FAST	**EAP-FAST Configuration**—Select to open the EAP-FAST Configuration Page. **Note** If you are using ACS to implement NAC, enable each option and then click **Submit**. When the page reappears, select EAP-FAST Configuration to open the EAP-FAST Settings page.

Field	Description
EAP-TLS	Check this box to use the EAP TLS Authentication protocol and configure 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 presented by the end-user client. This comparison occurs after an EAP-TLS tunnel is established between ACS and the end-user client. Select one of: **Note** EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps on the ACS Certificate Setup page. See Installing an ACS Server Certificate, page 10-25 for more information. Select one or more EAP-TLS comparison methods. If you select more than one comparison type, ACS performs the comparisons in the order listed. If the one comparison type fails, ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison. • **Certificate SAN comparison**—If you want ACS to verify user identity by comparing the name in the Subject Alternative Name field of the end-user certificate to the username in the applicable user database, check this check box. • **Certificate CN comparison**—If you want ACS to verify user identity by comparing the name in the Common Name field of the end-user certificate to the username in the applicable user database, check this check box. • **Certificate Binary comparison**—If you want ACS to verify user identity by doing a binary comparison of the end-user certificate to the user certificate stored in Active Directory, check this check box. EAP-TLS session timeout (minutes)—Enter a value in minutes for that defines the maximum time for the EAP-TLS session. ACS supports an EAP-TLS session resume feature that caches the TLS session created during a new EAP-TLS authentication. When an EAP-TLS client reconnects, the cached TLS session is used to restore the session without performing a certificate comparison, which improves EAP-TLS performance. ACS deletes cached TLS sessions when they time out. If ACS or the end-user client is restarted, certificate comparison is required even if the session timeout interval has not ended. To disable the session resume feature, set the timeout value to zero (0).
LEAP	The Allow LEAP (For Aironet only) check box controls whether ACS performs LEAP authentication. LEAP is currently used only for Cisco Aironet wireless networking. If you disable 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 on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.
EAP-MD5	To enable EAP-based Message Digest 5 hashed authentication, check this check box.

Field	Description
Allow EAP request timeout (seconds)	You use this option to instruct Cisco Aironet Access Points (APs) to use the specified timeout value during EAP conversations. The value that is specified must be the number of seconds after which Cisco Aironet APs should assume that an EAP transaction with ACS has been lost and should be restarted. A value of zero (0) disables this feature. During EAP conversations, ACS sends the value that is defined in the AP EAP request timeout box by using the IETF RADIUS Session-Timeout (27) attribute.
MS-CHAP Configuration	For RADIUS authentication, ACS supports MS-CHAP versions 1 and 2. You can configure whether ACS authenticates users with MS-CHAP when the AAA protocol is RADIUS and, if so, which versions it uses. To enable MS-CHAP in RADIUS-based authentication, check the check box corresponding to the MS-CHAP version that you want to use. To allow MS-CHAP to use either version, check both check boxes. To disable MS-CHAP in RADIUS-based authentication, clear both check boxes. **Note** For TACACS+, ACS supports only MS-CHAP version 1. TACACS+ support for MS-CHAP version 1 is always enabled and is not configurable.

EAP-FAST Configuration Page

This page contains:

Field	Description
Allow EAP-FAST	Whether ACS permits EAP-FAST authentication.
Active master key TTL	The duration that a master key is used to generate new PACs. Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) that is defined for the Master Key expires, the master key is considered retired and a new master key is generated.The default master key TTL is one month. Decreasing the master key TTL can cause retired master keys to expire because a master key expires when it is older than the sum of the master key TTL and the retired master key TTL; therefore, decreasing the master key TTL requires PAC provisioning for end-user clients with PACs that are based on the newly expired master keys. For more information about master keys, see About Master Keys, page 10-10.
Retired master key TTL	Enter a value for the amount of time that PACs that are generated by using a retired master key are acceptable for EAP-FAST authentication. When an end-user client gains network access by using a PAC that is based on a retired master key, ACS sends a new PAC to the end-user client. The default retired master key TTL is three months. **Note** Decreasing the retired master key TTL can cause retired master keys to expire; therefore, decreasing the retired master key TTL requires PAC provisioning for end-user clients with PACs based on the newly expired master keys.
Tunnel PAC TTL	The duration that a PAC is used before it expires and must be replaced. Enter a value for the amount of time that a PAC is used before it expires and must be replaced. If the master key that is used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC that expired, you must use automatic or manual provisioning to provide the end-user client with a new PAC. For more information about PACs, see About PACs, page 10-11.

Field	Description
Client initial display message	Specify a message to be sent to users who authenticate with an EAP-FAST client. Maximum length is 40 characters. A user will see the initial message only if the end-user client supports its display.
Authority ID Info	The textual identity of this ACS server, which an end user can user to determine which ACS server to be authenticated against. Filling in this field is mandatory.
Allow anonymous in-band PAC provisioning	ACS provisions an end-user client with a PAC by using EAP-FAST phase zero. If you check this check box, 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-MS-CHAP will be used as the only inner method in phase zero.
Allow authenticated in-band PAC provisioning	ACS provisions an end-user client with a PAC by using EAP-FAST phase zero with SSL server-side authentication. This option requires that a server certificate and a trusted root CA are installed on ACS. One of the allowed inner methods will then be used to authenticate the user. In addition, the client may send its certificate to the server, causing the mutual TLS authentication. In this case, ACS skips the inner methods and provisions the PAC.
Accept client on authenticated provisioning	This option is only available when the allow authenticated in-band PAC provisioning option is selected. The server always sends an Access-Reject at the end of the provisioning phase, forcing the client to reauthenticate using the tunnel PAC. This option enables ACS to send an Access-Accept to the client at the end of the provisioning phase.
Require client certificate for provisioning	Allows provisioning PACs based on certificates only. Other inner EAP methods for PAC provisioning are not allowed. If the client does not present its certificate during the first TLS handshake, the server initiates a TLS renegotiation. The renegotiation requests the client to start a new TLS handshake; the cipher that was negotiated in the first handshake protects it. During the second TLS handshake, the server requests the client 's certificate. If the certificate is not sent, the handshake fails and the user is denied access.
Allow Machine Authentication	ACS provisions an end-user client with a machine PAC and performs machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by 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 database or external databases. After these details are correctly verified, no further authentication is performed. **Note** After performing machine authentication and when the **Required** or **Posture Only** check boxes are checked, ACS also requests the posture credentials.
Machine PAC TTL	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).
Allow Stateless session resume	Uncheck this option: • If you do not want ACS to provision authorization PACs for EAP-FAST clients. • To always perform phase two of EAP-FAST.
Authorization PAC TTL	This option determines the expiration time of the user authorization PAC. When ACS receives an expired authorization PAC, Allow Stateless session resume fails and, therefore, phase two EAP-FAST authentication is performed.

Field	Description
Allowed inner methods	This option determines which inner EAP methods can run inside the EAP-FAST TLS tunnel. For anonymous in-band provisioning, you must enable EAP-GTC and EAP-MS-CHAP for backward compatibility. If you selected Allow anonymous in-band PAC provisioning, you must select EAP-MS-CHAP (phase zero) and EAP-GTC (phase two). If you selected Allow authenticated in-band PAC provisioning, the inner method in the authentication phase is negotiable. (EAP-GTC is used by default in phase zero.) Select one or more of the following inner methods: • **EAP-GTC**—To enable EAP-GTC in EAP FAST authentication, check this check box. • **EAP-MS-CHAPv2**—To enable EAP-MS-CHAPv2 in EAP FAST authentication, check this check box. • **EAP-TLS**—To enable EAP-TLS in EAP FAST authentication, check this check box. **Note** ACS always runs the first enabled EAP method. For example, if you select EAP-GTC and EAP-MS-CHAPv2, then the first enabled EAP method is EAP-GTC.
Select one or more of the following EAP-TLS comparison methods:	Select one or more EAP-TLS comparison methods. If you select more than one comparison type, ACS performs the comparisons in the order listed. If the one comparison type fails, ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison. • **Certificate SAN comparison**—Verifies user identity by comparing the name in the Subject Alternative Name field of the end-user certificate to the username in the applicable user database, check this check box. • **Certificate CN comparison**—Verifies user identity by comparing the name in the Common Name field of the end-user certificate to the username in the applicable user database, check this check box. • **Certificate Binary comparison**—Verifies user identity by doing a binary comparison of the end-user certificate to the user certificate stored in Active Directory, check this check box.
EAP-TLS session timeout (minutes)	EAP-TLS session timeout (minutes)—Enter a value in minutes that defines the maximum time for the EAP-TLS session. ACS supports an EAP-TLS session resume feature that caches the TLS session created during a new EAP-TLS authentication. When an EAP-TLS client reconnects, the cached TLS session is used to restore the session without performing a certificate comparison, which improves EAP-TLS performance. ACS deletes cached TLS sessions when they time out. If ACS or the end-user client is restarted, certificate comparison is required; even if the session timeout interval has not ended. To disable the session resume feature, set the timeout value to zero (0).
EAP-FAST Master Server	Select this check box to determine whether ACS creates its own master keys, and uses its own EAP-FAST settings and Authority ID; or, if it uses the EAP-FAST settings, master keys, and Authority ID received from another (slave or replicated) ACS that has been replicated. If you change this setting, click **Submit + Restart**.

Field	Description
Actual EAP-FAST server status	This option displays the status of the ACS. If you uncheck the EAP-FAST master server check box, the server status does not change to `Slave` until after ACS receives replicated EAP-FAST settings. **Note** If you uncheck the EAP-FAST Master Server check box, EAP-FAST server status remains `Master` until ACS receives replicated EAP-FAST components.

ACS Certificate Setup

This section contains the following topics:

- Installing an ACS Server Certificate, page 10-25
- Adding a Certificate Authority Certificate, page 10-27
- Editing the Certificate Trust List, page 10-27
- Managing Certificate Revocation Lists, page 10-28
- Generating a Certificate Signing Request, page 10-31
- Using Self-Signed Certificates, page 10-32
- Updating or Replacing an ACS Certificate, page 10-35

Installing an ACS Server Certificate

Perform this procedure to install (that is, enroll) a server certificate for your ACS. You can perform certificate enrollment to support EAP-TLS and PEAP authentication, as well as to support HTTPS protocol for GUI access to ACS.

The three options for obtaining your server certificate are:

- Obtain a certificate from a CA.
- Use an existing certificate from local machine storage.
- Generate a self-signed certificate.

Before You Begin

You must have a server certificate for your ACS before you can install it. With ACS, certificate files must be in Base64-encoded X.509. If you do not already have a server certificate in storage, you can use the procedure in Generating a Certificate Signing Request, page 10-31, or any other means, to obtain a certificate for installation.

If you are installing a server certificate that replaces an existing server certificate, the installation could affect the configuration of the CTL and CRL settings on your ACS. After you have installed a replacement certificate, you should determine whether you need to reconfigure any CTL or CRL settings.

If you want to use a server certificate from local machine storage, we recommend that you read *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks*, available on the ACS CD and at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml. This white paper provides information about how to add a certificate to machine storage and how to configure a Microsoft certification authority server for use with ACS.

To install an existing certificate for use on ACS:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

ACS displays the Install ACS Certificate page.

Step 4 You must specify whether ACS reads the certificate from a specified file or uses a certificate already on the local machine. To specify that ACS:

- Reads the certificate from a specified file, select the **Read certificate from file** option, and then type the full directory path and filename of the certificate file in the Certificate file box.
- Uses a particular existing certificate from local machine certificate storage, select the **Use certificate from storage** option, and then type the certificate CN (common name or subject name) in the Certificate CN box.

Tip Type the certificate CN only; omit the **cn=** prefix.

Step 5 If you generated the request by using ACS, in the Private key file box, type the full directory path and name of the file that contains the private key.

Note If the certificate was installed in storage with the private key, you do not have the private key file and do not need to type it.

Tip This is the private key that is associated with the server certificate.

Step 6 In the Private key password box, type the private key password.

Tip If you used ACS to generate the certificate signing request, this is the same value that you entered in Private key password on the Generate Certificate Signing Request page. If the private key file is unencrypted, leave this box empty.

Step 7 Click **Submit**.

To show that the certificate setup is complete, ACS displays the Installed Certificate Information table, which contains:

- Issued to: *certificate subject*
- Issued by: *CA common name*
- Valid from:
- Valid to:
- Validity:

Adding a Certificate Authority Certificate

Use this procedure to add new CA certificates to ACS local certificate storage.

Note If the clients and ACS are getting their certificates from the same CA, you do not need to perform this procedure because ACS automatically trusts the CA that issued its certificate.

When a user certificate is from an unknown CA (that is, one that is different from the CA that certifies the ACS), you must specifically configure ACS to trust that CA or authentication fails. Until you perform this procedure to explicitly extend trust by adding another CA, ACS only recognizes certificates from the CA that issued its own certificate.

Configuring ACS to trust a specific CA is a two-step process that comprises this procedure of adding a CAs certificate and the procedure in Editing the Certificate Trust List, page 10-27, in which you specify that the particular CA is to be trusted. (ACS comes configured with a list of popular CAs, none of which is enabled until you explicitly specify trustworthiness.)

To add a certificate authority certificate to your local storage:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **ACS Certification Authority Setup**.

ACS displays the CA Operations table on the Certification Authorities Setup page.

Step 4 In the CA certificate file box, type the full path and filename for the certificate to use.

Step 5 Click **Submit**.

The new CA certificate is added to local certificate storage. And, if it is not already there, the name of the CA that issued the certificate is placed on the CTL.

Tip To use this new CA certificate to authenticate users, you must edit the certificate trust list to specify that this CA is trusted. For more information, see Editing the Certificate Trust List, page 10-27.

Editing the Certificate Trust List

ACS uses the CTL to verify the client certificates. For ACS to trust a CA, its certificate must be installed and the ACS administrator must explicitly configure the CA as trusted by editing the CTL. If the ACS server certificate is replaced, the CTL is erased; you must then configure the CTL explicitly each time you install or replace a ACS server certificate.

Note The single exception to the requirement that you must explicitly specify a CA as trustworthy occurs when the clients and ACS are getting their certificates from the same CA. You do not need to add this CA to the CTL because ACS automatically trusts the CA that issued its certificate.

How you edit your CTL determines the type of trust model that you have. Many use a restricted trust model wherein very few privately controlled CAs are trusted. This model provides the highest level of security; but restricts adaptability and scalability. The alternative, an open trust model, allows for more CAs or public CAs. This open trust model trades increased security for greater adaptability and scalability.

We recommend that you fully understand the implications of your trust model before editing the CTL in ACS.

Use this procedure to configure CAs on your CTL as trusted or not trusted. Before you can configure a CA as trusted on the CTL, you must have added the CA to the local certificate storage; for more information, see Adding a Certificate Authority Certificate, page 10-27. If a user's certificate is from a CA that you have not specifically configured ACS to trust, authentication fails.

To edit the CTL:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Edit Certificate Trust List**.

The Edit the Certificate Trust List (CTL) table appears.

Warning **Adding a public CA, which you do not control, to your CTL may reduce your system security.**

Step 4 To configure a CA on your CTL as trusted, check the corresponding check box.

Tip You can check, or uncheck, as many CAs as you want. Unchecking a CA check box configures the CA as not trusted.

Step 5 Click **Submit**.

ACS configures the specified CA (or CAs) as trusted or not trusted in accordance with checking or unchecking check boxes. The selected Certificate Trust Lists automatically appear on the CRL Issuers page.

Managing Certificate Revocation Lists

Certificate revocation lists (CRLs) are the means by which ACS determines that the certificates employed by users who seek authentication are still valid, according to the CA that issued them.

This section contains the following topics:

- About Certificate Revocation Lists, page 10-29
- Certificate Revocation List Configuration Options, page 10-29
- Editing a Certificate Revocation List Issuer, page 10-31

About Certificate Revocation Lists

When a digital certificate is issued, you generally expect it to remain valid throughout its predetermined period of validity. However, various circumstances may call for invalidating the certificate earlier than expected. Such circumstances might include compromise or suspected compromise of the corresponding private key, or a change in the CAs issuance program. Under such circumstances, a CRL provides the mechanism by which the CA revokes the legitimacy of a certificate and calls for its managed replacement.

ACS performs certificate revocation by using the X.509 CRL profile. A CRL is a signed and time-stamped with a data structure that a CA (or CRL issuer) issues and which is freely available in a public repository (for example, in an LDAP server). Details on the operation of the X.509 CRL profile are contained in RFC3280.

CRL functionality in ACS includes:

- **Trusted publishers and repositories configuration**—In the ACS web interface, you can view and configure CRL issuers, and their CRL Distribution Points (CDPs) and periods.
- **Retrieval of CRLs from a CDP**—Using a transport protocol (LDAP or HTPP), ACS is configured to periodically retrieve CRLs for each CA that you configure. These CRLs are stored for use during EAP-TLS authentication. Note that there is no timestamp mechanism; instead ACS waits for a specified period of time and then automatically downloads the CRL. If the new CRL differs from the existing CRL, the new version is saved and added to the local cache. CRL retrievals appear in the log for the CSAuth service only when you have configured the level of detail in service logs to `full`. The status, date, and time of the last retrieval appears on the Certificate Revocation List Issuer edit page of the ACS web interface.

  Note Automatic CRL retrieval scheduling only functions if EAP-TLS is enabled.

- **Verification of certificate status**—During EAP-TLS authentication, ACS checks the certificate that the user against the corresponding CRL that the CA of the user's certificate issues. If, according to the CRL that ACS currently stores, the certificate has been revoked and authentication fails.

CRL issuers can only be added in association with trusted CAs (that is, CAs on the CTL). If you install a new server certificate for ACS, your CTL is cleared of all trust relationships. While you must reestablish CAs on the CTL, the associated CRLs that you previously configured remain in place and do not have to be reconfigured.

Certificate Revocation List Configuration Options

The Certificate Revocation List Issuers edit page contains the following configuration options:

- **Name**—The name given by the CA Issuer.
- **Description**—A description that you give this CRL issuer.
- **CRL Distribution URL**—The URL that ACS should use to retrieve the CRL. If a CA certificate contains a `CRL distribution points` parameter, this field will be populated automatically. Otherwise, ensure that you specify a URL for the CRL corresponding to the CA that you selected from the Issuer's Certificate list. You can specify a URL that uses HTTP, LDAP, or FTP. Alternatively, you can specify the URL for the file itself; however, this is only necessary when the repository URL lists multiple files.

  An example of an HTTP URL is:

  http://crl.verisign.com/pca1.1.1.crl.

An example of an LDAP URL is:

ldap://10.36.193.5:388/CN=development-CA,CN=acs-westcoast2,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cisco,DC=com

Note In LDAP, the default placement for the CRL is under objectclass=crlDistributionPoint. ACS adds the object class information to the URL. If the CRL is located elsewhere, you must add the object class to the URL. For example, if the CRL is situated under objectclass=CertificateRevocationList the URL should be: *ldap://10.36.193.5:388/CN=development-CA,CN=acs-westcoast2,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cisco,DC=com?(objectclass=CertificateRevocationList*).

Tip The URL must specify the CRL itself when the repository contains multiple files.

- **Retrieve CRL**—Initially ACS attempts to download a CRL from the CA. The CRL folder and file are created in the installation directory after a CRL is successfully downloaded. The CRL issuer is not modifiable. The Next Update field in the CRL file contains a value for the Next Update. Select the method that ACS should use for retrieving a CRL:
  - **Automatically**—Uses the value in the Next Update field in the CRL file to retrieve a new CRL from the CA. If unsuccessful, ACS tried to retrieve the CRL every 10 minutes after the first failure until it succeeds.
  - **Every**—Determines the frequency between retrieval attempts. Enter the amount in units of time.

Note For the automatic CRL retrieval function to operate, ensure that you have enabled EAP-TLS.

Note In both modes, if retrieval fails, a reattempt occurs every 10 minutes.

- **Last Retrieve Date—**This entry lists the status, and the date and time of the last CRL retrieval or retrieval attempt.
- **Options—**You check the **Ignore Expiration Date** check box to check a certificate against an outdated CRL.

  When the **Ignore Expiration Date** is unchecked, ACS examines the expiration date of the CRL in the Next Update field in the CRL file and continues to use this CRL; even though it has expired. If the expiry date passed, the CRL is not valid and all EAP-TLS authentications will be rejected.

  When the **Ignore Expiration Date** is checked, ACS continues to use the expired CRL and permits or rejects EAP-TLS authentications according to the contents of the CRL.
- **CRL is in Use**—When checked, the CRL is active and is used in the EAP-TLS authentication process.
- **Submit**—Click **Submit** to download and verify the CRL with the public key of the issuer. Inconsistencies generate CRL Issuer Configuration errors.

When submission succeeds, you must restart ACS to apply the new configuration.

Editing a Certificate Revocation List Issuer

To edit a certificate revocation list issuer:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Certificate Revocation Lists**.

The CRL Issuers page appears.

Step 4 Click the name of the CRL issuer that you want to edit.

The system displays the CRL Issuer Edit page for the CRL that you chose.

Step 5 Edit the information and settings that you want to change.

Step 6 Click **Submit**.

The corresponding CRL is changed in ACS to that of the edited issuer (or is scheduled to be changed at the time that you specify in the Retrieve CRL field).

Tip You can refer to the **Last Retrieve date** box to see the status, date, and time of the last CRL retrieval attempt.

Generating a Certificate Signing Request

You can use ACS to generate a certificate signing request (CSR). After you generate a CSR, you can submit it to a CA to obtain your certificate. You perform this procedure to generate the CSR for future use with a certificate enrollment tool.

Note If you already have a server certificate, you do not need to use this portion of the ACS Certificate Setup page.

To generate a certificate signing request:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Select **ACS Certificate Setup**, then **Generate Certificate Signing Request**.

ACS displays the Generate Certificate Signing Request page.

Step 3 In the Certificate subject box, type values for the certificate fields that the CA to which to submit the CSR. Filling in the CN field is mandatory. The format is:

field=value, *field=value*, . . .

where *field* is the field name, such as ***CN***, and *value* is the applicable value for the field, such as ***acs01primary***. You can type a maximum of 256 characters in the Certificate subject box. Separate multiple values with commas (,); for example:

```
CN=acs01primary, O=WestCoast, C=US, S=California
```

Table 10-3 defines the valid fields that you can include in the Certificate subject box.

Table 10-3 Certificate Subject Fields

Field	Field Name	Min. Length	Max. Length	Required?
CN	commonName	1	64	Yes
OU	organizationalUnitName	—	—	No
O	organizationName	—	—	No
S	stateOrProvinceName	—	—	No
C	countryName	2	2	No
E	emailAddress	0	40	No
L	localityName	—	—	No

Step 4 In the **Private key file** box, type the full directory path and name of the file in which the private key is saved; for example, `c:\privateKeyFile.pem`.

Step 5 In the **Private key password** box, type the private key password (that you have invented).

Step 6 In the **Retype private key password** box, retype the private key password.

Step 7 From the **Key length** list, select the length of the key to use.

Tip The choices for Key length are 512 or 1024 bits. The default and more secure choice is 1024 bits.

Step 8 From the **Digest to sign with** list, select the digest (or hashing algorithm). The choices are MD2, MD5, SHA, and SHA1. The default is SHA1.

Step 9 Click **Submit**.

ACS displays a CSR on the right side of the browser.

Step 10 Submit the CSR to the CA of your choice.

After you receive the certificate from the CA, you can perform the steps in Installing an ACS Server Certificate, page 10-25.

Using Self-Signed Certificates

You can use ACS to generate a self-signed digital certificate to use for the PEAP authentication protocol or HTTPS support of ACS administration. This capability supports TLS/SSL protocols and technologies without the requirement of interacting with a CA.

This section contains the following topics:

- About Self-Signed Certificates, page 10-33
- Self-Signed Certificate Configuration Options, page 10-33
- Generating a Self-Signed Certificate, page 10-34

About Self-Signed Certificates

ACS supports TLS/SSL-related protocols, including PEAP, EAP-FAST, and HTTPS, that require the use of digital certificates. Employing self-signed certificates is a way for administrators to meet this requirement without having to interact with a CA to obtain and install the certificate for the ACS. The administrator uses the self-signed certificate feature in ACS to generate the self-signed digital certificate, and use it for the PEAP and EAP-FAST authentication protocols or for HTTPS support in web administration service.

Other than the lack of interaction with a CA to obtain the certificate, installing a self-signed certificate requires exactly the same user actions as any other digital certificate. Although ACS does not support the replication of self-signed certificates, you can export a certificate for use on more than one ACS. To do this, you copy the certificate file (*.cer* format) and the corresponding private key file (*.pvk* format) to another ACS where you then install the certificate in the standard manner. For information on installing certificates, see Installing an ACS Server Certificate, page 10-25.

To ensure that a self-signed certificate interoperates with the client, refer to your client documentation. You may find that you must import the self-signed server certificate as a CA certificate on your particular client.

Self-Signed Certificate Configuration Options

The Generate Self-Signed Certificate edit page contains the following mandatory configuration fields:

- **Certificate subject**—The subject for the certificate, prefixed with **cn=**. We recommend using the ACS name. For example, **cn=ACS11**. The Certificate subject field here can contain a number of content entries as comma-separated items; these include:
  - **CN—**common name (the mandatory entry)
  - **OU—**organizational unit name
  - **O—**organization name
  - **S—**state or province
  - **E—**email address
  - **L—**locality name

  For example, the Certificate subject field might appear as:

  ```
  cn=ACS 11, O=Acme Enterprises, E=admin@acme.com
  ```

- **Certificate file**—The full path and filename for the certificate file that you want to generate. For example, **c:\acs_server_cert\acs_server_cert.cer**. When you submit this page, ACS creates the certificate file by using the location and filename that you specify.
- **Private key file**—The full path and filename for the private key file you want to generate. For example, **c:\acs_server_cert\acs_server_cert.pvk**. When you submit this page, ACS creates the private key file using the location and filename you specify.
- **Private key password**—A private key password for the certificate. Minimum length for the private key password is 4 characters, and the maximum length is 64 characters.
- **Retype private key password**—The private key password typed again, to ensure accuracy.
- **Key length**—Select the key length from the list. The choices include 512 bits, 1024 bits, and 2048 bits.
- **Digest to sign with**—Select the hash digest to use to encrypt the key from the list. The choices include SHA1, SHA, MD2, and MD5.

- **Install generated certificate**—Select this check box if you want ACS to install the self-signed certificate that it generates when you click **Submit**. If you employ this option, you must restart ACS services after you submit the page for the new settings to take effect. If you do not select this option, the certificate file and private key file are generated and saved; but are not installed into local machine storage.

Generating a Self-Signed Certificate

All fields on the Generate Self-Signed Certificate page are mandatory. For information on the fields' contents, see Self-Signed Certificate Configuration Options, page 10-33.

To generate a self-signed certificate:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Generate Self-Signed Certificate**.

The Generate Self-Signed Certificate edit page appears.

Step 4 In the **Certificate subject** box, type the certificate subject in the form **cn=XXXX**. You can enter additional information here, for more information see Self-Signed Certificate Configuration Options, page 10-33.

Step 5 In the **Certificate file** box, type the full path and file name for the certificate file.

Step 6 In the **Private key file** box, type the full path and file name for the private key file.

Step 7 In the **Private key password** box, type the private key password.

Step 8 In the **Retype private key password** box, retype the private key password.

Step 9 In the **Key length** box, select the key length.

Step 10 In the **Digest to sign with** box, select the hash digest to be used to encrypt the key.

Step 11 To install the self-signed certificate when you submit the page, select the **Install generated certificate** option.

Note If you select the Install generated certificate option, you must restart ACS services after submitting this form for the new settings to take effect.

Tip If you do not select the Install generated certificate option, the certificate file and private key file are generated and saved when you click Submit in the next step; but are not installed in local machine storage.

Step 12 Click **Submit**.

The specified certificate and private key files are generated and stored. If you selected the Install generated certificate option, the certificate becomes operational, only after you restart ACS services.

Updating or Replacing an ACS Certificate

Use this procedure to update or replace an existing ACS certificate that is out of date or out of order.

Caution This procedure eliminates your existing ACS certificate and erases your CTL configuration.

To install a new ACS certificate:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

ACS displays the Installed Certificate Information table on the ACS Certificate Setup page.

Note If your ACS has not already been enrolled with a certificate, you do not see the Installed Certificate Information table. Rather, you see the Install new certificate table. If this is the case, proceed to Step 5.

Step 3 Click **Enroll New Certificate**.

A confirmation dialog box appears.

Step 4 To confirm that you intend to enroll a new certificate, click **OK**.

The existing ACS certificate is removed and your CTL configuration is erased.

Step 5 You can now install the replacement certificate in the same manner as an original certificate. For detailed steps, see Installing an ACS Server Certificate, page 10-25.

Logs and Reports

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, produces a variety of logs, and provides a way to view most of these logs in the ACS web interface as HTML reports.

This chapter contains the following topics:

- Logging Formats, page 11-1
- Special Logging Attributes, page 11-2
- Posture-Validation Attributes in Logs, page 11-3
- Update Packets in Accounting Logs, page 11-3
- About ACS Logs and Reports, page 11-4
- Working with CSV Logs, page 11-10
- Working with ODBC Logs, page 11-16
- Remote Logging, page 11-19
- Service Logs, page 11-23

Logging Formats

ACS logs a variety of user and system activities. Depending on the log and how you have configured ACS, logs can be recorded in one of two formats:

- **Comma-separated value (CSV) files**—The CSV format records data in columns separated by commas. This format is easily imported into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After data from a CSV file is imported into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, please see the documentation from the third-party vendor. You can access the CSV files on the ACS server hard drive or by downloading the CSV file from the web interface. For more information about downloading the CSV file from the web interface, see Viewing a CSV Report, page 11-12.
- **ODBC-compliant database tables**—You can use Open DataBase Connectivity (ODBC) logging to configure ACS to log directly in an ODBC-compliant relational database, where it is stored in tables, one table per log. After the data is exported to the relational database, you can use the data however you need. For more information about querying the data in your relational database, refer to the documentation from the relational database vendor.

For information about the formats that are available for a specific log, see About ACS Logs and Reports, page 11-4.

Special Logging Attributes

Among the many attributes that ACS can record in its logs, a few are of special importance. The following list explains the special logging attributes that ACS provides.

- **User Attributes**—These logging attributes appear in the Attributes list for any log configuration page. ACS lists them by using their default names: Real Name, Description, User Field 3, User Field 4, and User Field 5. If you change the name of a user-defined attribute, the default name rather, than the new name, still appears in the Attributes list.

  The values that you enter in the corresponding fields in the user account determine the content of these attributes. For more information about user attributes, see User Data Configuration Options, page 3-4.

- **ExtDB Info**—If the user is authenticated with an external user database, this attribute contains a value that the database returns. In the case of a Windows user database, this attribute contains the name of the domain that authenticated the user.

  In entries in the Failed Attempts log, this attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user-authentication attempt.

- **Access Device**—The name of the AAA client that is sending the logging data to ACS.

- **Network Device Group**—The network device group to which the access device (AAA client) belongs.

- **Filter Information**—The result of network access restrictions (NARs) applied to the user, if any. The message in this field indicates whether all applicable NARs permitted the user access, all applicable NARs denied the user access, or more specific information about which NAR denied the user access. If no NARs apply to the user, this logging attribute notes that no NARs were applied.

  The Filter Information attribute is available for Passed Authentication and Failed Attempts logs.

- **Device Command Set**—The name of the device command set, if any, that was used to satisfy a command authorization request.

  The Device Command Set attribute is available for Failed Attempts logs.

- **Remote Logging Result**—Whether a remote logging service successfully processes a forwarded accounting packet. This attribute is useful for determining which accounting packets, if any, a central logging service did not log. It is dependent upon the receipt of an acknowledgment message from the remote logging service. The acknowledgment message indicates that the remote logging service properly processed the accounting packet in the manner that the remote logging service is configured to do. A value of `Remote-logging-successful` indicates that the remote logging service successfully processed the accounting packet. A value of `Remote-logging-failed` indicates that the remote logging service did not process the accounting packet successfully.

Note ACS cannot determine how a remote logging service is configured to process accounting packets that it is forwarded. For example, if a remote logging service is configured to discard accounting packets, it discards a forwarded accounting packet and responds to ACS with an acknowledgment message, causing ACS to write a value of `Remote-logging-successful` in the Remote Logging Result attribute in the local log that records the account packet.

- **Application-Posture-Token**—The application posture token (APT) returned by a particular policy during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs. For more information, see Posture-Validation Attributes in Logs, page 11-3.
- **System-Posture-Token**—The system posture token (SPT) that is returned during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs. For more information, see Posture-Validation Attributes in Logs, page 11-3.
- **Other Posture-Validation Attributes**—Attributes that a NAC client sends to ACS during a posture-validation request. The attributes are uniquely identified by the vendor name, application name, and attribute name. For example, the NAI:AV:DAT-Date attribute is an attribute containing information about the date of the DAT file on the NAC client for the anti-virus application by Network Associates, Inc. These attributes are available only in the Passed Authentications and Failed Attempts logs. For more information, see Posture-Validation Attributes in Logs, page 11-3.

Posture-Validation Attributes in Logs

You can choose to log posture-validation attributes in the Passed Authentications and Failed Attempts logs. All inbound attributes are available for logging. The only two outbound attributes that you can record in logs are `Application-Posture-Assessment` and `System-Posture-Assessment`.

All posture-validation requests resulting in a system posture assessment/token (SPT) are logged in the Passed Authentications log. posture-validation requests resulting in an SPT of anything other than `Healthy` are logged in the Failed Attempts log. For more information about posture tokens, see Posture Tokens, page 14-3.

Reporting HCAP Errors

The `Authen-Failure-Code` entry in the Failed-Attempts report may display one of the following errors when HCAP fails:

- `Version failure - Could not communicate with external policy server - wrong HCAP version`
- `Connection failure - Could not open a connection to external policy server`
- `Authentication failure - Could not communicate with external policy server - authentication failure`
- `Timeout error - Could not connect to external policy server - timeout error`
- `Other - Posture Validation Failure on External Policy`

Update Packets in Accounting Logs

Whenever you configure ACS to record accounting data for user sessions, ACS records start and stop packets. If you want, you can configure ACS to record update packets, too. In addition to providing interim accounting information during a user session, update packets drive password-expiry messages via ACS Authentication Agent. In this use, the update packets are called watchdog packets.

Note To record update packets in ACS accounting logs, you must configure your AAA clients to send the update packets. For more information about configuring your AAA client to send update packets, refer to the documentation for your AAA clients.

- **Logging Update Packets Locally**—To log update packets according to the local ACS logging configuration, enable the Log Update/Watchdog Packets from this Access Server option for each AAA client in Network Configuration.

  For more information on setting this option for a AAA client, see Adding AAA Clients, page 4-11.

- **Logging Update Packets Remotely**—To log update packets on a remote logging server, enable the Log Update/Watchdog Packets from this remote AAA Server option for the remote server AAA Server table entry on the local ACS.

  For more information on setting this option for a AAA server, see Adding AAA Servers, page 4-16.

About ACS Logs and Reports

ACS provides logs that can be divided into four types:

- Accounting logs
- Dynamic ACS administration reports
- ACS system logs
- Service logs

This section contains information about the items from the previous list. For information about service logs, see Service Logs, page 11-23.

This section contains the following topics:

- Accounting Logs, page 11-4
- Dynamic Administration Reports, page 11-6
- ACS System Logs, page 11-8

Note All reports open instantly when selected, except for the Logged-In Users report, which might take up to 20 seconds to open. Specific user information might take up to several minutes to appear.

Accounting Logs

Accounting logs contain information about the use of remote access services by users. By default, these logs are available in CSV format, with the exception of the Passed Authentications log. You can also configure ACS to export the data for these logs to an ODBC-compliant relational database that you configure to store the log data. Table 11-1 describes all accounting logs.

In the web interface, all accounting logs can be enabled, configured, and viewed. Table 11-2 contains information about what you can do with the accounting logs.

Table 11-1 Accounting Log Descriptions

Log	Description
TACACS+ Accounting	Contains: • User sessions stop and start times • AAA client messages with username • Caller line identification (CLID) • Session duration
TACACS+ Administration	Lists configuration commands entered on a AAA client by using TACACS+ (Cisco IOS). Particularly if you use ACS to perform command authorization, we recommend that you use this log. **Note** To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with ACS.
RADIUS Accounting	Contains: • User sessions stop and start times • AAA client messages with username • Caller line identification information • Session duration You can configure ACS to include accounting for Voice-over-IP (VoIP) in the RADIUS Accounting log, in a separate VoIP accounting log, or in both places.
VoIP Accounting	Contains: • VoIP session stop and start times • AAA client messages with username • CLID information • VoIP session duration You can configure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places.
Failed Attempts	Lists authentication and authorization failures with an indication of the cause. For posture-validation requests, this log records the results of any posture validation that returns a posture token other than `Healthy`. **Note** In entries in the Failed Attempts log, the `ExtDB Info` attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user-authentication attempt.
Passed Authentications	Lists successful authentication requests. This log is not dependent upon accounting packets from your AAA clients, so it is available; even if your AAA clients do not support RADIUS accounting or if you have disabled accounting on your AAA clients. For posture-validation requests, this log records the results of all posture-validation requests resulting in an SPT.

Table 11-2 What You Can Do with Accounting Logs

What You Can Do	Description and Related Topics
Enable an accounting log	You can enable the log in CSV or ODBC format. • **CSV**—For instructions on how to enable an accounting log in CSV format, see Enabling or Disabling a CSV Log, page 11-11. • **ODBC**—For instructions on how to enable an account log in ODBC format, see Configuring an ODBC Log, page 11-17.
View an accounting report	For instructions on viewing an accounting report in the web interface, see Viewing a CSV Report, page 11-12.
Configure an accounting log	The steps for configuring an accounting log vary depending upon which format you use. For more information about log formats, see Logging Formats, page 11-1. • **CSV**—For instructions on configuring the CSV accounting log, see Configuring a CSV Log, page 11-14. • **ODBC**—For instructions on configuring ODBC accounting log, see Configuring an ODBC Log, page 11-17.

Dynamic Administration Reports

These reports show the status of user accounts when you access them in the ACS web interface. They are available only in the web interface, are always enabled, and require no configuration.

Table 11-3 contains descriptions of all dynamic administration reports and information about what you can do regarding dynamic administration reports.

Table 11-3 Dynamic Administration Report Descriptions and Related Topics

Report	Description and Related Topics
Logged-In Users	Lists all users receiving services for a single AAA client or all AAA clients. Users accessing the network with Cisco Aironet equipment appear on the list for the access point that they are currently associated with, provided that the firmware image on the Cisco Aironet Access Point supports sending the RADIUS Service-Type attribute for rekey authentications. On a computer configured to perform machine authentication, machine authentication occurs when the computer starts. When a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section. Once user authentication begins, the computer no longer appears on the Logged-In Users List. For more information about machine authentication, see EAP and Windows Authentication, page 13-10. **Note** To use the logged-in user list feature, you must configure AAA clients to perform authentication and accounting by using the same protocol—TACACS+ or RADIUS. For instructions on viewing the Logged-in User report in the web interface, see Viewing the Logged-in Users Report, page 11-7. For instructions about deleting logged-in users from specific AAA clients or from all AAA clients, see Deleting Logged-in Users, page 11-7.
Disabled Accounts	Lists all user accounts that are disabled and the reason they were disabled. For instructions on viewing the Disabled Accounts report in the web interface, see Viewing the Disabled Accounts Report, page 11-8.

Viewing the Logged-in Users Report

To view the Logged-in Users report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users who are logged in through the AAA client. At the bottom of the table, the **All AAA Clients** entry shows the total number of users who are logged in.

Tip You can sort the table by any column's entries, in ascending or descending order. Click a column title once to sort the table by the entries in that column in ascending order. Click the column a second time to sort the table by the entries in that column in descending order.

Step 3 Do one of the following:

- To see a list of all users who are logged in, click **All AAA Clients**.
- To see a list of users who are logged in through a particular AAA client, click the name of the AAA client.

ACS displays a table of users who are logged in, including:

- Date and Time
- User
- Group
- Assigned IP
- Port
- Source AAA Client

Tip You can sort the table by the entries in any column, in ascending or descending order. Click a column title once to sort the table by the entries in that column, in ascending order. Click the column a second time to sort the table by the entries that column in descending order.

Deleting Logged-in Users

From a Logged-in Users Report, you can instruct ACS to delete users who are logged into a specific AAA client. When a user session terminates without a AAA client sending an accounting stop packet to ACS, the Logged-in Users Report continues to show the user. Deleting logged-in users from a AAA client ends the accounting for those user sessions.

Note Deleting logged-in users only ends the ACS accounting record of users who are logged in to a particular AAA client. It does not terminate active user sessions, nor does it affect user records.

To delete logged-in users:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users who are logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users who are logged in.

Step 3 Click the name of the AAA client whose users you want to delete from the Logged-in Users report.

ACS displays a table of all users who are logged in through the AAA client. The Purge Logged in Users button appears below the table.

Step 4 Click **Purge Logged in Users**.

ACS displays a message, indicating the number of users who are purged from the report and the IP address of the AAA client.

Viewing the Disabled Accounts Report

To view the Disabled Accounts report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Disabled Accounts**.

The Select a user account to edit page displays disabled user accounts, the account status, and the group to which the user account is assigned.

Step 3 To edit a user account listed, in the User column, click the username.

ACS opens the user account for editing.

For more information about editing a user account, see Basic User Setup Options, page 7-2.

ACS System Logs

System logs are logs about the ACS system and therefore record system-related events. These logs are useful for troubleshooting or audits. They are always enabled and are only available in CSV format. Some system logs can be configured. For information about each system log, including which system logs are configurable, see Table 11-4.

For instructions on viewing a CSV report in the web interface, see Viewing a CSV Report, page 11-12.

Table 11-4 Accounting Log Descriptions and Related Topics

Log	Description and Related Topics
ACS Backup and Restore	Lists ACS backup and restore activity. You cannot configure this log.
RDBMS Synchronization	Lists RDBMS Synchronization activity. You cannot configure this log.
Database Replication	Lists database replication activity. You cannot configure this log.

Table 11-4 Accounting Log Descriptions and Related Topics (continued)

Log	Description and Related Topics
Administration Audit	Lists actions taken by each system administrator, such as adding users, editing groups, configuring a AAA client, or viewing reports. For instructions on configuring the Administration Audit log, see Configuring the Administration Audit Log, page 11-9.
User Password Changes	Lists user password changes that users initiate, regardless of which password-change mechanism was used to change the password. Thus, this log contains records of password changes accomplished by the ACS Authentication Agent, by the User Changeable Password web interface, or by Telnet session on a network device using TACACS+. It does not list password changes that an administrator makes in the ACS web interface. For information about configuring the User Password-Changes log, see Configuring Local Password Management, page 8-6.
ACS Service Monitoring	Lists when ACS services start and stop. For information about configuring the ACS Service Monitoring log, see ACS Active Service Management, page 8-13.

Configuring the Administration Audit Log

You use this procedure to configure how often, or at what size limit, ACS generates a new Administration Audit Log file. You can also use this procedure to configure the Administration Audit Log file storage limits with regard to number or age.

To configure the Administrative Audit log:

Step 1 In the navigation bar, click **Administration Control**.

Step 2 Click **Audit Policy**.

The Audit Policy Setup page appears.

Step 3 To generate a new Administrative Audit CSV file at a regular interval, select a frequency:

- **Every day**— ACS generates a new Administrative Audit CSV file at the start of each day.
- **Every week**— ACS generates a new Administrative Audit CSV file at the start of each week.
- **Every month**— ACS generates a new Administrative Audit CSV file at the start of each month.

Step 4 To generate a new Administrative Audit CSV file when the current file reaches a specific size, select the **When size is greater than** *x* **KB** option and type the file size threshold in kilobytes in the *X* box.

Step 5 To manage which Administrative Audit CSV files ACS keeps:

a. Check the **Manage Directory** check box.

b. To limit the number of Administrative Audit CSV files that ACS retains, select the **Keep only the last** *X* **files** option and type in the *X* box the number of files that you want ACS to retain.

c. To limit the age of Administrative Audit CSV files that ACS retains, select the **Delete files older than** *X* **days** option and type the number of days for which ACS should retain a Administrative Audit CSV file before deleting it.

Step 6 Click **Submit**.

ACS saves and implements the Administrative Audit log settings you specified.

Working with CSV Logs

This section contains the following topics:

- CSV Log File Names, page 11-10
- CSV Log File Locations, page 11-10
- Enabling or Disabling a CSV Log, page 11-11
- Viewing a CSV Report, page 11-12
- Log Filtering, page 11-13
- Configuring a CSV Log, page 11-14

Tip Using a CSV file may not work well in different countries; for example, when imported into programs such as Word or Excel. You may need to replace the commas (,) with semicolons (;), if necessary.

CSV Log File Names

When you access a report in Reports and Activity, ACS lists the CSV files in chronological order, with the current CSV file at the top of the list. The current file is named *log*.csv, where *log* is the name of the log.

Older files are named as:

log`yyyy-mm-dd.csv`

where

log is the name of the log.

yyyy is the year that the CSV file was started.

mm is the month that the CSV file was started, in numeric characters.

dd is the date that the CSV file was started.

For example, a Database Replication log file that was generated on October 13, 2002, would be named *Database Replication 2002-10-13.csv*.

CSV Log File Locations

By default, ACS keeps log files in directories that are unique to the log. You can use the web interface to configure the log file location for some logs while the location for other log files is not configurable. The default directories for all logs are within *sysdrive*`:\Program Files\CiscoSecure ACS v`*x.x*. For the subdirectory of this location for a specific log, see Table 11-5.

Table 11-5 Default CSV Log File Locations

Log	Default Location	Configurable?
TACACS+ Accounting	`Logs\TACACS+Accounting`	Yes
CSV TACACS+ Administration	`Logs\TACACS+Administration`	Yes
CSV RADIUS Accounting	`Logs\RADIUS Accounting`	Yes
CSV VoIP Accounting	`Logs\VoIP Accounting`	Yes
CSV Failed Attempts	`Logs\Failed Attempts`	Yes
Passed Authentications	`Logs\Passed Authentications`	Yes
ACS Backup and Restore	`Logs\Backup and Restore`	No
RDBMS Synchronization	`Logs\DbSync`	No
RDBMS Synchronization	`Logs\DBReplicate`	No
Administration Audit	`Logs\AdminAudit`	No
User Password Changes	`CSAuth\PasswordLogs`	No
ACS Active Service Monitoring	`Logs\ServiceMonitoring`	No

Enabling or Disabling a CSV Log

This procedure describes how to enable or disable a CSV log. For instructions about configuring the content of a CSV log, see Configuring a CSV Log, page 11-14.

Note Some CSV logs are always enabled. For information about specific logs, including whether you can disable them, see About ACS Logs and Reports, page 11-4.

To enable or disable a CSV log:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Step 3 Click the name of the CSV log that you want to enable.

The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log that you selected.

Step 4 To enable the log, under Enable Logging, select the **Log to CSV** *log* **report** check box, where *log* is the name of the CSV log that you selected in Step 3.

Step 5 To disable the log, under Enable Logging, clear the **Log to CSV** *report* **log** check box, where *log* is the name of the CSV log that you selected in Step 3.

Step 6 Click **Submit**.

If you enabled the log, ACS begins logging information for the log that you selected. If you disabled the log, ACS stops logging information for the log that you selected.

Viewing a CSV Report

When you select Logged-in Users or Disabled Accounts, a list of logged-in users or disabled accounts appears in the display area, which is the pane on the right side of the web browser. For all other types of reports, a list of applicable reports appears. Files appear in chronological order, with the most recent file at the top of the list. The reports are named and listed by the date on which they were created; for example, a report ending with *2002-10-13.csv* was created on October 13, 2002.

Files in CSV format can be imported into spreadsheets by using most popular spreadsheet application software. Refer to your spreadsheet software documentation for instructions. You can also use a third-party reporting tool to manage report data. For example, aaa-reports! by Extraxi supports ACS (http://www.extraxi.com).

You can download the CSV file for any CSV report that you view in ACS.

To view a CSV report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click the name of the CSV report that you want to view.

On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV report files.

Tip You can configure how ACS handles old CSV report files. For more information, see Configuring a CSV Log, page 11-14.

Step 3 Click the CSV report filename whose contents that you want to view.

If the CSV report file contains information, the information appears in the display area.

Tip You can sort the table by any entries in the column, in ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.

Tip To check for newer information in the current CSV report, click **Refresh**.

Step 4 If you want to download the CSV log file for the report you are viewing:

a. Click **Download**.

Your browser displays a dialog box for accepting and saving the CSV file.

b. Choose a location to save the CSV file and click **Save** to save the file.

Log Filtering

You can use ACS to filter CSV log reports. When you select a report type from the available reports types list, a report history (log) files list of the selected report type appears. After you select a specific CSV log file, and its contents appear, you can specify the filtering criteria. The filtering criteria is applied on the original log file, and only rows that match the criteria appear.

Filtering criteria includes a regular expression, a time range or both.

Regular expression-based filtering checks that at least one of each column's value, per row, matches the provided regular expression. When you use regular expression filtering, ACS traverses each column and displays only the rows that match the filtering criteria.

You can use time-based filtering by specifying values for a Start Date & Timeand an End Date & Time. Rows dated within the specified time range appear.

You can enter a regular expression for filtering, a time-based filter, or a combination of both. When you enter a regular expression and use time-based filtering as well, the report will include only the rows that match both criteria.

Note The functionality of the **Refresh** and **Download** links remain unchanged (without filtering). See Viewing a CSV Report, page 11-12.

To apply a log filter:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click the name of the CSV report type that you want to view.

On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV (log) report files.

Step 3 Select a log file. The contents appear.

You can then specify filtering criteria and apply the filter to the log file’s content.

Step 4 In the **Regular Expression** text box enter a string value. The expression can be up to 100 characters long.

Step 5 In the **Start Date & Time** and **End Date & Time** text boxes, enter string values. The date and time format is dd/mm/yyyy,hh:mm:ss or mm/dd/yyyy,hh:mm:ss as defined in the ACS system configuration for the date format.

Step 6 In the **Rows per Page** box choose the number of rows to display per page. (The default is 50.)

Step 7 Click **Apply Filter.** The ACS web server will apply the specified filtering criteria to the report file and display the filtered results in the report's table.

Click **Clear Filter** to reset filtering parameters to their default values. Use this option to display the entire report unfiltered.

Step 8 Use the **Next** and **Previous** buttons to navigate forward and backward through the report pages.

Regular Expression Basic Syntax Reference

Table 11-6 lists the Regular Expression characters and their syntax definitions.

Table 11-6 Regular Expression Syntax Definitions

Character	Regular Expression Use
^	A caret (^) matches to the beginning of the string. Referred to as "begins with." For example, **^A** will match **ABc**, **A123**, but not **1A234**. See the last table entry for another caret usage.
$	The dollar sign ($) matches the end of the string. Referred to as "ends with." For example, **yz$** will match strings ending with **xyz**, **0123yz**, but not **12yzA**.
\	The backslash (\) matches a given string at any location. Referred to as "contains." A backslash is also used for expressing 'special characters' in a given regular expression (For example, **\+** will match against the plus sign (+), to differentiate from the plus sign (+) usage in regular expressions.
.	The dot (.) matches any character.
*	The asterisk (*) indicates that the character to the left of the asterisk in the expression should match for any number of instances (that is, 0 or more times).
+	The plus sign (+) is similar to the asterisk (*) but at least one match of the character should appear to the left of the plus sign (+) in the expression.
?	The question mark (?) matches the expression or character to its left 0 or 1 times.
|	The pipe (|) allows the expression on either side of it to match the target string. For example, **A|a** matches against **A** as well as **a**.
-	The hyphen (-) indicates a range of values. For example, a-z.
()	The parentheses are used for grouping of expressions and affects the order of pattern evaluation
[]	Brackets ([) and (]) enclosing a set of characters indicate that any of the enclosed characters may match the target character. Values in brackets can be one or more characters, or ranges. For example, [02468], [0-9].
[^	When a caret (^) is positioned to immediately follow a left bracket ([), it excludes the remaining characters within brackets from matching the target string. For example, **[^0-9]** indicates that the target character is alpha rather than numeric.

Configuring a CSV Log

This procedure describes how to configure the content of a CSV log. For instructions to enable or disable a CSV log, see Enabling or Disabling a CSV Log, page 11-11.

The logs to which this procedure applies are:

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Failed Attempts
- Passed Authentications

Note You cannot configure the ACS Backup and Restore, RDBMS synchronization, and Database Replication CSV logs.

You can configure several aspects of a CSV log, including:

- **Log content**—Select which data attributes are included in the log.
- **Log generation frequency**—Determine whether a new log is started after a specific length of time or when the current CSV file reaches a particular size.
- **CSV file location**—Specify where on the local hard drive ACS writes the CSV file.
- **CSV file retention**—Specify how many old CSV files ACS maintains or set a maximum number of files to retain.

To configure a CSV log:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Step 3 Click the name of the CSV log that you want to enable.

The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log that you selected.

The Select Columns To Log table contains two lists, Attributes and Logged Attributes. The attributes in the Logged Attributes list appear on the log that you selected.

Step 4 To add an attribute to the log, select the attribute in the Attributes list, and then click **-->** (right arrow button).

The attribute moves to the Logged Attributes list.

Tip Use the vertical scroll bar to find attributes that are not visible in the list box.

Step 5 To remove an attribute from the log, select the attribute in the Logged Attributes list, and then click **<--** (left arrow button).

The attribute moves to the Attributes list.

Tip Use the vertical scroll bar to find attributes that are not visible in the list.

Step 6 To set the attributes in the Logged Attributes list back to the default selections, at the bottom of the browser window, click **Reset Columns**.

Step 7 To generate a new CSV file at a regular interval, select a frequency:

- **Every day**— ACS generates a new CSV file at the start of each day.
- **Every week**— ACS generates a new CSV file at the start of each week.
- **Every month**— ACS generates a new CSV file at the start of each month.

Step 8 To generate a new CSV file when the current file reaches a specific size, select the **When size is greater than** *x* **KB** option and type the file size threshold, in kilobytes, in the *X* box.

Step 9 To manage which CSV files ACS keeps:

a. Select the **Manage Directory** check box.

b. To limit the number of CSV files that ACS retains, select the **Keep only the last *X* files** option and type the number of files you want ACS to retain in the *X* box.

c. To limit the age of the CSV files that ACS can retain, select the **Delete files older than *X* days** option and type the number of days for which ACS should retain a CSV file before deleting it.

Step 10 Click **Submit**.

ACS implements the CSV log configuration that you specified.

Working with ODBC Logs

This section contains the following topics:

- Preparing for ODBC Logging, page 11-16
- Configuring a System Data Source Name for ODBC Logging, page 11-17
- Configuring an ODBC Log, page 11-17

Preparing for ODBC Logging

The following procedure explains how to prepare for ODBC logging. After you have prepared for ODBC logging, you can configure individual ODBC logs.

To prepare for ODBC logging:

Step 1 Set up the relational database to which you want to export logging data. For more information, refer to your relational database documentation.

Step 2 Set up a system data source name (DSN) on the computer that is running ACS. For instructions, see Configuring a System Data Source Name for an ODBC External User Database, page 13-43.

Step 3 Enable ODBC logging in the ACS web interface:

a. In the navigation bar, click **Interface Configuration**.

b. Click **Advanced Options**.

c. Select the **ODBC Logging** check box.

d. Click **Submit**.

ACS enables the ODBC logging feature. On the Logging page, in the System Configuration section, ACS displays links for configuring ODBC logs.

You can now configure individual ODBC logs. For instructions, see Configuring an ODBC Log, page 11-17.

Configuring a System Data Source Name for ODBC Logging

On the computer running that is ACS, you must create a system DSN for ACS to communicate with the relational database that will store your logging data.

To create a system DSN for use with ODBC logging:

Step 1 In Windows Control Panel, double-click **ODBC Data Sources**.

Step 2 In the ODBC Data Source Administrator page, click the **System DSN** tab.

Step 3 Click **Add**.

Step 4 Select the driver to use with your new DSN, and then click **Finish**.

A dialog box displays fields requiring information that is specific to the ODBC driver that you selected.

Step 5 Type a descriptive name for the DSN in the Data Source Name box.

Step 6 Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant relational database runs.

Step 7 Click **OK**.

Step 8 Close the ODBC window and Windows Control Panel.

The System DSN to be used by ACS for communicating with the relational database is created on the computer running ACS. The name you assigned to the DSN appears in the Data Source list on each ODBC log configuration page.

Configuring an ODBC Log

The logs to which this procedure applies are:

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Failed Attempts
- Passed Authentications

Note Before you can configure an ODBC log, you must prepare for ODBC logging. For more information, see Preparing for ODBC Logging, page 11-16.

To configure an ODBC log:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Step 3 Click the name of the ODBC log you want to enable.

The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.

The Select Columns To Log table contains two lists: Attributes and Logged Attributes. When you first access the ODBC configuration page for a log, the Logged Attributes list contains the default set of attributes. ACS includes in the log only those attributes that are in the Logged Attributes list.

Step 4 Specify the attributes that you want ACS to send to the relational database:

a. To add an attribute to the log, select the attribute in the Attributes list, and then click **-->** (right arrow button).

The attribute moves to the Logged Attributes list.

Tip Use the vertical scroll bar to find attributes that are not visible in the list box.

b. To remove an attribute from the log, select the attribute in the Logged Attributes list, and then click **<--** (left arrow button).

The attribute moves to the Attributes list.

Tip Use the vertical scroll bar to find attributes not visible in the list box.

c. To set the attributes in the Logged Attributes list back to the default selections, click **Reset Columns**.

Step 5 In the ODBC Connection Settings table, configure ACS to communicate with the ODBC database:

a. From the Data Source list, select the system DSN that you created to allow ACS to send ODBC logging data to your relational database.

b. In the **Username** box, type the username of a user account in your relational database (up to 80 characters).

Note The user must have sufficient privileges in the relational database to write the ODBC logging data to the appropriate table.

c. In the **Password** box, type the password (up to 80 characters) for the relational database user account you specified in Step b.

d. In the **Table Name** box, type the name (up to 80 characters) of the table to which you want ODBC logging data appended.

Step 6 Click **Submit**.

ACS saves the log configuration.

Step 7 Click the name of the ODBC log that you are configuring.

The ODBC log configuration page reappears.

Step 8 Click **Show Create Table**.

The right side of the browser displays an SQL create table statement for Microsoft SQL Server. The table name is the name that is specified in the **Table Name** box. The column names are the attributes that are specified in the Logged Attributes list.

Note The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.

Step 9 Using the information provided in the generated SQL, create a table in your relational database for this ODBC log.

Note For ODBC logging to work, the table name and the column names must exactly match the names in the generated SQL.

Step 10 Continuing in ACS, access the configuration page for the ODBC log that you are configuring:

a. In the navigation bar, click **System Configuration**.

b. Click **Logging**.

c. Click the name of the ODBC log that you are configuring.

The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log that you selected.

Step 11 Select the **Log to ODBC** *log* **report** check box, where *log* is the name of the ODBC log that you selected.

Step 12 Click **Submit**.

ACS begins sending logging data to the relational database table specified by using the system DSN you configured.

Remote Logging

This section discusses the remote logging capabilities of ACS.

This section contains the following topics:

- About Remote Logging, page 11-19
- Implementing Centralized Remote Logging, page 11-20
- Remote Logging Options, page 11-21
- Enabling and Configuring Remote Logging, page 11-21
- Disabling Remote Logging, page 11-22

About Remote Logging

You can use the Remote Logging feature to centralize accounting logs that multiple ACSs generate. You can configure each ACS to point to one ACS to use as a central logging server. The central logging ACS still performs AAA functions, but it also is the repository for accounting logs that it receives. For more information about ACS accounting logs, see Accounting Logs, page 11-4.

The Remote Logging feature enables ACS to send accounting data received from AAA clients directly to the CSLog service on the remote logging server, where the accounting data is written to the logs. The logging server generates the accounting logs in the formats that it is configured to use—CSV and ODBC—regardless of the local logging configuration on the ACSs that are sending the data to the central logging server.

ACS listens on TCP port 2001 for remote logging communication. Remote logging data is encrypted by a 128-bit proprietary algorithm.

Note The Remote Logging feature does not affect the forwarding of accounting data for proxied authentication requests. ACS only applies Remote Logging settings to accounting data for sessions that the proxy authenticates when accounting data for sessions that the proxy authenticates is logged locally. For more information about proxied authentication requests and accounting data for sessions that the proxy authenticates, see Proxy Distribution Table Configuration, page 4-23.

Implementing Centralized Remote Logging

Before You Begin

Ensure that gateway devices between remote ACSs and the central logging ACS permit the central logging ACS to receive data on TCP port 2001.

To implement centralized remote logging:

Step 1 On a computer on which you will to store centralized logging data, install ACS. For information about installing ACS, see the *Installation Guide for Cisco Secure ACS for Windows*.

Step 2 In the ACS that is running on the central logging server:

a. Configure the accounting logs as needed. All accounting data that is sent to the central logging server will be recorded in the way that you configure accounting logs on this ACS. For information about accounting logs, see Accounting Logs, page 11-4.

Accounting logs can be recorded in CSV or ODBC format. For information about configuring CSV logs, see Working with CSV Logs, page 11-10. For information about configuring ODBC logs, see Configuring an ODBC Log, page 11-17.

b. Add to the AAA Servers table each ACS that the central logging server is to receive accounting data from. For more information, see AAA Server Configuration, page 4-15.

Note If the central logging server is to log watchdog and update packets for a ACS, you must check the Log Update/Watchdog Packets from this remote AAA Server check box for that ACS in the AAA Servers table.

Step 3 For each ACS that will send its accounting data to the central logging server:

a. Add the central logging server to the AAA Servers table in Network Configuration. For more information, see AAA Server Configuration, page 4-15.

b. Enable remote logging. For more information, see Enabling and Configuring Remote Logging, page 11-21.

Step 4 If you want to create other central logging servers for use as secondary servers or as mirrored logging servers, perform Step 1 through Step 3 for each additional server.

Remote Logging Options

ACS provides the following remote logging options. These options appear on the Remote Logging Setup page.

- **Do not log Remotely**— ACS writes accounting data for locally authenticated sessions only to the local logs that are enabled.
- **Log to all selected remote log services**— ACS sends accounting data for locally authenticated sessions to all ACSs in the Selected Log Services list.
- **Log to subsequent remote log services on failure**— ACS sends accounting data for locally authenticated sessions to the first ACS that is operational in the Selected Log Services list. You can, therefore, configure one or more backup central logging servers so that no accounting data is lost if the first central logging server fails or is otherwise unavailable to ACS.
- **Remote Log Services**—This list represents the ACSs that are configured in the Remote Agents table in Network Configuration to which ACS *does not* send accounting data for locally authenticated sessions.
- **Selected Log Services**—This list represents the ACSs that are configured in the Remote Agents table in Network Configuration to which ACS *does* send accounting data for locally authenticated sessions.

Enabling and Configuring Remote Logging

Note Before configuring the Remote Logging feature on ACS, ensure that you have configured your central logging ACS. For more information, see Implementing Centralized Remote Logging, page 11-20.

To enable and configure remote logging:

Step 1 To enable the Remote Logging feature in the web interface:

a. Click **Interface Configuration**.

b. Click **Advanced Options**.

c. Select the **Remote Logging** check box.

d. Click **Submit**.

ACS displays the Remote Logging link on the Logging page in the System Configuration section.

Step 2 Click **System Configuration**.

Step 3 Click **Logging**.

The Logging Configuration page appears.

Step 4 Click **Remote Logging**.

Step 5 Select the applicable remote logging option:

a. To send the accounting information for this ACS to more than one ACS, select the **Log to all selected remote log services** option.

b. To send the accounting information for this ACS to one ACS, select the **Log to subsequent remote log services on failure** option.

Note Use the **Log to subsequent remote log services on failure** option when you want to configure ACS to send accounting data to a second remote ACS if the first ACS fails.

Step 6 For each remote ACS that you want to include in the Selected Log Services list:

a. In the Remote Log Services list, select the name of a ACS to which you want to send accounting data for locally authenticated sessions.

Note The ACSs that are available in the Remote Log Services list is determined by the AAA Servers table in Network Configuration. For more information about the AAA Servers table, see AAA Server Configuration, page 4-15.

b. Click **-->** (right arrow button) to move the selected ACS to the Selected Log Services list.

Step 7 To assign an order to the servers in the Selected Log Services list, click **Up** and **Down** to move selected ACSs until the order is what you need.

Note If the **Log to subsequent remote log services on failure** option is selected, ACS logs to the first accessible ACS in the Selected Log Services list.

Step 8 Click **Submit**.

ACS saves and implements the remote logging configuration that you specified.

Disabling Remote Logging

By disabling the Remote Logging feature, you prevent ACS from sending its accounting information to a central logging ACS.

To disable remote logging:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Step 3 Click **Remote Logging**.

Step 4 Select the **Do not log Remotely** option.

Step 5 Click **Submit**.

ACS no longer sends its accounting information for locally authenticated sessions to remote logging servers.

Service Logs

Service logs are considered diagnostic logs which you use for troubleshooting or debugging purposes only. These logs are not intended for general use by ACS administrators; instead, they are mainly sources of information for Cisco support personnel. Service logs contain a record of all ACS service actions and activities. When service logging is enabled, each service generates a log whenever the service is running, regardless of whether you are using the service. For example, RADIUS service logs are created even if you are not using the RADIUS protocol in your network.

This section covers:

- Services Logged, page 11-23
- Configuring Service Logs, page 11-24
- Helping Customer Support Gather Data, page 11-25

For more information about ACS services, see Chapter 1, "Overview."

Services Logged

ACS generates logs for the following services:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

These files are located in the `\Logs` subdirectory of the applicable service directory. For example, the following is the default directory for the ACS authentication service:

`c:\Program Files\CiscoSecure ACS v`*x.x*`\CSAuth\Logs`

The most recent debug log is named:

SERVICE`.log`

where *SERVICE* is the name of the applicable service.
Older debug logs are named with the year, month, and date on which they were created. For example, a file that was created on July 13, 1999, would be named:

SERVICE `1999-07-13.log`

where *SERVICE* is the name of the applicable service.

If you selected the Day/Month/Year format, the file would be named:

SERVICE `13-07-1999.log`

Configuring Service Logs

You can configure how ACS generates and manages the service log file. The options for configuring the service log file are:

- **Level of detail**—You can set the service log file to contain one of three levels of detail:
  - **None**—No log file is generated.
  - **Low**—Only start and stop actions are logged. This is the default setting.
  - **Full**—All services actions are logged.
- **Generate new file**—You can control how often a new service log file is created:
  - **Every Day**— ACS generates a new log file at 12:01 A.M. local time every day.
  - **Every Week**— ACS generates a new log file at 12:01 A.M. local time every Sunday.
  - **Every Month**— ACS generates a new log file at 12:01 A.M. on the first day of every month.
  - **When Size is Greater than *x* KB**— ACS generates a new log file after the current service log file reaches the size specified, in kilobytes, by *x*.
- **Manage Directory**—You can control how long service log files are kept:
  - **Keep only the last *x* files**— ACS retains up to the number of files specified by *x*.
  - **Delete files older than *x* days**— ACS retains only those service logs that are not older than the number of days specified by *x*.

To configure how ACS generates and manages the service log file:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the computer that is running ACS.

Step 3 To disable the service log file, under Level of detail, select the **None** option.

After you click **Restart**, ACS does not generate a new service log file.

Step 4 To configure how often ACS creates a service log file, select one of the options under **Generate New File**.

Note Settings under **Generate New File** have no effect if you selected **None** under Level of detail.

Step 5 To determine which service log files ACS keeps:

a. Select the **Manage Directory** check box.

b. To limit the number of service log files that ACS retains, select the **Keep only the last *x* files** option and in the *x* box type the number of files that you want ACS to retain.

c. To limit the age of service log files that ACS retains, select the **Delete files older than *x* days** option and in the *x* box type the number of days for which ACS should retain a service log file before deleting it.

Step 6 Click **Restart**.

ACS restarts its services and implements the service log settings that you specified.

Helping Customer Support Gather Data

Before You Begin

So that customer support will have enough data to research potential issues, you must set your services log configuration correctly. Choose **System Configuration > Service Control** and select **Full**. Ensure that you have enough disk space to handle your log entries.

If a problem exists on your ACS, customer support will ask you to create a *package.cab* file. The *package.cab* file contains various files including:

- **Certificate files**—The ACS server certificate, as well as the certificate's CA.
- ***Admin.txt***—Contains information regarding ACS administrators.
- ***Host.txt*** **and** ***HostServices.txt***—Contain information regarding hosts and hosts configuration.
- ***NDG.txt***—Contains configured network device groups.
- ***DictionaryKey.txt*** **and** ***DictionaryValue.txt***—Contains ACS dictionary files.

To create a *package.cab* file:

Step 1 At the command prompt, type **drwtsn32**.

Check the Dr. Watson settings to be sure the **Dump all Symbol Table** and **Dump All Thread Contents** options are selected in addition to the default options.

Step 2 Go to the directory in which ACS was installed.

Step 3 Type **CSSupport.exe**.

Run the executable with all default options. The program will collect all the necessary information including Dr. Watson logs and place them in a file called *package.cab*. The location of the file appears when the executable is finished.

Note When creating a *package.cab* file that is larger than 2GB, additional *.cab* files are created due to the size limit of the packer. The sequence is: the first package name is *package.cab*, the second is *package1.cab*, and so on, until the N package, *packageN.cab*, where N is the number of packages minus one. The files are saved in the same location that is specified before the packing begins. These files are not standalone and all of them must be sent to package. Problems with the packed file (package.cab) may arise if there is not enough hard-disk space.

CHAPTER 12

Administrators and Administrative Policy

This chapter addresses the features found in the Administration Control section of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains the following topics:

- Administrator Accounts, page 12-1
- Access Policy, page 12-8
- Session Policy, page 12-11
- Audit Policy, page 12-12

Administrator Accounts

This section provides details about ACS administrators.

This section contains the following topics:

- About Administrator Accounts, page 12-1
- Administrator Privileges, page 12-2
- Adding an Administrator Account, page 12-4
- Editing an Administrator Account, page 12-5
- Unlocking a Locked Out Administrator Account, page 12-7
- Deleting an Administrator Account, page 12-7

About Administrator Accounts

Administrators are the only users of the ACS web interface. To access the ACS web interface from a browser run elsewhere than on the ACS Windows server itself, you must log in to ACS by using an administrator account. If your ACS is so configured, you may need to log in to ACS even in a browser run on the ACS Windows server. For more information about automatic local logins, see Session Policy, page 12-11.

Note ACS administrator accounts are unique to ACS. They are not related to other administrator accounts, such as Windows users with administrator privileges.

In the web interface, an administrator can configure any of the features provided in ACS; however, the ability to access various parts of the web interface can be limited by revoking privileges to those parts of the web interface that a given administrator is not allowed to access.

By default no privileges are granted to a new administrator, unless Grant All is selected.

For example, you may want to limit access to the Network Configuration section of the web interface to administrators whose responsibilities include network management. To do so, you would select only the Network Configuration privilege for applicable administrator accounts. For more information about administrator privileges, see Administrator Privileges, page 12-2.

ACS administrator accounts have no correlation with ACS user accounts or username and password authentication. ACS stores accounts created for authentication of network service requests and those created for ACS administrative access in separate internal databases.

Note When ACS is running on Windows 2003, the ACS administrator account that runs the ACS services must have a Domain Administrator account to authenticate against Windows 2003.

Administrator Privileges

You can grant appropriate privileges to each ACS administrator by assigning privileges on an administrator-by-administrator basis. You control privileges by selecting the options from the Administrator Privileges table on the Add Administrator or Edit Administrator pages. These options are:

- **User and Group Setup**—Contains the following privilege options for the User Setup and Group Setup sections of the web interface:
  - **Add/Edit users in these groups**—Enables the administrator to add or edit users and to assign users to the groups in the Editable groups list.
  - **Setup of these groups**—Enables the administrator to edit the settings for the groups in the Editable groups list.
  - **Available Groups**—Lists the user groups for which the administrator *does not* have edit privileges and to which the administrator *cannot* add users.
  - **Editable Groups**—Lists the user groups for which the administrator *does* have edit privileges and to which the administrator *can* add users.
- **Shared Profile Components**—Contains the following privilege options for the Shared Profile Components section of the web interface:
  - **Network Access Restriction Sets**—Allows the administrator full access to the Network Access Restriction Sets feature.
  - **Network Access Filtering Sets**—Allows the administrator full access to the Network Access Filtering Sets feature.
  - **Downloadable ACLs**—Allows the administrator full access to the Downloadable PIX ACLs feature.
  - **RADIUS Authorization Components**—Allows the administrator full access to RAC.
  - **Create New Device Command Set Type**—Allows the administrator account to be used as valid credentials by another Cisco application for adding new device command set types. New device command set types that are added to ACS using this privilege appear in the Shared Profile Components section of the web interface.

  - **Shell Command Authorization Sets**—Allows the administrator full access to the Shell Command Authorization Sets feature.
  - **PIX/ASA Command Authorization Sets**—Allows the administrator full access to the PIX/ASA Command Authorization Sets feature.

Note Additional command authorization set privilege options may appear, if other Cisco network management applications, such as CiscoWorks, have updated the configuration of ACS.

- **Network Configuration**—Allows the administrator full access to the features in the Network Configuration section of the web interface.
- **System Configuration—**Contains the privilege options for the features found in the System Configuration section of the web interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **Service Control**—For more information about this feature, see Service Control, page 8-1.
  - **Date/Time Format Control**—For more information about this feature, see Date Format Control, page 8-3.
  - **Logging Control**—For more information about this feature, see Logging, page 8-3.
  - **Password Validation**—For more information about this feature, see Local Password Management, page 8-4.
  - **DB Replication**—For more information about this feature, see ACS Internal Database Replication, page 9-1.
  - **RDBMS Synchronization**—For more information about this feature, see RDBMS Synchronization, page 9-17.
  - **IP Pool Address Recovery**—For more information about this feature, see IP Pools Address Recovery, page 9-33.
  - **IP Pool Server Configuration**—For more information about this feature, see IP Pools Server, page 9-28.
  - **ACS Backup**—For more information about this feature, see ACS Backup, page 8-7.
  - **ACS Restore**—For more information about this feature, see ACS System Restore, page 8-11.
  - **ACS Service Management**—For more information about this feature, see ACS Active Service Management, page 8-13.
  - **VoIP Accounting Configuration**—For more information about this feature, see VoIP Accounting Configuration, page 8-15.
  - **ACS Certificate Setup**—For more information about this feature, see ACS Certificate Setup, page 10-25.
  - **Global Authentication Setup**—For more information about this feature, see Global Authentication Setup, page 10-19.
- **Interface Configuration**—Allows the administrator full access to the features in the Interface Configuration section of the web interface.
- **Administration Control**—Allows the administrator full access to the features in the Administration Control section of the web interface.
- **External User Databases**—Allows the administrator full access to the features in the External User Databases section of the web interface.

- **Posture Validation**—Allows the administrator access to Network Admission Control (NAC) configuration.
- **Network Access Profiles**—Allows the administrator access to service-based policy configuration.
- **Reports & Activity**—Contains the privilege options for the reports and features found in the Reports and Activity section of the web interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **TACACS+ Accounting**—For more information about this report, see Accounting Logs, page 11-4.
  - **TACACS+ Administration**—For more information about this report, see Accounting Logs, page 11-4.
  - **RADIUS Accounting**—For more information about this report, see Accounting Logs, page 11-4.
  - **VoIP Accounting**—For more information about this report, see Accounting Logs, page 11-4.
  - **Passed Authentications**—For more information about this report, see Accounting Logs, page 11-4.
  - **Failed Attempts**—For more information about this report, see Accounting Logs, page 11-4.
  - **Logged-in Users**—For more information about this report, see Dynamic Administration Reports, page 11-6.
  - **Purge of Logged-in Users**—For more information about this feature, see Deleting Logged-in Users, page 11-7.
  - **Disabled Accounts**—For more information about this report, see Dynamic Administration Reports, page 11-6.
  - **ACS Backup and Restore**—For more information about this report, see ACS System Logs, page 11-8.
  - **DB Replication**—For more information about this report, see ACS System Logs, page 11-8.
  - **RDBMS Synchronization**—For more information about this report, see ACS System Logs, page 11-8.
  - **Administration Audit**—For more information about this report, see ACS System Logs, page 11-8.
  - **ACS Service Monitor**—For more information about this report, see ACS System Logs, page 11-8.
  - **User Change Password**—For more information about this report, see ACS System Logs, page 11-8.

Adding an Administrator Account

Before You Begin

For descriptions of the options available while adding an administrator account, see Administrator Privileges, page 12-2.

To add a ACS administrator account:

Step 1 In the navigation bar, click **Administration Control**.

Step 2 Click **Add Administrator**.

The Add Administrator page appears.

Step 3 Complete the boxes in the Administrator Details table:

a. In the Administrator Name box, type the login name (up to 32 characters) for the new ACS administrator account.

b. In the Password box, type the password (from 4 to 32 characters) for the new ACS administrator account.

c. In the Confirm Password box, type the password a second time.

Step 4 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

All privilege options are selected. All user groups move to the Editable groups list.

Tip To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Step 5 To grant user and user group editing privileges:

a. Check the desired check boxes under User & Group Setup.

b. To move a user group to the Editable groups list, select the group in the Available groups list, and then click **-->** (right arrow button).

The selected group moves to the Editable groups list.

c. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click **<--** (left arrow button).

The selected group moves to the Available groups list.

d. To move all user groups to the Editable groups list, click **>>**.

The user groups in the Available groups list move to the Editable groups list.

e. To remove all user groups from the Editable groups list, click **<<**.

The user groups in the Editable groups list move to the Available groups list.

Step 6 To grant any of the remaining privilege options, in the Administrator Privileges table, check the applicable check boxes.

Step 7 Click **Submit**.

ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.

Editing an Administrator Account

You can edit a ACS administrator account to change the privileges granted to the administrator. You can effectively disable an administrator account by revoking all privileges.

Note You cannot change the name of an administrator account; however, you can delete an administrator account and then create an account with the new name. For information about deleting an administrator account, see Deleting an Administrator Account, page 12-7. For information about creating an administrator account, see Adding an Administrator Account, page 12-4.

For information about administrator privilege options, see Administrator Privileges, page 12-2.

Before You Begin

For descriptions of the options available while editing an administrator account, see Administrator Privileges, page 12-2.

To edit ACS administrator account privileges:

Step 1 In the navigation bar, click **Administration Control**.

ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose privileges you want to edit.

The Edit Administrator *name* page appears, where *name* is the name of the administrator account that you just selected.

Step 3 To change the administrator password:

a. In the **Password** box, double-click the asterisks (*), and then type the new password (from 4 to 32 characters) for the administrator.

The new password replaces the existing, masked password.

b. In the **Confirm Password** box, double-click the asterisks, and then type the new administrator password a second time.

The new password is effective immediately after you click Submit in Step 9.

Step 4 If the Reset current failed attempts count check box appears below the Confirm Password box and you want to allow the administrator whose account you are editing to access the ACS web interface, check the **Reset current failed attempts count** check box.

Note If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator cannot access ACS unless you complete Step 4. For more information about re-enabling an administrator account, see Unlocking a Locked Out Administrator Account, page 12-7.

Step 5 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

All privilege options are selected. All user groups move to the Editable groups list.

Step 6 To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

All privileges options are cleared. All user groups move to the Available groups list.

Step 7 To grant user and user group editing privileges, follow these steps:

a. Under User & Group Setup, check the applicable check boxes.

b. To move all user groups to the Editable groups list, click **>>**.

The user groups in the Available groups list move to the Editable groups list.

c. To move a user group to the Editable groups list, select the group in the Available groups list, and then click **-->** (right arrow button).

The selected group moves to the Editable groups list.

d. To remove all user groups from the Editable groups list, click **<<**.

The user groups in the Editable groups list move to the Available groups list.

e. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click **<--** (left arrow button).

The selected group moves to the Available groups list.

Step 8 To grant any remaining privilege options, check the applicable check boxes in the Administrator Privileges table.

Step 9 To revoke any remaining privilege options, clear the applicable check boxes in the Administrator Privileges table.

Step 10 Click **Submit**.

ACS saves the changes to the administrator account.

Unlocking a Locked Out Administrator Account

ACS disables the accounts of administrators who have attempted to access the ACS web interface and have provided an incorrect password in more successive attempts than is specified on the Session Policy Setup page. Until the failed attempts counter for a disabled administrator account is reset, the administrator cannot access the web interface.

For more information about configuring how many successive failed login attempts can occur before ACS disables an administrator account, see Session Policy, page 12-11.

To reset the failed attempts count for an administrator:

Step 1 In the navigation bar, click **Administration Control**.

ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose account you want to re-enable.

The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator account cannot access the web interface.

Step 3 Check the **Reset current failed attempts count** check box.

Step 4 Click **Submit**.

ACS saves the changes to the administrator account.

Deleting an Administrator Account

You can delete a ACS administrator account when you no longer need it. We recommend deleting any unused administrator accounts.

To delete a ACS administrator account:

Step 1 In the navigation bar, click **Administration Control**.

ACS displays the Administration Control page.

Step 2 In the Administrators table, click the name of the administrator account that you want to delete.

The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

Step 3 Click **Delete**.

ACS displays a confirmation dialog box.

Step 4 Click **OK**.

ACS deletes the administrator account. The Administrators table on the Administration Control page no longer lists the administrator account that you deleted.

Access Policy

The Access Policy feature affects access to the ACS web interface. You can limit access by IP address and by the TCP port range used for administrative sessions. You can also enable secure socket layer (SSL) for access to the web interface.

This section contains the following topics:

- Access Policy Options, page 12-8
- Setting Up Access Policy, page 12-9

Access Policy Options

You can configure the following options on the Access Policy Setup page:

- **IP Address Filtering**—Contains the following IP address filtering options:
  - **Allow all IP addresses to connect**—Allow access to the web interface from any IP address.
  - **Allow only listed IP addresses to connect**—Allow access to the web interface only from IP addresses *inside* the address range(s) specified in the IP Address Ranges table.
  - **Reject connections from listed IP addresses**—Allow access to the web interface only from IP addresses *outside* the address range(s) specified in the IP Address Ranges table.
- **IP Address Ranges**—The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the start and end IP addresses. The IP addresses entered to define a range must differ only in the last octet (Class C format).

  The IP Address Ranges table contains one column of each of the following boxes:
  - **Start IP Address**—Defines the lowest IP address of the range specified in the current row.
  - **End IP Address**—Defines the highest IP address of the range specified in the current row.
- **HTTP Port Allocation**—Contains the following options for configuring TCP ports used for remote access to the web interface.
  - **Allow any TCP ports to be used for Administration HTTP Access**—Allow the ports used by administrative HTTP sessions to include the full range of TCP ports.

- **Restrict Administration Sessions to the following port range From Port *X* to Port *Y***—Restrict the ports used by administrative HTTP sessions to the range specified in the *X* and *Y* boxes, inclusive. The size of the range specified determines the maximum number of concurrent administrative sessions.

  ACS uses port 2002 to start all administrative sessions. You do not need to include port 2002 in the port range. Also, ACS does not allow you to define an HTTP port range that consists only of port 2002. Your port range must consist of at least one port other than port 2002.

  A firewall configured to permit HTTP traffic over the ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port that a web browser must address to initiate an administrative session.

Note We do not recommend allowing administration of ACS from outside a firewall. If you do choose to allow access to the web interface from outside a firewall, keep the HTTP port range as narrow as possible. This can help prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or "spoof," the IP address of a legitimate host to make use of the active administrative session HTTP port.

- **Secure Socket Layer Setup**—The Use HTTPS Transport for Administration Access check box defines whether ACS uses secure socket layer protocol to encrypt HTTP traffic between the CSAdmin service and a web browser used to access the web interface. When this option is enabled, all HTTP traffic between the browser and ACS is encrypted, as reflected by the URLs, which begin with HTTPS. Additionally, most browsers include an indicator for when a connection is SSL-encrypted.

  To enable SSL, you must have completed the steps in Installing an ACS Server Certificate, page 10-25, and Adding a Certificate Authority Certificate, page 10-27.

Setting Up Access Policy

For information about access policy options, see Access Policy Options, page 12-8.

Before You Begin

If you want to enable SSL for administrative access, before completing this procedure, you must have completed the steps in Installing an ACS Server Certificate, page 10-25, and Adding a Certificate Authority Certificate, page 10-27.

To set up ACS Access Policy:

Step 1 In the navigation bar, click **Administration Control**.

ACS displays the Administration Control page.

Step 2 Click **Access Policy**.

The Access Policy Setup page appears.

Step 3 To allow remote access to the web interface from any IP address, in the IP Address Filtering table, select the **Allow all IP addresses to connect** option.

Step 4 To allow remote access to the web interface only from IP addresses *within* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Allow only listed IP addresses to connect** option.

b. For each IP address range from within which you want to allow remote access to the web interface, complete one row of the IP Address Ranges table. In the **Start IP Address** box, type the lowest IP address (up to 16 characters) in the range. In the **End IP Address** box, type the highest IP address (up to 16 characters) in the range. Use dotted decimal format.

Note The IP addresses entered to define a range must differ only in the last octet.

Step 5 To allow remote access to the web interface only from IP addresses *outside* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Reject connections from listed IP addresses** option.

b. For each IP address range from outside which you want to allow remote access to the web interface, complete one row of the IP Address Ranges table. Type the lowest IP address (up to 16 characters) in the range in the **Start IP Address** box. Type the highest IP address (up to 16 characters) in the range in the **End IP Address** box.

Note The IP addresses entered to define a range must differ only in the last octet.

Step 6 If you want to allow ACS to use any valid TCP port for administrative sessions, under HTTP Port Allocation, select the **Allow any TCP ports to be used for Administration HTTP Access** option.

Step 7 If you want to allow ACS to use only a specified range of TCP ports for administrative sessions, follow these steps:

a. Under HTTP Port Allocation, select the **Restrict Administration Sessions to the following port range From Port** *X* **to Port** *Y* option.

b. In the *X* box type the lowest TCP port (up to 5 characters) in the range.

c. In the *Y* box type the highest TCP port (up to 5 characters) in the range.

Step 8 If you want to enable SSL encryption of administrator access to the web interface, under Secure Socket Layer Setup, check the **Use HTTPS Transport for Administration Access** check box.

Note To enable SSL, you must have completed the steps in Installing an ACS Server Certificate, page 10-25, and Adding a Certificate Authority Certificate, page 10-27.

Step 9 Click **Submit**.

ACS saves and begins enforcing the access policy settings.

If you have enabled SSL, at the next administrator login, ACS begins using HTTPS. Any current administrator sessions are unaffected.

Session Policy

The Session Policy feature controls various aspects of ACS administrative sessions.

This section contains the following topics:

- Session Policy Options, page 12-11
- Setting Up Session Policy, page 12-11

Session Policy Options

You can configure the following options on the Session Policy Setup page:

- **Session idle timeout (minutes)**—Defines the time in minutes that an administrative session, local or remote, must remain idle before ACS terminates the connection. This parameter applies to the ACS administrative session in the browser only. It does not apply to an administrative dial-up session.

  An administrator whose administrative session is terminated receives a dialog box asking whether the administrator wants to continue. If the administrator chooses to continue, ACS starts a new administrative session.

- **Allow Automatic Local Login**—Enables administrators to start an administrative session without logging in if they are using a browser on the computer running ACS. Such administrative sessions are conducted using a default administrator account named *local_login*. The local_login administrator account has all privileges. Local administrative sessions with automatic local login are recorded in the Administrative Audit report under the local_login administrator name.

  Note If there are no administrator accounts defined, no administrator name and password are required to access ACS locally. This prevents you from accidentally locking yourself out of ACS.

- **Respond to Invalid IP Address Connections**—Enables an error message in response to attempts to start a remote administrative session using an IP address that is invalid according to the IP address ranges configured in Access Policy. Disabling this option can help prevent unauthorized users from discovering ACS.

- **Lock out Administrator after *X* successive failed attempts—**Enables ACS to lock out an administrator after a number of successive failed attempts to log in to the web interface. The number of successive attempts is specified in the *X* box. If this check box is checked, the X box cannot be set to zero. If this check box is not checked, ACS allows unlimited successive failed login attempts by an administrator.

Setting Up Session Policy

For information about session policy options, see Session Policy Options, page 12-11.

To set up ACS Session Policy:

Step 1 In the navigation bar, click **Administration Control**.

ACS displays the Administration Control page.

Step 2 Click **Session Policy**.

The Session Policy Setup page appears.

Step 3 To define the number of minutes of inactivity after which ACS ends an administrative session, in the Session idle timeout (minutes) box, type the number of minutes (up to 4 characters).

Step 4 Set the automatic local login policy:

a. To allow administrators to log in to ACS locally without using their administrator names and passwords, check the **Allow Automatic Local Login** check box.

b. To require administrators to log in to ACS locally using their administrator names and passwords, clear the **Allow Automatic Local Login** check box.

Step 5 Set the invalid IP address response policy:

a. To configure ACS to respond with a message when an administrative session is requested from an invalid IP address, check the **Respond to invalid IP address connections** check box.

b. To configure ACS to send no message when an administrative session is requested from an invalid IP address, clear the **Respond to invalid IP address connections** check box.

Step 6 Set the failed administrative login attempts policy:

a. To enable ACS to lock out an administrator after a specified number of successive failed administrative login attempts, check the **Lock out Administrator after** *X* **successive failed attempts** check box.

b. In the *X* box, type the number of successive failed login attempts after which ACS locks out an administrator. The *X* box accepts up to 4 characters.

Step 7 Click **Submit**.

ACS saves and begins enforcing the session policy settings you made.

Audit Policy

The Audit Policy feature controls the generation of the Administrative Audit log.

For more information about enabling, viewing, or configuring the Administrative Audit log, see ACS System Logs, page 11-8.

CHAPTER 13

User Databases

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, authenticates users against one of several possible databases, including its internal database. You can configure ACS to authenticate users with more than one type of database. With this flexibility you can use user account data that is collected in different locations without having to explicitly import the users from each external user database into the ACS internal database. You can also apply different databases to different types of users, depending on the security requirements that are associated with user authorizations on your network. For example, a common configuration is to use a Windows user database for standard network users and a token server for network administrators.

Note For information about the Unknown User Policy and group mapping features, see Chapter 16, "Unknown User Policy" and Chapter 17, "User Group Mapping and Specification."

This chapter contains the following topics:

- ACS Internal Database, page 13-1
- About External User Databases, page 13-3
- Windows User Database, page 13-5
- Generic LDAP, page 13-22
- ODBC Database, page 13-34
- LEAP Proxy RADIUS Server Database, page 13-46
- Token Server User Databases, page 13-48
- Deleting an External User Database Configuration, page 13-54

ACS Internal Database

The ACS internal database supports authentication by using:

- American Standard Code for Information Interchange (ASCII)
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP)
- AppleTalk Remote Access Protocol (ARAP)
- Lightweight and Efficient Application Protocol (LEAP)

- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP) Extensible Authentication Protocol-Generic Token Card (EAP-GTC)
- Protected Extensible Authentication Protocol (PEAP) Extensible Authetication Protocol-Microsoft-Challenge Handshake Authentication Protocol (EAP-MS-CHAPv2)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) (phase zero and phase two)

The ACS internal database is crucial for the authorization process. Regardless of whether a user is authenticated by the internal user database or by an external user database, ACS authorizes network services for users based on group membership and specific user settings in the ACS internal database. Thus, all users that ACS authenticates, even those authenticated by an external user database, have an account in the ACS internal database.

About the ACS Internal Database

For users who are authenticated by using the ACS internal database, ACS stores user passwords in a database which is protected by an administration password and encrypted by using the AES 128 algorithm. For users who are authenticated with external user databases, ACS does not store passwords in the ACS internal database.

Unless you have configured ACS to authenticate users with an external user database, ACS uses usernames and passwords in the ACS internal database during authentication. For more information about specifying an external user database for authentication of a user, see Adding a Basic User Account, page 7-3.

User Import and Creation

There are five ways to create user accounts in ACS for Windows. Of these, Relational Database Management System (RDBMS) Synchronization and `CSUtil.exe` support importing user accounts from external sources.

- **ACS web interface**—The web interface provides the ability to create user accounts manually, one user at a time. Regardless of how a user account was created, you can edit a user account by using the web interface. For detailed steps, see Adding a Basic User Account, page 7-3.
- **Unknown User Policy**—The Unknown User Policy enables ACS to add users automatically when it finds a user without an account in an external user database. The creation of a user account in ACS occurs only when the user attempts to access the network and is successfully authenticated by an external user database. For more information, see Chapter 16, “Unknown User Policy.”

  If you use the Unknown User Policy, you can also configure group mappings so that each time a user who was added to ACS by the Unknown User Policy is authenticated, the user group assignment is made dynamically. For some external user database types, user group assignment is based on group membership in the external user database. For other database types, all users who were authenticated by a given database are assigned to a single ACS user group. For more information about group mapping, see Chapter 17, “User Group Mapping and Specification.”

- **RDBMS Synchronization**—You can use RDBMS Synchronization to create large numbers of user accounts and configure many settings for user accounts. We recommend that you use this feature whenever you need to import users by bulk; however, setting up RDBMS Synchronization for the first time requires several important decisions and time to implement them. For more information, see RDBMS Synchronization, page 9-17.
- **CSUtil.exe**—The `CSUtil.exe` command-line utility provides a simple means of creating basic user accounts. When compared to RDBMS Synchronization, its functionality is limited; however, it is simple to prepare for importing basic user accounts and assigning users to groups. For more information, see Appendix D, "CSUtil Database Utility."
- **Database Replication**—Database Replication creates user accounts on a secondary ACS by overwriting all existing user accounts on a secondary ACS with the user accounts from the primary ACS. Any user accounts that are unique to a secondary ACS are lost in the replication. For more information, see ACS Internal Database Replication, page 9-1.

About External User Databases

You can configure ACS to forward authentication of users to one or more external user databases. Support for external user databases means that ACS does not require that you create duplicate user entries in the user database. In organizations in which a substantial user database already exists, ACS can leverage the work already invested in building the database without any additional input.

In addition to performing authentication for network access, ACS can perform authentication for TACACS+ enabling privileges by using external user databases. For more information about TACACS+ enable passwords, see Setting TACACS+ Enable Password Options for a User, page 7-23.

Note You can only use external user databases to authenticate users and to determine the group to which ACS assigns a user. The ACS internal database provides all authorization services. With few exceptions, ACS cannot retrieve authorization data from external user databases. Exceptions are noted where applicable in the discussions of specific databases in this chapter. For more information about group mapping for unknown users, see Chapter 17, "User Group Mapping and Specification."

Users can be authenticated by using the following databases:

- Windows Database
- Generic Lightweight Directory Access Protocol (LDAP)
- Novell NetWare Directory Services (NDS)
- Open Database Connectivity (ODBC)-compliant relational databases
- LEAP Proxy Remote Access Dial-In User Service (RADIUS) servers
- Rivest, Shamir, and Adelman (RSA) SecurID token servers
- RADIUS-compliant token servers

For ACS to interact with an external user database, ACS requires an API for third-party authentication source. The ACS communicates with the external user database by using the API. For Windows user databases and Generic LDAP, the program interface for the external authentication is local to ACS. In these cases, no further components are required.

In the case of Novell NDS authentication, you must install the Novell Requestor on the same Windows server as ACS.

In the case of Open Database Connectivity (ODBC) authentication sources, in addition to the Windows ODBC interface, you must install the third-party ODBC driver on the ACS Windows server.

To communicate with an RSA token server, you must have installed software components that RSA provides. For token servers by other vendors, the standard RADIUS interface serves as the third-party API.

Authenticating with External User Databases

Authenticating users with an external user database requires more than configuring ACS to communicate with an external user database. Performing one of the configuration procedures in this chapter for an external database does not, on its own, instruct ACS to authenticate any users with that database.

After you have configured ACS to communicate with an external user database, you can configure ACS to authenticate users with the external user database in one of two ways:

- **By Specific User Assignment**—You can configure ACS to authenticate specific users with an external user database. To do this, the user must exist in the ACS internal database and you must set the Password Authentication list in User Setup to the external user database that ACS should use to authenticate the user.

  While setting the Password Authentication for every user account is time-consuming, this method of determining which users are authenticated with an external user database is secure because it requires explicit definition of who should authenticate by using the external user database. In addition, the users may be placed in the desired ACS group and thereby receive the applicable access profile.

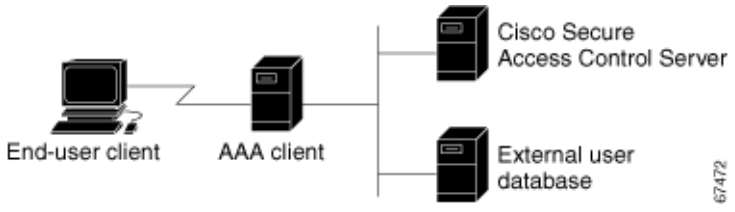
- **By Unknown User Policy**—You can configure ACS to attempt authentication of users who are not in the ACS internal database by using an external user database. You do not need to define new users in the ACS internal database for this method. For more information about the Unknown User Policy, see About Unknown User Authentication, page 16-3.

You can also configure ACS with both of the previous methods; these two methods are not mutually exclusive.

External User Database Authentication Process

When ACS attempts user authentication with an external user database, it forwards the user credentials to the external user database. The external user database passes or fails the authentication request from ACS. On receiving the response from the external user database, ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the external user database. Figure 13-1 shows a AAA configuration with an external user database.

Figure 13-1 A Simple AAA Scenario



The specifics of the method that is used to communicate with the external user database vary with the database type. For LDAP and Novell NDS, ACS uses TCP connections. For Windows user databases, ACS uses the authentication API provided in the Windows operating system. With the exception of RSA token servers, ACS communicates with token servers by using RADIUS. For RSA token servers, ACS acts an RSA client in order to use the RSA proprietary interface.

For more information, see the section regarding the database type in which you are interested.

Windows User Database

You can configure ACS to use a Windows user database to authenticate users.

This section contains the following topics:

- Windows User Database Support, page 13-6
- Authentication with Windows User Databases, page 13-6
- Trust Relationships, page 13-7
- Windows Dial-Up Networking Clients, page 13-7
  - Windows Dial-Up Networking Clients with a Domain Field, page 13-7
  - Windows Dial-Up Networking Clients without a Domain Field, page 13-7
- Usernames and Windows Authentication, page 13-8
  - Username Formats and Windows Authentication, page 13-8
  - Nondomain-Qualified Usernames, page 13-9
  - Domain-Qualified Usernames, page 13-9
  - UPN Usernames, page 13-10
- EAP and Windows Authentication, page 13-10
  - EAP-TLS Domain Stripping, page 13-10
  - Machine Authentication, page 13-11
  - Machine Access Restrictions, page 13-13
  - Microsoft Windows and Machine Authentication, page 13-14
  - Enabling Machine Authentication, page 13-16
- User-Changeable Passwords with Windows User Databases, page 13-17
- Preparing Users for Authenticating with Windows, page 13-18
- Windows User Database Configuration Options, page 13-18
- Configuring a Windows External User Database, page 13-21

Windows User Database Support

ACS supports the use of Windows external user databases for:

- **User Authentication**— ACS supports ASCII, PAP, MS-CHAP (versions 1 and 2), LEAP, PEAP (EAP-GTC), PEAP (EAP-MS-CHAPv2), and EAP-FAST (phase zero and phase two) authentication with Windows Security Accounts Manager (SAM) database or a Windows Active Directory database. ACS also supports EAP-TLS authentication with a Windows Active Directory database. Windows external databases support no other authentication protocols.

  Note A different external user database might support authentication protocols that are not supported with Windows external user databases. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-7.

- **Machine Authentication**—ACS supports machine authentication with EAP-TLS and PEAP (EAP-MS-CHAPv2). For more information, see EAP and Windows Authentication, page 13-10.
- **Group Mapping for Unknown Users**— ACS supports group mapping for unknown users by requesting group membership information from Windows user databases. For more information about group mapping for users authenticated with a Windows user database, see Group Mapping by Group Set Membership, page 17-3.
- **Password-Aging**— ACS supports password aging for users who are authenticated by a Windows user database. For more information, see User-Changeable Passwords with Windows User Databases, page 13-17.
- **Dial-in Permissions**—ACS supports use of dial-in permissions from Windows user databases. For more information, see Preparing Users for Authenticating with Windows, page 13-18.
- **Callback Settings**—ACS supports use of callback settings from Windows user databases. For information about configuring ACS to use Windows callback settings, see Setting the User Callback Option, page 7-6.

Authentication with Windows User Databases

ACS forwards user credentials to a Windows database by passing the user credentials to the Windows operating system of the computer that is running ACS. The Windows database passes or fails the authentication request from ACS. When receiving the response from the Windows database, ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the Windows database.

ACS grants authorization based on the ACS group to which the user is assigned. While you can determine the group to which a user is assigned information from the Windows database, it is ACS that grants authorization privileges.

To further control access by a user, you can configure ACS to also check the setting for granting dial-in permission to the user. This setting is labeled Grant dialin permission to user in Windows NT and Allow access in the Remote Access Permission area in Windows 2000 and Windows 2003. If this feature is disabled for the user, access is denied; even if the username and password are typed correctly.

Trust Relationships

ACS can take advantage of trust relationships established between Windows domains. If the domain that contains ACS trusts another domain, ACS can authenticate users whose accounts reside in the other domain. ACS can also reference the Grant dialin permission to user setting across trusted domains.

Note If ACS is running on a member server, rather than a domain controller, taking advantage of trust relationships depends on proper configuration of ACS at installation. For more information, see "Windows Authentication from a Member Server" in the *Installation Guide for Cisco Secure ACS for Windows*.

ACS can take advantage of indirect trusts for Windows authentication. Consider the example of Windows domains A, B, and C, where ACS resides on a server in domain A. Domain A trusts domain B, but no trust relationship is established between domain A and domain C. If domain B trusts domain C, ACS in domain A can authenticate users whose accounts reside in domain C, making use of the indirect trust of domain C.

For more information on trust relationships, refer to your Microsoft Windows documentation.

Windows Dial-Up Networking Clients

The dial-up networking clients for Windows NT/2000/2003/XP Professional and Windows 95/98/Millennium Edition (ME)/XP Home enable users to connect to your network remotely; but the fields that are provided differ.

Windows Dial-Up Networking Clients with a Domain Field

If users dial in to your network by using the dial-up networking client that is provided with Windows NT, Windows 2000, Windows 2003, or Windows XP Professional, three fields appear:

- **username**—Type your username.
- **password**—Type your password.
- **domain**—Type your valid domain name.

Note For more information about the implications of completing or leaving the domain box blank, see Nondomain-Qualified Usernames, page 13-9.

Windows Dial-Up Networking Clients without a Domain Field

If users access your network by using the dial-up networking client that is provided with Windows 95, Windows 98, Windows ME, or Windows XP Home, two fields appear:

- **username**—Type your username.

Note You can also prefix your username with the name of the domain in to which you want to log. For more information about the implications of prefixing or not prefixing the domain name before the username, see Nondomain-Qualified Usernames, page 13-9.

- **password**—Type your password.

Usernames and Windows Authentication

This section contains the following topics:

- Username Formats and Windows Authentication, page 13-8
- Nondomain-Qualified Usernames, page 13-9
- Domain-Qualified Usernames, page 13-9
- UPN Usernames, page 13-10

Username Formats and Windows Authentication

ACS supports Windows authentication for usernames in a variety of formats. When ACS attempts Windows authentication, it first determines the username format and submits the username to Windows in the applicable manner. To implement reliable Windows authentication with ACS, you must understand how ACS determines a username format, how it supports each of these formats, and how the types of support are related.

To determine the format of a username that is submitted for Windows authentication, ACS searches the username for the:

- At symbol (@)
- Backslash (\)

Based on the presence and position of these two characters in the username, ACS determines username format by using the following logic:

1. If the username does not contain a backslash (\) *and* does not contain an at symbol (@), ACS considers the username to be nondomain qualified. For example, the username `cyril.yang` is nondomain qualified. For more information, see Nondomain-Qualified Usernames, page 13-9.
2. If the username contains a backslash (\) that precedes any "at" characters, ACS considers the username to be domain qualified. For example, ACS considers the following usernames to be domain qualified:
   - *MAIN\cyril.yang*
   - *MAIN\cyril.yang@central-office*

   For more information, see Domain-Qualified Usernames, page 13-9.
3. If the username contains an at symbol (@) that does not follow a backslash (\), ACS considers the username to be in User Principal Name (UPN) format. For example, ACS considers the following usernames to be UPN usernames:
   - *cyril.yang@example.com*
   - *cyril.yang@main.example.com*
   - *cyril.yang@main*
   - *cyril.yang@central-office@example.com*
   - *cyril.yang@main\example.com*

   For more information, see UPN Usernames, page 13-10.

Nondomain-Qualified Usernames

ACS supports Windows authentication of usernames that are not domain qualified, provided the username does not contain an at symbol (@). Users with at symbols (@) in their usernames must submit the username in UPN format or in a domain-qualified format. Examples of nondomain-qualified usernames are *cyril.yang* and *msmith*.

In Windows environments with multiple domains, authentication results with nondomain-qualified usernames can vary. This variance occurs because Windows, not ACS, determines which domains are used to authenticate a nondomain-qualified username. If Windows does not find the username in its local domain database, it then checks all trusted domains. If ACS runs on a member server and the username is not found in trusted domains, Windows also checks its local accounts database. Windows attempts to authenticate a user with the first occurrence of the username that it finds.

When Windows authentication for a nondomain-qualified username succeeds, the privileges that are assigned during authentication will be those that are associated with the Windows user account in the first domain with a matching username and password. This condition also illustrates the importance of removing usernames from a domain when the user account is no longer needed.

Note If the credentials that the user submits do not match the credentials that are associated with the first matching username that Windows finds, authentication fails. Thus, if different users in different domains share the same exact username, logging in with a nondomain-qualified username can result in inadvertent authentication failure.

Use of the Domain List is not required to support Windows authentication, but it can alleviate authentication failures that nondomain-qualified usernames cause. If you have configured the Domain List in the Windows User Database Configuration page of the External User Databases section, ACS submits the username and password to each domain in the list in a domain-qualified format until it successfully authenticates the user. If ACS has tried each domain in the Domain List or if no trusted domains have been configured in the Domain List, ACS stops attempting to authenticate the user and does not grant that user access.

Note If your Domain List contains domains and your Windows Security Account Manager (SAM) or Active Directory user databases are configured to lock out users after a number of failed attempts, users can be inadvertently locked out because ACS tries each domain in the Domain List explicitly, resulting in failed attempts for identical usernames that reside in different domains.

Domain-Qualified Usernames

The most reliable method of authenticating users against a specific domain is to require users to submit the domains that they should be authenticated against along with their usernames. Authentication of a domain-qualified username is directed to a specific domain; rather than depending on Windows to attempt authentication with the correct domain or on using the Domain List to direct ACS to submit the username repeatedly in a domain-qualified format.

Domain-qualified usernames have the following format:

DOMAIN\user

For example, the domain-qualified username for user Mary Smith (*msmith*) in Domain10 would be *Domain10\msmith*.

For usernames containing an at symbol (@), such as *cyril.yang@central-office*, using a domain-qualified username format is required. For example, *MAIN\cyril.yang@central-office*. If a username containing an at symbol (@) is received in a nondomain-qualified format, ACS perceives it as a username in UPN format. For more information, see UPN Usernames, page 13-10.

UPN Usernames

ACS supports authentication of usernames in UPN format, such as *cyril.yang@example.com* or *cyril.yang@central-office@example.com*.

If the authentication protocol is EAP-TLS, by default, ACS submits the username to Windows in UPN format; however, you can configure ACS to strip from the username all characters after and including the last at symbol (@). For more information, see EAP-TLS Domain Stripping, page 13-10.

For all other authentication protocols that it can support with Windows databases, ACS submits the username to Windows that is stripped of all characters after and including the last at symbol (@). This behavior allows for usernames that contain an at symbol (@). For example:

- If the username received is *cyril.yang@example.com*, ACS submits to Windows an authentication request containing the username *cyril.yang*.
- If the username received is *cyril.yang@central-office@example.com*, ACS submits to Windows an authentication request containing the username *cyril.yang@central-office*.

Note ACS cannot tell the difference between a nondomain-qualified username that contains an at symbol (@) and a UPN username; all usernames containing an at symbol (@) that do not follow a backslash (\) are submitted to Windows with the final at symbol (@) and the characters that follow it removed. Users with at symbols (@) in their usernames must submit the username in UPN format or in a domain-qualified format.

EAP and Windows Authentication

This section contains information about Windows-specific EAP features that you can configure on the Windows User Database Configuration page.

This section contains the following topics:

- EAP-TLS Domain Stripping, page 13-10
- Machine Authentication, page 13-11
- Machine Access Restrictions, page 13-13
- Microsoft Windows and Machine Authentication, page 13-14
- Enabling Machine Authentication, page 13-16

EAP-TLS Domain Stripping

If you use Windows Active Directory to authenticate users with EAP-TLS, you can use ACS to strip the domain name from the username that is stored in the Subject Alternative Name (SAN) field of the user certificate. Performing domain name stripping can speed EAP-TLS authentication when the domain that must authenticate a user is not the domain represented in the SAN field.

For example, a user's SAN field might contain *jsmith@corporation.com* but *jsmith* might need to authenticate by using the domain controller for a subdomain named *engineering*. Stripping *@corporation.com* from the username eliminates the needless attempt at authenticating *jsmith* against the *corporation.com* domain controller. Without stripping the domain name, only after *jsmith* cannot be found in corporation.com will ACS use the Domain List and find the user in the engineering domain. The additional delay could be several seconds. For more information about the Domain List, see Nondomain-Qualified Usernames, page 13-9.

You can enable EAP-TLS domain name stripping on the Windows User Database Configuration page.

Note EAP-TLS domain name stripping operates independently of support for UPN-formatted usernames. For information about support for Windows authentication of UPN-formatted usernames, see UPN Usernames, page 13-10.

Machine Authentication

ACS supports the authentication of computers that are running the Microsoft Windows operating systems that support EAP computer authentication, such as Windows XP with Service Pack 1. 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 user database. If you use Active Directory and the matching computer account in Active Directory 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. 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.

Tip 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 logged in to the domain successfully from this computer.

- **User network authentication**—ACS authenticates the user, allowing the user to have network connectivity. If the user profile exists, the user database that is specified is used to authenticate the user. While the user database is not required to be the Windows user database, 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 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 has selected to shutdown or restart the computer; rather than just logging off.

ACS supports EAP-TLS and PEAP (EAP-MS-CHAPv2) for machine authentication. You can enable each separately on the Windows User Database Configuration page, which allows a mix of computers that authenticate with EAP-TLS or PEAP (EAP-MS-CHAPv2). Microsoft operating systems that perform machine authentication might limit the user authentication protocol to the same protocol that is used for machine authentication. For more information about Microsoft operating systems and machine authentication, see Microsoft Windows and Machine Authentication, page 13-14.

The Unknown User Policy supports machine authentication. Computers that were previously unknown to ACS are handled similarly to users. If the Unknown User Policy is enabled and an Active Directory external user database is included on the Selected Databases list on the Configure Unknown User Policy page, machine authentication succeeds; provided that the machine credentials presented to Active Directory are valid.

On a computer that is configured to perform machine authentication, machine authentication occurs when the computer started. Provided that the AAA client sends RADIUS accounting data to ACS, when a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section. Once user authentication begins, the computer no longer appears on the Logged-In Users List.

PEAP-based machine authentication uses PEAP (EAP-MS-CHAPv2) and the password for the computer established automatically when it was added to the Microsoft Windows domain. The computer sends its name as the username and the format is:

`host/`*computer*`.`*domain*

where *computer* is the name of the computer and *domain* is the domain to which the computer belongs. The domain segment might also include subdomains, if they are used; so that the format may be:

`host/`*computer*`.`*subdomain*`.`*domain*

The usernames of computers that are authenticated must appear in the ACS internal database. If you enable unknown user processing, ACS adds them automatically once they authenticate successfully. During authentication, the domain name is not used.

EAP-TLS-based machine authentication uses EAP-TLS to authenticate the computer that is using a client certificate. The certificate that the computer uses can be one installed automatically when the computer was added to the domain or one that was added to the local machine storage later. As with PEAP-based machine authentication, the computer name must appear in the ACS internal database in the format contained in the computer client certificate and the user profile corresponding to the computer name must be configured to authenticate by using the Windows external user database. If you enable unknown user processing, ACS adds the computer names to the ACS internal database automatically; once they authenticate successfully. It also automatically configures the user profiles that are created to use the external user database in which the user was found. For machine authentication, this will always be the Windows external user database.

Machine Access Restrictions

You can use the machine access restrictions (MAR) feature as an additional means of controlling authorization for Windows-authenticated EAP-TLS, EAP-FASTv1a, and Microsoft PEAP users, based on machine authentication of the computer used to access the network.

When you enable the feature:

- For every successful machine authentication, ACS caches the value that was received in the Internet Engineering Task Force (IETF) RADIUS `Calling-Station-Id attribute (31)` as evidence of the successful machine authentication. ACS stores each `Calling-Station-Id` attribute value for the number of hours that is specified on the Windows User Database Configuration page before deleting it from the cache.
- When a user authenticates with an EAP-TLS, EAP-FASTv1a, or Microsoft PEAP end-user client, ACS searches the cache of `Calling-Station-Id` values from successful machine authentications for the `Calling-Station-Id` value received in the user authentication request. Whether ACS finds the user-authentication `Calling-Station-Id` value in the cache affects how ACS assigns the user requesting authentication to a user group.
  - **Calling-Station-Id value found in the cache**—ACS assigns the user to a user group by normal methods, which include manual specification of a group in the user profile, group mapping, or RADIUS-based group specification. For example, if a user logs in with a computer that was successfully authenticated and the user profile indicates that the user is a member of group 137, ACS applies to the user session the authorization that were settings specified in group 137.
  - **Calling-Station-Id value not found in the cache**—ACS assigns the user to the user group specified by **Group map for successful user authentication without machine authentication** list. This can include the **<No Access>** group.

Note User profile settings always override group profile settings. If a user profile grants an authorization that is denied by the group specified in the **Group map for successful user authentication without machine authentication** list, ACS grants the authorization.

The MAR feature supports full EAP-TLS, EAP-FASTv1a, and Microsoft PEAP authentication, as well as resumed sessions for EAP-TLS and Microsoft PEAP and fast reconnections for Microsoft PEAP.

The MAR feature has the following limitations and requirements:

- Machine authentication must be enabled.
- Users must authenticate with EAP-TLS, EAP-FASTv1a, or a Microsoft PEAP client. MAR does not apply to users who are authenticated by other protocols, such as EAP-FAST, LEAP, or MS-CHAP.
- The AAA client must send a value in the IETF RADIUS `Calling-Station-Id attribute (31).`
- ACS does not replicate the cache of `Calling-Station-Id` attribute values from successful machine authentications.
- Users that are authenticated through dial-up will always be treated according to the MAR configuration, since there is no machine authentication when by using dial up. A user will be mapped to a specific group, as defined in the External User Databases > Database Group Mappings > Windows Database settings, when machine authentication occurs. If group mapping is not configured, the user will be mapped to the default group.

Setting Up a MAR Exception List

You might need to set up a MAR exception list if you need to set up specific users (for example managers and administrators) to have access to the network; regardless of whether they pass machine authentication. This feature allows you to select user groups that would be exempt from the MAR.

Before You Begin

So that users can immediately authenticate as part of the MAR exception list, you should set up the required number of groups and permissions before changing your Windows database settings. To manage your group settings, see Group TACACS+ Settings, page 6-2 and Listing Users in a User Group, page 6-40.

To set up a MAR exception list for selected user groups:

Step 1 From the navigation bar, choose **External User Databases > Database Configuration > Windows Database**.

Step 2 Click **Configure**.

Step 3 In the Windows User Database Configuration page, enable the correct machine authentication settings and move the user groups that you want to include in the MAR exemption list to the Selected Groups list.

Step 4 Click **Submit**.

The exception list is based on ACS user groups to which the relevant NT groups would map. You can create exceptions for several user groups, and map different authorization permission to each group.

Microsoft Windows and Machine Authentication

ACS supports machine authentication with Active Directory in Windows 2000 and 2003. To enable machine authentication support in Windows Active Directory you must:

1. Apply Service Pack 4 to the computer that is running Active Directory.
2. Complete the steps in Microsoft Knowledge Base Article 306260: Cannot Modify Dial-In Permissions for Computers That Use Wireless Networking.

Client operating systems that support machine authentication are:

- Microsoft Windows XP with Service Pack 1 applied.
- Microsoft Windows 2000 with:
  - Service Pack 4 applied.
  - Patch Q313664 applied (available from Microsoft.com).
- Microsoft Windows 2003

The following list describes the essential details of enabling machine authentication on a client computer with a Cisco Aironet 350 wireless adapter. For more information about enabling machine authentication in Microsoft Windows operating systems, please refer to Microsoft documentation.

1. Ensure that the wireless network adapter is installed correctly. For more information, see the documentation that is provided with the wireless network adapter.

2. Ensure that the certification authority (CA) certificate of the CA that issued the ACS server certificate is stored in machine storage on client computers. User storage is not available during machine authentication; therefore, if the CA certificate is in user storage, machine authentication fails.
3. Select the wireless network:
   - In Windows XP, you can choose **Windows Network Connection > Properties > Network Connection Properties**.
   - In Windows 2000, you can manually enter the Service Set Identifier (SSID) of the wireless network. Use the Advanced tab of the properties dialog box for the wireless network adapter.
4. To enable PEAP machine authentication, configure the Authentication tab. In Windows XP, the Authentication tab is available from the properties of the wireless network. In Windows 2000, it is available from the properties of the wireless network connection. To configure the Authentication tab:
   a. Check the **Enable network access control using IEEE 802.1X** check box.
   b. Check the **Authenticate as computer when computer information is available** check box.
   c. From the EAP type list, select **Protected EAP (PEAP)**.
   d. On the **Protected EAP Properties** dialog box, you can enforce that ACS has a valid server certificate by checking the **Validate server certificate** check box. If you do check this check box, you must also select the applicable **Trusted Root Certification Authorities**.
   e. Also open the PEAP properties dialog box, from the **Select Authentication Method** list, select **Secured password (EAP-MS-CHAP v2)**.
5. To enable EAP-TLS machine authentication, configure the Authentication tab. In Windows XP, the Authentication tab is available from the properties of the wireless network. In Windows 2000, it is available from the properties of the wireless network connection.
   a. Check the **Enable network access control using IEEE 802.1X** check box.
   b. Check the **Authenticate as computer when computer information is available** check box.
   c. From the **EAP type** list, select **Smart Card or other Certificate**.
   d. On the **Smart Card or other Certificate Properties** dialog box, select the **Use a certificate on this computer** option.
   e. Also on the **Smart Card or other Certificate Properties** dialog box, you can enforce that ACS has a valid server certificate by checking the **Validate server certificate** check box. If you check this check box, you must also select the applicable Trusted Root Certification Authorities.

If you have a Microsoft certification authority server that is configured on the domain controller, you can configure a policy in Active Directory to produce a client certificate automatically when a computer is added to the domain. For more information, see the Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows.

Enabling Machine Authentication

This procedure contains an overview of the detailed procedures required to configure ACS to support machine authentication.

Note You must configure end-user client computers and the applicable Active Directory to support machine authentication. This procedure is specific to configuration of ACS only. For information about configuring Microsoft Windows operating systems to support machine authentication, see Microsoft Windows and Machine Authentication, page 13-14.

To enable ACS to perform machine authentication:

Step 1 Install a server certificate in ACS. PEAP (EAP-MS-CHAPv2) and EAP-TLS require a server certificate. ACS uses a single certificate to support both protocols. For detailed steps, see Installing an ACS Server Certificate, page 10-25.

Note If you have installed a certificate to support EAP-TLS or PEAP user authentication or to support HTTPS protection of remote ACS administration, you do not need to perform this step. A single server certificate will support all certificate-based ACS services and remote administration.

Step 2 For EAP-TLS machine authentication, if certificates on end-user clients are issued by a different CA than the CA that issued the server certificate on ACS, you must edit the certification trust list so that CAs that issue end-user client certificates are trusted. If you do not perform this step and the CA of the server certificate is not the same as the CA of an end-user client certificate CA, EAP-TLS will operate normally; but reject the EAP-TLS machine authentication because it does not trust the correct CA. For detailed steps, see Editing the Certificate Trust List, page 10-27.

Step 3 Enable the applicable protocols on the Global Authentication Setup page:

- To support machine authentication with PEAP, enable the PEAP (EAP-MS-CHAPv2) protocol.
- To support machine authentication with EAP-TLS, enable the EAP-TLS protocol.

You can use ACS to complete this step only after you have successfully completed Step 1. For detailed steps, see Configuring Authentication Options, page 10-19.

Step 4 Configure a Windows external user database and enable the applicable types of machine authentication on the Windows User Database Configuration page:

- To support machine authentication with PEAP, check the **Permit PEAP machine authentication** check box.
- To support machine authentication with EAP-TLS, check the **Permit EAP-TLS machine authentication** check box.
- To require machine authentication in addition to user authentication, check the **Enable machine access restrictions** check box.

Note If you already have a Windows external user database configured, modify its configuration to enable the applicable machine authentication types.

For detailed steps, see Configuring a Windows External User Database, page 13-21.

ACS is ready to perform machine authentication for computers whose names exist in the ACS internal database.

Step 5 If you have not already enabled the Unknown User Policy and added the Windows external user database to the Selected Databases list, consider doing so to allow computers that are not known to ACS to authenticate. For detailed steps, see Configuring the Unknown User Policy, page 16-8.

Note Enabling the Unknown User Policy to support machine authentication also enables the Unknown User Policy for user authentication. ACS makes no distinction in unknown user support between computers and users.

Step 6 If you have users to whom you want to allow access to the network, even if they do not pass machine authentication, you might want to set up a list of user groups that are exempt from the MAR. For detailed steps, see Machine Access Restrictions, page 13-13.

ACS is ready to perform machine authentication for computers; regardless of whether the computer names exist in ACS internal database.

User-Changeable Passwords with Windows User Databases

For network users who are authenticated by a Windows user database, ACS supports user-changeable passwords on password expiration. You can enable this feature in the MS-CHAP Settings and Windows EAP Settings tables on the Windows User Database Configuration page in the External User Databases section. The use of this feature in your network requires that:

- Users must be present in the Windows Active Directory or SAM user database.
- User accounts in ACS must specify the Windows user database for authentication.
- End-user clients must be compatible with MS-CHAP, PEAP (EAP-GTC), PEAP (EAP-MS-CHAPv2), or EAP-FAST.
- The AAA client that the end-user clients connect to must support the applicable protocols:
  - For MS-CHAP password aging, the AAA client must support RADIUS-based MS-CHAP authentication.
  - For PEAP (EAP-MS-CHAPv2), PEAP (EAP-GTC), and EAP-FAST password aging, the AAA client must support EAP.

When the previous conditions are met and this feature is enabled, users receive a dialog box prompting them to change their passwords on their first successful authentication after their passwords have expired. The dialog box is the same as Windows presents to users when a user with an expired password accesses a network via a remote-access server.

For more information about password aging support in ACS, see Enabling Password Aging for Users in Windows Databases, page 6-19.

Preparing Users for Authenticating with Windows

Before using the Windows user database for authentication:

Step 1 Ensure that the username exists in the Windows user database.

Step 2 In Windows, for each user account, clear the following **User Properties** check boxes:

- User must change password at next logon
- Account disabled

Step 3 If you want to control dial-in access from within Windows NT, click **Dial-in** and select **Grant dialin permission to user**. In Windows 2000 and Windows 2003, access the **User Properties** dialog box, select the **Dial-In** tab, and in the Remote Access area, click **Allow access**. You must also configure the option to reference this feature under Database Group Mappings in the External User Databases section of ACS.

Windows User Database Configuration Options

The Windows User Database Configuration page contains:

- **Dialin Permission**—You can restrict network access to users whose Windows accounts have Windows dial-in permission. The Grant dialin permission to user check box controls this feature.

Note This feature applies to all users when ACS authenticates with a Windows external user database; despite the name of the feature, it is not limited to users who access the network with a dial-up client but is applied regardless of client type. For example, if you have configured a PIX Firewall to authenticate Telnet sessions by using ACS as a RADIUS server, a user authenticated by a Windows external user database would be denied Telnet access to the PIX Firewall if the Dialin Permission feature is enabled and the Windows user account does not have dial-in permission.

Tip Windows dial-in permission is enabled in the Dialin section of user properties in Windows NT and on the Dial-In tab of the user properties in Windows 2000 and Windows 2003.

- **Windows Callback**—You should enable this setting if you have Windows users that require dial-up access with callback and the User Setup or Group Setup callback setting is configured for Windows Database Callback. If dial-in access with callback is not required or is not configured for Windows Database Callback, then do not enable this setting.

Note If you disable the Windows Callback option, be certain to disable the callback options in the User Setup or Group Setup callback settings. If the settings contain inconsistencies, the client will not receive the callback number.

- **Unknown User Policy**—If the unknown user policy contains additional external databases and the Windows database is not the last database on the Selected Databases list, you might enable this option. For example, If a user does not exist in the Windows database, or has typed an incorrect password, the error `1326(bad username or password)` is returned. ACS treats this error as a `wrong`

password error and does not default to another external database. You should enable this option when additional external databases appear after the Windows database in the Selected Databases list. When enabled, ACS searches for the unknown user in the other external databases.

- **Configure Domain List**—Use this option only when *all* the following occur:
  - You are using PAP or MSCHAP.
  - Usernames are not domain-prefixed.
  - Duplicate usernames exist; for example, administrator.

  When usernames are not domain-prefixed, and the same username occurs multiple times across the entire network, if no domains are in the **Domain List**, Windows can try to authenticate the wrong credentials. When Windows rejects the initial user-authentication request, ACS stops attempting to authenticate the user. For more information, see Nondomain-Qualified Usernames, page 13-9. If domains are in the **Domain List**, ACS qualifies the username with a domain from the list and submits the domain-qualified username to Windows, once for each domain in the Domain List, until each domain has rejected the user or until one of the domains authenticates the user.

  In all other cases, leave the **Domain List** empty as it might cause performance problems if you use it when you do not need to. Also, each time ACS uses the Domain List and checks the wrong account, Windows counts that as a failed login for that user, which can cause an account lockout.

- **MS-CHAP Settings**—You can control whether ACS supports MS-CHAP-based password changes for Windows user accounts. You can use the Permit password changes by checking the MS-CHAP version *N* check boxes to specify which versions of MS-CHAP ACS supports.

  Note The check boxes under MS-CHAP Settings do no affect password aging for Microsoft PEAP, EAP-FAST, or machine authentication.

  For more information about Windows password changes, see Enabling Password Aging for Users in Windows Databases, page 6-19.

- **Windows EAP Settings:**
  - **Enable password change inside PEAP or EAP-FAST**—The **Permit password change inside PEAP or EAP-FAST** check box controls whether ACS supports PEAP-based or EAP-FAST-based password changes for Windows user accounts. PEAP password changes are supported only when the end-user client uses PEAP (EAP-MS-CHAPv2) for user authentication. For EAP-FAST, ACS supports password changes in phase zero and phase two.
  - **EAP-TLS Strip Domain Name**—The **EAP-TLS Strip Domain Name** check box controls whether ACS removes the domain name from a username that is derived from the Subject Alternative Name (SAN) field in an end-user certificate.

    Performing domain name stripping can speed EAP-TLS authentication when the domain that must authenticate a user is not the domain that is represented in the SAN field. For example, a user's SAN field might contain *jsmith@corporation.com* but *jsmith* might need to authenticate by using the domain controller for a subdomain named *engineering*. Stripping *@corporation.com* from the username eliminates the needless attempt at authenticating jsmith against the *corporation.com* domain controller. Without stripping the domain name, only after jsmith cannot be found in *corporation.com* will ACS use the Domain List and find the user in the engineering domain. The additional delay could last several seconds.
  - **Enable PEAP machine authentication**—This check box controls whether ACS performs machine authentication by using a machine name and password with PEAP (EAP-MS-CHAPv2). For more information about machine authentication, see Machine Authentication, page 13-11.

- **Enable EAP-TLS machine authentication**—This check box controls whether ACS performs machine authentication by using a machine name and password with EAP-TLS. For more information about machine authentication, see Machine Authentication, page 13-11.
- **EAP-TLS and PEAP machine authentication name prefix**—This box defines the string of characters that ACS adds to the beginning of any machine name being authenticated. By default, the end-user client prefixes machine names with *host/*. If the PEAP machine authentication name prefix box contains any text, ACS prefixes the machine name with this text instead.

Note If you configure the EAP-TLS and PEAP machine authentication name prefix box with a string other than *host/*, authentication might fail.

- **Enable machine access restrictions**—If you enable PEAP or EAP-TLS machine authentication, the **Enable machine access restrictions** check box controls whether ACS restricts network access of users who access the network with a computer that fails machine authentication. For more information about the MAR feature, see Machine Access Restrictions, page 13-13.

Note Ensure that you have enabled the types of machine authentication that your Windows computers are configured to use: PEAP machine authentication or EAP-TLS authentication, or both. If the MAR feature is enabled but ACS does not perform machine authentication for a computer, EAP-TLS and Microsoft PEAP users who access the network with that computer will be assigned to the group that is specified in the Group map for successful user authentication without machine authentication list.

Tip To enable machine access restrictions, you must specify a number greater than zero (0) in the **Aging time (hours)** box.

- **Aging time (hours)**—This box specifies the number of hours that ACS caches IETF RADIUS `Calling-Station-Id` attribute values from successful machine authentications, for use with the MAR feature. The default value is zero (0) hours, which means that ACS does not cache `Calling-Station-Id` values.

Note If you do not change the value of the **Aging time (hours)** box to something other than zero (0), all EAP-TLS and Microsoft PEAP users whose computers perform machine authentication are assigned to the group that is specified in the **Group map for successful user authentication without machine authentication** list.

Tip To clear the cache of `Calling-Station-Id` values, type zero (0) in the **Aging time (hours)** box and click **Submit**.

- **Group map for successful user authentication without machine authentication**—This list specifies the group profile that ACS applies to a user who accesses the network from a computer that has not passed machine authentication for longer than the number of hours specified in the Aging time (hours) box. To deny such users any access to the network, select **<No Access>** (which is the default setting).

Note User profile settings always override group profile settings. If a user profile grants an authorization that is denied by the group that is specified in the Group map for successful user authentication without machine authentication list, ACS grants the authorization.

– **User Groups that are exempt from passing machine authentication**— The Selected User Group list controls what ACS does when machine authentication is not successfully completed. If the Selected User Group list contains no groups and Windows rejects the initial machine authentication, ACS stops attempting to authenticate the user. If the Selected User Group list contains groups, ACS will provide authentication and the privileges within that group to the user; even though their computers are unknown to Active Directory.

Note Configuring the User Group list is optional. For more information about the user group management, see User Group Management, page 6-1.

Caution If your User Group list contains groups and you configure your Windows SAM or Active Directory user databases to lock out users after a number of failed attempts, users can be inadvertently locked out. You should ensure that your group settings are configured properly.

- **Available User Groups**—This list represents the user groups for which ACS *requires* machine authentication.
- **Selected User Groups**—This list represents the user groups for which ACS *do not require* machine authentication to gain entry into the network.

Configuring a Windows External User Database

For information about the options that are available on the Windows User Database Configuration page, see Windows User Database Configuration Options, page 13-18.

To configure ACS to authenticate users against the Windows user database in the trusted domains of your network:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS displays a list of all possible external user database types.

Step 3 Click **Windows Database**.

If no Windows database configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 4 Click **Configure**.

The Windows User Database Configuration page appears.

Step 5 As needed, configure the options in:

- Dialin Permission
- Windows Callback

- Unknown User Policy
- Domain List
- MS-CHAP Settings
- Windows EAP Settings

For information about the options on the Windows User Database Configuration page, see Windows User Database Configuration Options, page 13-18.

Note All the settings on the Windows User Database Configuration page are optional and need not be enabled; unless you want to permit and configure the specific features that they support.

Step 6 Click **Submit**.

ACS saves the Windows user database configuration that you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 16-3. For more information about configuring user accounts to authenticate by using this database, see Chapter 7, "User Management."

Generic LDAP

ACS supports ASCII, PAP, EAP-TLS, PEAP (EAP-GTC), and EAP-FAST (phase two only) authentication via generic Lightweight Directory Access Protocol (LDAP) databases, such as Netscape Directory Services. Other authentication protocols are not supported with LDAP external user databases.

Note Another type of external user database might support authentication protocols that are not supported with LDAP databases. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-7.

ACS supports group mapping for unknown users by requesting group membership information from LDAP user databases. For more information about group mapping for users who are authenticated with an LDAP user database, see Group Mapping by Group Set Membership, page 17-3.

Configuring ACS to authenticate against an LDAP database has no effect on the configuration of the LDAP database. To manage your LDAP database, see your LDAP database documentation.

This section contains the following topics:

- ACS Authentication Process with a Generic LDAP User Database, page 13-23
- Multiple LDAP Instances, page 13-23
- LDAP Organizational Units and Groups, page 13-23
- Domain Filtering, page 13-24
- LDAP Failover, page 13-25
- LDAP Admin Logon Connection Management, page 13-26
- Distinguished Name Caching, page 13-26

- LDAP Configuration Options, page 13-26
- Configuring a Generic LDAP External User Database, page 13-30

ACS Authentication Process with a Generic LDAP User Database

ACS forwards the username and password to an LDAP database by using a Transmission Control Protocol (TCP) connection on a port that you specify. The LDAP database passes or fails the authentication request from ACS. When receiving the response from the LDAP database, ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the LDAP server.

ACS grants authorization based on the ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the LDAP server, ACS grants authorization privileges.

Multiple LDAP Instances

You can create more than one LDAP configuration in ACS. By creating more than one LDAP configuration 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 configuration instance.

ACS does not require that each LDAP instance corresponds to a unique LDAP database. You can have more than one LDAP configuration 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 configuration 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.

For each LDAP instance, you can add it to or omit it from the Unknown User Policy. For more information, see About Unknown User Authentication, page 16-3.

For each LDAP instance, you can establish unique group mapping. For more information, see Group Mapping by Group Set Membership, page 17-3.

Multiple LDAP instances are also important when you use domain filtering. For more information, see Domain Filtering, page 13-24.

LDAP Organizational Units and Groups

LDAP groups do not need the same name as their corresponding ACS groups. You can map the LDAP group to an ACS group with any name that you want to assign. For more information about how your LDAP database handles group membership, see your LDAP database documentation. For more information on LDAP group mappings and ACS, see Chapter 17, “User Group Mapping and Specification.”

Domain Filtering

Using domain filtering, you can control which LDAP instance is authenticates a user based on domain-qualified usernames. Domain filtering is based on parsing the characters at the beginning or end of a username that is submitted for authentication. Domain filtering provides you with greater control over the LDAP instance to which ACS submits any given user authentication request. You can also control whether usernames are submitted to an LDAP server with their domain qualifiers intact.

For example, when EAP-TLS authentication a Windows XP client initiates, ACS receives the username in `username@domainname` format. When PEAP authentication is initiated by a Cisco Aironet end-user client, ACS receives the username without a domain qualifier. If both clients are to be authenticated with an LDAP database that stores usernames without domain qualifiers, ACS can strip the domain qualifier. If separate user accounts are maintained in the LDAP database—domain-qualified and nondomain-qualified user accounts—ACS can pass usernames to the LDAP database without domain filtering.

If you choose to make use of domain filtering, each LDAP configuration that you create in ACS can perform domain filtering:

- **Limiting users to one domain**—Per each LDAP configuration in ACS, you can require that ACS only attempts to authenticate usernames that are qualified with a specific domain name. This corresponds to the Only process usernames that are domain qualified option on the LDAP Configuration page. For more information about this option, see LDAP Configuration Options, page 13-26.

  With this option, each LDAP configuration is limited to one domain and to one type of domain qualification. You can specify whether ACS strips the domain qualification before submitting the username to an LDAP server. If the LDAP server stores usernames in a domain-qualified format, you should not configure ACS to strip domain qualifiers.

  Limiting users to one domain is useful when the LDAP server stores usernames differently per domain: by user context or how the username is stored in ACS—domain qualified or nondomain qualified. The end-user client or AAA client must submit the username to ACS in a domain-qualified format; otherwise ACS cannot determine the user's domain and does not attempt to authenticate the user with the LDAP configuration that uses this form of domain filtering.

- **Allowing any domain but stripping domain qualifiers**—Per each LDAP configuration in ACS, you can configure ACS to attempt to strip domain qualifiers based on common domain-qualifier delimiting characters. This method corresponds to the Process all usernames after stripping domain name and delimiter option on the LDAP Configuration page. For more information about this option, see LDAP Configuration Options, page 13-26.

  ACS supports prefixed and suffixed domain qualifiers. A single LDAP configuration can attempt to strip both prefixed and suffixed domain qualifiers; however, you can only specify one delimiting character each for prefixed and suffixed domain qualifiers. To support more than one type of domain-qualifier delimiting character, you can create more than one LDAP configuration in ACS.

  Allowing usernames of any domain but stripping domain qualifiers is useful when the LDAP server stores usernames in a nondomain-qualified format but the AAA client or end-user client submits the username to ACS in a domain-qualified format.

  Note With this option, ACS submits usernames that are nondomain qualified, too. Usernames are not required to be domain qualified to be submitted to an LDAP server.

LDAP Failover

ACS 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, such as when the server is down or is otherwise unreachable by ACS. To use this feature, you must define the primary and secondary LDAP servers on the LDAP Database Configuration page. Also, you must check the **On Timeout Use Secondary** check box. For more information about configuring an LDAP external user database, see Configuring a Generic LDAP External User Database, page 13-30.

If you check the **On Timeout Use Secondary** check box, 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 attempt and on the value that you enter in the **Failback Retry Delay** box.

Successful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, ACS successfully connected to the primary LDAP server, ACS attempts to connect to the primary LDAP server. If ACS cannot connect to the primary LDAP server, ACS attempts to connect to the secondary LDAP server.

If ACS cannot connect with LDAP server, ACS stops attempting LDAP authentication for the user. If the user is an unknown user, ACS tries the next external user database in the Unknown User Policy list. For more information about the Unknown User Policy list, see About Unknown User Authentication, page 16-3.

Unsuccessful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, ACS could not connect to the primary LDAP server, whether ACS first attempts to connect to the primary server or secondary LDAP server for the current authentication attempt depends on the value in the Failback Retry Delay box. If the Failback Retry Delay box is set to zero (0), ACS always attempts to connect to the primary LDAP server first. And if ACS cannot connect to the primary LDAP server, ACS then attempts to connect to the secondary LDAP server.

If the Failback Retry Delay box is set to a number other than zero (0), ACS determines how many minutes have passed since the last authentication attempt by using the primary LDAP server. If more minutes have passed than the value in the Failback Retry Delay box, ACS attempts to connect to the primary LDAP server first. And if ACS cannot connect to the primary LDAP server, ACS then attempts to connect to the secondary LDAP server.

If fewer minutes have passed than the value in the Failback Retry Delay box, ACS attempts to connect to the secondary LDAP server first. And if ACS cannot connect to the secondary LDAP server, ACS then attempts to connect to the primary LDAP server.

If ACS cannot connect to either LDAP server, ACS stops attempting LDAP authentication for the user. If the user is an unknown user, ACS tries the next external user database in the Unknown User Policy list. For more information about the Unknown User Policy list, see About Unknown User Authentication, page 16-3.

LDAP Admin Logon Connection Management

When ACS checks authentication and authorization of a user on an LDAP server, it uses a connection with the LDAP administrator account permissions. It uses the connection to search for the user and user groups on the Directory subtree. ACS retains the administrator connections that are open for successive use and additional binds are not required for each authentication request. You can limit the maximum number of concurrent administrator connections per Generic LDAP External DB configuration (primary and secondary).

Distinguished Name Caching

Searching can be an expensive LDAP operation, which introduces an element of unpredictability into the authentication. ACS takes the username that the authentication process supplies, and asks the LDAP server to search a full subtree of unknown depth, over an unknown user population.

After successful authentication ACS caches the Distinguished Name (DN) that the search returns. Reauthentications can then use the cached DN to perform an immediate lookup of the user.

A cached DN cannot appear on a screen. If a bind to a cached DN fails, ACS falls back to a full search of the data base for authenticating a user.

LDAP Configuration Options

The LDAP Database Configuration page contains many options, presented in three tables:

- **Domain Filtering**—This table contains options for domain filtering. The settings in this table affect all LDAP authentication that is performed by using this configuration; regardless of whether the primary or secondary LDAP server handles the authentication. For more information about domain filtering, see Domain Filtering, page 13-24

  This table contains:

  - **Process all usernames**—When you select this option, ACS does not perform domain filtering on usernames before submitting them to the LDAP server for authentication.
  - **Only process usernames that are domain qualified**—When you select this option, ACS only attempts authentication for usernames that are domain-qualified for a single domain. You must specify the type of domain qualifier and the domain in the **Qualified by** and **Domain** options. ACS only submits usernames that are qualified in the method that you specify in the **Qualified by** option and that are qualified with the username that is specified in the Domain Qualifier box. You can also specify whether ACS removes the domain qualifier from usernames before submitting them to an LDAP server.
  - **Qualified by**—When you select **Only process usernames that are domain qualified**, this option specifies the type of domain qualification. If you select **Prefix**, ACS only processes usernames that begin with the characters that you specify in the Domain Qualifier box. If you select **Suffix**, ACS only processes usernames that end in the characters that you specify in the Domain Qualifier box.

Note Regardless of the domain qualifier type that is selected, the domain name must match the domain that is specified in the Domain Qualifier box.

- **Domain Qualifier**—When Only process usernames that are domain qualified is selected, this option specifies the domain name and delimiting character that must qualify usernames so ACS can submit the username to an LDAP server. The Domain box accepts up to 512 characters; however, only one domain name and its delimiting character are permitted.

  For example, if the domain name is mydomain, the delimiting character is the at symbol (@), and Suffix is selected on the Qualified by list, the Domain box should contain *@mydomain*. If the domain name is *yourdomain*, the delimiting character is the backslash (\), and Prefix is selected on the Qualified by list, the Domain Qualifier box should contain *yourdomain*.

- **Strip domain before submitting username to LDAP server**—When you select Only process usernames that are domain qualified, this option specifies whether ACS removes the domain qualifier and its delimiting character before submitting a username to an LDAP server. For example, if the username is *jwiedman@domain.com*, the stripped username is *jwiedman*.

- **Process all usernames after stripping domain name and delimiter**—When this option is selected, ACS submits all usernames to an LDAP server after attempting to strip domain names. Usernames that are not domain qualified are processed, too. Domain name stripping occurs as specified by the following two options:

  - **Strip starting characters through the last *X* character**—When you select Process all usernames after stripping domain name and delimiter, this option specifies that ACS attempts to strip a prefixed domain qualifier. If, in the username, ACS finds the delimiter character that is specified in the *X* box, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the *X* 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.

Note The *X* 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 *X* box contains any of these characters, stripping fails.

  - **Strip ending characters through the first *Y* character**—When you select Process all usernames after stripping domain name and delimiter, this option specifies that ACS attempts to strip a suffixed domain qualifier. 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. 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 *jwiedman@domain*, then ACS submits *jwiedman* to an LDAP server.

Note The *Y* 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 *Y* box contains any of these characters, stripping fails.

- **Common LDAP Configuration**—This table contains options that apply to all LDAP authentication that is performed by using this configuration. ACS uses the settings in this section; regardless of whether the primary or secondary LDAP server handles the authentication.

This table contains:

- **User Directory Subtree**—The distinguished name (DN) for the subtree that contains all users. For example:

  `ou=`*organizational unit*`[,ou=`*next organizational unit*`]o=corporation.com`

  If the tree containing users is the base DN, type:

  `o=corporation.com`

  or

  `dc=corporation,dc=com`

  as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

- **Group Directory Subtree**—The DN for the subtree that contains all groups. For example:

  `ou=`*organizational unit*`[,ou=`*next organizational unit*`]o=corporation.com`

  If the tree containing groups is the base DN, type:

  `o=corporation.com`

  or

  `dc=corporation,dc=com`

  as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

- **UserObjectType**—The name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation. ACS contains default values that reflect the default configuration of a Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.

- **UserObjectClass**—The value of the LDAP `objectType` attribute that identifies the record as a user. Often, user records have several values for the `objectType` attribute, some of which are unique to the user, some of which are shared with other object types. This box should contain a value that is not shared.

- **GroupObjectType**—The name of the attribute in the group record that contains the group name.

- **GroupObjectClass**—A value of the LDAP `objectType` attribute in the group record that identifies the record as a group.

- **Group Attribute Name**—The name of the attribute of the group record that contains the list of user records that are a member of that group.

- **Server Timeout**—The number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server has failed.

- **On Timeout Use Secondary**—Whether ACS performs failover of LDAP authentication attempts. For more information about the LDAP failover feature, see LDAP Failover, page 13-25.

- **Failback Retry Delay**—The number of minutes after the primary LDAP server fails to authenticate a user that ACS resumes sending authentication requests to the primary LDAP server first. A value of zero (0) causes ACS to always use the primary LDAP server first.

  - **Max. Admin Connections**—The maximum number of concurrent connections (greater than zero (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.

- **Primary and Secondary LDAP Servers**—You can use the Primary LDAP Server table and the Secondary LDAP Server table to identify the LDAP servers and make settings that are unique to each. You do not need to complete the Secondary LDAP Server table if you do not intend to use LDAP failover. These tables contain:
  - **Hostname**—The name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.
  - **Port**—The TCP/IP port number on which the LDAP server is listening. 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 those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.
  - **LDAP Version**—Whether ACS uses LDAP version 3 or version 2 to communicate with your LDAP database. If you check this check box, ACS uses LDAP version 3. If it is not checked, ACS uses LDAP version 2.
  - **Security**—Whether ACS uses SSL to provide more secure communication with the LDAP server. If you do not enable SSL, user credentials are passed to the LDAP server in clear text. If you select this option, then you must select **Trusted Root CA** or **Certificate Database Path**. ACS supports only server-side authentication for SSL communication with the LDAP server.
  - **Trusted Root CA** —LDAP over SSL includes the option to authenticate by using the certificates database files other than the Netscape *cert7.db* file. This option uses the same mechanism as other SSL installations in the ACS environment. Select the certification authority that issued the server certificate that is installed on the LDAP server.
  - **Certificate Database Path**—The path to the Netscape *cert7.db* file. This file must contain the certificates for the server to be queried and the trusted CA. You can use a Netscape web browser to generate *cert7.db* files. For information about generating a *cert7.db* file, refer to Netscape documentation.

    To perform secure authentication by using SSL, you must enter the path of the Netscape *cert7.db* certificate database file. ACS requires a certificate database so that it can establish the SSL connection. The certificate database must be local to the ACS Windows server.

    ACS requires a certificate database file for each LDAP server that you configure. For example, to support users who are distributed in multiple LDAP trees, you could configure two LDAP instances in ACS that would communicate with the same LDAP servers. Each LDAP instance would have a primary and a secondary LDAP server. Even though the two LDAP configurations share the same primary server, each LDAP configuration requires that you download a certificate database file to ACS.

Note The database must be a *cert7.db* certificate database file. No other filename is supported.

  - **Admin DN**—The DN of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree. It must contain the following information about your LDAP server:

    uid=*user id*,[ou=*organizational unit*,][ou=*next organizational unit*]o=*organization*

    where *user id* is the username, *organizational unit* is the last level of the tree, and *next organizational unit* is the next level up the tree.

For example:

```
uid=joesmith,ou=members,ou=administrators,o=cisco
```

You can use anonymous credentials for the administrator username if the LDAP server is configured to make the group name attribute visible in searches by anonymous credentials. Otherwise, you must specify an administrator username that permits the group name attribute to be visible to searches.

Note If the administrator username that you specify does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.

- **Password**—The password for the administrator account that you specified in the **Admin DN** box. The LDAP server determines case sensitivity.

Configuring a Generic LDAP External User Database

Creating a generic LDAP configuration provides ACS information that enables it to pass authentication requests to an LDAP database. This information reflects the way that you have implemented your LDAP database and does not dictate how your LDAP database is configured or functions. For information about your LDAP database, refer to your LDAP documentation.

Note ACS supports authentication of Novell Directory Services (NDS) users by using standard LDAP.

Before You Begin

For information about the options on the LDAP Database Configuration page, see LDAP Configuration Options, page 13-26.

To configure ACS to use the LDAP User Database or to configure LDAP to authenticate Novell NDS Users:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS displays a list of all possible external user database types.

Step 3 Click **Generic LDAP**.

Note The user authenticates against only one LDAP database.

If no LDAP database configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

Step 4 If you are creating a configuration:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for generic LDAP in the box provided.

c. Click **Submit**.

ACS lists the new configuration in the External User Database Configuration table.

Step 5 Under External User Database Configuration, select the name of the LDAP database that to configure.

Note If only one LDAP configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

Step 6 Click **Configure**.

Caution If you click **Delete**, the configuration of the selected LDAP database is deleted.

Step 7 If you do not want ACS to filter LDAP authentication requests by username, under Domain Filtering, select **Process all usernames**.

Step 8 If you want to limit authentications processed by this LDAP configuration to usernames with a specific domain qualification:

Note For information about domain filtering, see Domain Filtering, page 13-24.

a. Under Domain Filtering, select **Only process usernames that are domain qualified**.

b. From the Qualified by list, select the applicable type of domain qualification, either Suffix or Prefix. Only one type of domain qualification is supported per LDAP configuration.

   For example, if you want this LDAP configuration to authenticate usernames that begin with a specific domain name, select **Prefix**. If you want this LDAP configuration to authenticate usernames that end with a specific domain name, select **Suffix**.

c. In the **Domain Qualifier** box, type the name of the domain for which you this LDAP configuration should authenticate usernames. Include the delimiting character that separates the user ID from the domain name. Ensure that the delimiting character appears in the applicable position: at the end of the domain name if **Prefix** is selected on the **Qualified by** list; at the beginning of the domain name if Suffix is selected on the Qualified by list.

   Only one domain name is supported per LDAP configuration. You can type up to 512 characters.

d. If you want ACS to remove the domain qualifier before submitting it to the LDAP database, check the **Strip domain before submitting username to LDAP server** check box.

e. If you want ACS to pass the username to the LDAP database *without* removing the domain qualifier, clear the **Strip domain before submitting username to LDAP server** check box.

Step 9 If you want to enable ACS to strip domain qualifiers from usernames before submitting them to an LDAP server:

Note For information about domain filtering, see Domain Filtering, page 13-24.

a. Under Domain Filtering, select **Process all usernames after stripping domain name and delimiter**.

b. If you want ACS to strip prefixed domain qualifiers, check the **Strip starting characters through the last *X* character** check box, and then type the domain-qualifier delimiting character in the *X* box.

Note The *X* 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 *X* box contains any of these characters, stripping fails.

c. If you want ACS to strip suffixed domain qualifiers, check the **Strip ending characters from the first *X* character** check box, and then type the domain-qualifier delimiting character in the *X* box.

Note The *X* 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 *X* box contains any of these characters, stripping fails.

Step 10 Under Common LDAP Configuration, in the **User Directory Subtree** box, type the DN of the tree containing all your users.

If you are authenticating Novell NDS users, set UserDirectorySubtree to **o=lab**.

Step 11 In the **Group Directory Subtree** box, type the DN of the subtree containing all your groups.

If you are authenticating Novell NDS users, set GroupDirectorySubtree to **o=lab**.

Step 12 In the **User Object Type** box, type the name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation.

Note The default values in the UserObjectType and following fields reflect the default configuration of the Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.

If you are authenticating Novell NDS users, set the user object type to **cn**.

Step 13 In the **User Object Class** box, type the value of the LDAP `objectType` attribute that identifies the record as a user. Often, user records have several values for the `objectType` attribute, some of which are unique to the user, some of which are shared with other object types. Select a value that is not shared.

Step 14 In the **GroupObjectType** box, type the name of the attribute in the group record that contains the group name.

Step 15 In the **GroupObjectClass** box, type a value of the LDAP `objectType` attribute in the group record that identifies the record as a group.

If you are authenticating Novell NDS users, set the **GroupObjectClass** to **groupOfNames**.

Step 16 In the **GroupAttributeName** box, type the name of the attribute of the group record that contains the list of user records who are a member of that group.

Step 17 In the **Server Timeout** box, type the number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server has failed.

Step 18 To enable failover of LDAP authentication attempts, check the **On Timeout Use Secondary** check box. For more information about the LDAP failover feature, see LDAP Failover, page 13-25.

Step 19 In the **Failback Retry Delay** box, type the number of minutes after the primary LDAP server fails to authenticate a user that ACS resumes sending authentication requests to the primary LDAP server first.

Note To specify that ACS should always use the primary LDAP server first, type zero (0) in the **Failback Retry Delay** box.

Step 20 In the **Max. Admin Connection** box, enter the number of maximum concurrent connections with LDAP administrator account permissions.

Step 21 For the Primary LDAP Server and Secondary LDAP Server tables:

Note If you did not check the On Timeout Use Secondary check box, you do not need to complete the options in the Secondary LDAP Server table.

a. In the **Hostname** box, type the name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.

b. In the **Port** box, type the TCP/IP port number on which the LDAP server is listening. 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 those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.

c. To specify that ACS should use LDAP version 3 to communicate with your LDAP database, check the **LDAP Version** check box. If the LDAP Version check box is not checked, ACS uses LDAP version 2.

d. The username and password credentials are normally passed over the network to the LDAP directory in clear text. To enhance security, check the **Use secure authentication** check box.

e. If you checked the **Use Secure authentication** checkbox, perform one of the following procedures:

- Click the **Trusted Root CA** button, and in the adjacent drop-down list, select a **Trusted Root CA**.
- Click the **Certificate Database Path** button, and in the adjacent box, type the path to the Netscape *cert7.db* file, which contains the certificates for the server to be queried and the trusted CA.

f. The Admin DN box requires the fully qualified (DN) of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree.

In the **Admin DN** box, type the following information from your LDAP server:

uid=*user id*`,[ou=`*organizational unit*`,]`
`[ou=`*next organizational unit*`]o=`*organization*

where *user id* is the username

organizational unit is the last level of the tree

next organizational unit is the next level up the tree.

For example:

```
uid=joesmith,ou=members,ou=administrators,o=cisco
```

Tip If you are using Netscape DS as your LDAP software, you can copy this information from the Netscape console.

Example-Novell NDS Server:

```
uid=admin.ou=Chicago.o=Corporation
```

You can use anonymous credentials for the administrator username if you configure the Novell NDS server to make the group name attribute visible in searches by anonymous credentials. Otherwise, you must specify an administrator username that permits the group name attribute to be visible to searches.

If the administrator username that you specified does not have permission to see the group name attribute in searches, group mapping fails for users who are authenticated by Novell NDS.

For more information, refer to your specific LDAP database documentation.

g. In the **Password** box, type the password for the administrator account that is specified in the Admin DN box. The server determines password case sensitivity.

Step 22 Click **Submit**.

ACS saves the generic LDAP configuration that you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 16-3. For more information about configuring user accounts to authenticate by using this database, see Chapter 7, "User Management."

ODBC Database

As with Windows user database support, you can use ACS ODBC-compliant relational database support to use existing user records in an external ODBC-compliant relational database. Configuring ACS to authenticate against an ODBC-compliant relational database does not affect the configuration of the relational database. To manage your relational database, refer to your relational database documentation.

Note As with all other external databases that ACS supports, the ODBC-compliant relational database is not supplied as part of ACS. For general guidance with setting up your ODBC external user database, see Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 13-36.

You can use the Windows ODBC feature to create a data source name (DSN), which specifies the database and other important parameters that are necessary for communicating with the database. Among the parameters that you provide are the username and password that are required for the ODBC driver to gain access to your ODBC-compliant relational database.

This section contains the following topics:

- What is Supported with ODBC User Databases, page 13-35
- ACS Authentication Process with an ODBC External User Database, page 13-35
- Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 13-36
- Implementation of Stored Procedures for ODBC Authentication, page 13-37
- Microsoft SQL Server and Case-Sensitive Passwords, page 13-38
- Sample Routine for Generating a PAP Authentication SQL Procedure, page 13-38
- Sample Routine for Generating an SQL CHAP Authentication Procedure, page 13-39
- Sample Routine for Generating an EAP-TLS Authentication Procedure, page 13-39
- PAP Authentication Procedure Input, page 13-40
- PAP Procedure Output, page 13-40

- CHAP/MS-CHAP/ARAP Authentication Procedure Input, page 13-41
- CHAP/MS-CHAP/ARAP Procedure Output, page 13-41
- EAP-TLS Authentication Procedure Input, page 13-42
- EAP-TLS Procedure Output, page 13-42
- Result Codes, page 13-43
- Configuring a System Data Source Name for an ODBC External User Database, page 13-43
- Configuring an ODBC External User Database, page 13-44

What is Supported with ODBC User Databases

ACS supports the use of ODBC external user databases for:

- **Authentication**—ACS supports ASCII, PAP, ARAP, CHAP, MS-CHAP (versions 1 and 2), LEAP, EAP-TLS, EAP-MD5, PEAP (EAP-GTC), PEAP (EAP-MSCHAPv2), and EAP-FAST (phase zero and phase two) authentication by using a relational database via the ODBC authenticator feature. Other authentication protocols are not supported with ODBC external user databases.

  Note Authentication protocols that are not supported with ODBC external user databases might be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-7.

- **Group Specification**—ACS supports group assignment for users who are authenticated by an ODBC user database. Authentication queries to the ODBC database must contain the group number to which you want to assign a user. For unknown users authenticated by an ODBC user database, group specification overrides group mapping.

  For more information about expected query output, see PAP Procedure Output, page 13-40, CHAP/MS-CHAP/ARAP Procedure Output, page 13-41, and EAP-TLS Procedure Output, page 13-42.

- **Group Mapping for Unknown Users**—ACS supports group mapping for unknown users by requesting group membership information from Windows user databases. For more information about group mapping for users who are authenticated with a Windows user database, see Group Mapping by Group Set Membership, page 17-3.

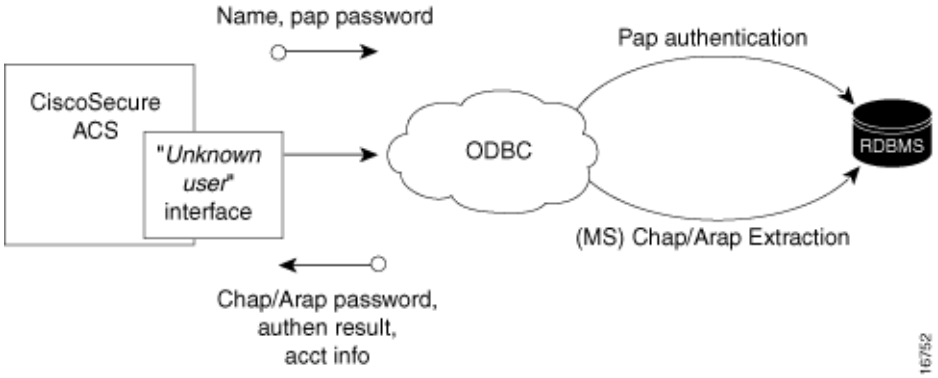
ACS Authentication Process with an ODBC External User Database

ACS forwards user authentication requests to an ODBC database when the user:

- Account in the ACS internal database lists an ODBC database configuration as the authentication method.
- Is unknown to the ACS internal database, and the Unknown User Policy dictates that an ODBC database is the next external user database to try.

In either case, ACS forwards user credentials to the ODBC database via an ODBC connection. The relational database must have a stored procedure that queries the appropriate tables and returns values to ACS. If the returned values indicate that the user credentials that were provided are valid, ACS instructs the requesting AAA client to grant the user access; otherwise, ACS denies the user access (Figure 13-2).

Figure 13-2 Using the ODBC Database for Authentication



ACS grants authorization based on the ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the ODBC database by using a process known as “group specification,” it is ACS that grants authorization privileges.

Preparing to Authenticate Users with an ODBC-Compliant Relational Database

Authenticating users with an ODBC-compliant relational database requires that you complete several significant steps that are external to ACS before configuring ACS with an ODBC external user database.

To prepare for authenticating with an ODBC-compliant relational database:

Step 1 Install your ODBC-compliant relational database on its server. For more information, refer to the relational database documentation.

Note The relational database that you use is not supplied with ACS.

Step 2 Create the database to hold the usernames and passwords. The database name is irrelevant to ACS, so that you can name the database however you like.

Step 3 Create the table or tables that will hold the usernames and passwords for your users. The table names are irrelevant to ACS, so you can name the tables and columns however you like.

Note For SQL database columns that hold user passwords, we recommend using **varchar** format. If you define password columns as **char**, password comparison might fail if the password does not use the full length of the field. For example, if a password column is 16 characters wide but the password is only ten characters long, the database might append six spaces. The value used for password comparison then grows to 16 characters, causing comparison to the actual password that the user submitted to fail.

Step 4 Write the stored procedures that are intended to return the required authentication information to ACS. For more information about these stored procedures, see Implementation of Stored Procedures for ODBC Authentication, page 13-37.

Step 5 Set up a system DSN on the computer that is running ACS. For steps, see Configuring a System Data Source Name for an ODBC External User Database, page 13-43.

Step 6 Configure ACS to authenticate users with an ODBC database. For steps, see Configuring an ODBC External User Database, page 13-44.

Implementation of Stored Procedures for ODBC Authentication

When you configure ACS to authenticate users against an ODBC-compliant relational database, you must create a stored procedure to perform the necessary query and return the values that ACS expects. The values that are returned and the tasks that are required of the stored procedure vary depending on the authentication protocol used.

Authentication for ASCII, PAP, or PEAP (EAP-GTC) occurs within the relational database; that is, if the stored procedure finds a record with the username and the password matching the input, the user is considered authenticated.

Authentication for CHAP, MS-CHAP, ARAP, LEAP, or EAP-MD5 occurs within ACS. The stored procedure returns the fields for the record with a matching username, including the password. ACS confirms or denies authentication based on the values that are returned from the procedure.

Authentication for EAP-TLS occurs within ACS. The stored procedure returns the field for the record, indicating whether it found the username in the ODBC database. ACS confirms or denies authentication based on the values that are returned from the procedure and on the validity of the user certificate. For more information about ACS support for the EAP-TLS protocol, see EAP-TLS Authentication, page 10-2.

To support the three sets of protocols, ACS provides different input to, and expects different output from, the ODBC authentication request. This feature requires a separate stored procedure in the relational database to support each of the three sets of protocols.

The ACS product CD contains **stub** routines for creating a procedure in Microsoft SQL Server or an Oracle database. You can modify a copy of these routines to create your stored procedure or write your own. You can see example routines for creating PAP and CHAP/MS-CHAP/ARAP authentication stored procedures in SQL Server in Sample Routine for Generating a PAP Authentication SQL Procedure, page 13-38, and Sample Routine for Generating an SQL CHAP Authentication Procedure, page 13-39.

The following sections provide reference information about ACS data types versus SQL data types, ASCII/PAP/PEAP (EAP-GTC) authentication procedure input and output, CHAP/MS-CHAP/ARAP authentication procedure input and output, EAP-TLS authentication procedure input and output, and expected result codes. You can use this information while writing your authentication stored procedures in your relational database.

Note Two stored procedures are required when using EAP-FAST; MS-CHAP (used for phase 0 provisioning) and PAP (used for phase 2 authentication).

Type Definitions

The ACS types and their matching SQL types are:

- **Integer**—SQL_INTEGER
- **String**—SQL_CHAR or SQL_VARCHAR

Note For SQL database columns that hold user passwords, we recommend using **varchar** format. If you define password columns as **char**, password comparison might fail if the password does not use the full length of the field. For example, if a password column is 16 characters wide but the password is only ten characters long, the database might append six spaces. The value used for password comparison then grows to 16 characters, causing comparison to the actual password that the user submitted to fail.

Microsoft SQL Server and Case-Sensitive Passwords

If you want your passwords to be case sensitive and are using Microsoft SQL Server as your ODBC-compliant relational database, configure your SQL Server to accommodate this feature. If your users are authenticating by using PPP via PAP or Telnet login, the password might not be case sensitive, depending on how you set the case-sensitivity option on the SQL Server. For example, an Oracle database will default to case sensitive, whereas Microsoft SQL Server defaults to case insensitive. However, in the case of CHAP/ARAP, the password is case sensitive if you configured the CHAP stored procedure.

For example, with Telnet or PAP authentication, the passwords **cisco** or **CISCO** or **CiScO** will all work if you configure the SQL Server to be case insensitive.

For CHAP/ARAP, the passwords **cisco** or **CISCO** or **CiScO** are not the same, regardless of whether the SQL Server is configured for case-sensitive passwords.

Sample Routine for Generating a PAP Authentication SQL Procedure

The following example routine creates a procedure named **CSNTAuthUserPap** in Microsoft SQL Server, the default procedure that ACS uses for PAP authentication. Table and column names that could vary for your database schema appear in variable text. For your convenience, the ACS product CD includes a stub routine for creating a procedure in SQL Server or Oracle. For more information about data type definitions, procedure parameters, and procedure results, see ODBC Database, page 13-34.

```
if exists (select * from sysobjects where id = object_id (`dbo.CSNTAuthUserPap') and
sysstat & 0xf = 4)drop procedure dbo.CSNTAuthUserPap
GO

CREATE PROCEDURE CSNTAuthUserPap
@username varchar(64), @pass varchar(255)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username
AND  csntpassword  = @pass )
SELECT 0,csntgroup,csntacctinfo,"No Error"
FROM  users
WHERE  username  = @username
ELSE
```

```
SELECT 3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTAuthUserPap TO ciscosecure
GO
```

Sample Routine for Generating an SQL CHAP Authentication Procedure

The following example routine creates in Microsoft SQL Server a procedure named **CSNTExtractUserClearTextPw**, the default procedure that ACS uses for CHAP/MS-CHAP/ARAP authentication. Table and column names that could vary for your database schema appear in variable text. For more information about data type definitions, procedure parameters, and procedure results, see ODBC Database, page 13-34.

```
if exists (select * from sysobjects where id = object_id(`dbo.CSNTExtractUserClearTextPw')
and sysstat & 0xf = 4) drop procedure dbo.CSNTExtractUserClearTextPw
GO

CREATE PROCEDURE CSNTExtractUserClearTextPw
@username varchar(64)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username )
SELECT 0,csntgroup,csntacctinfo,"No Error",csntpassword
FROM  users
WHERE  username  = @username
ELSE
SELECT 3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTExtractUserClearTextPw TO ciscosecure
GO
```

Sample Routine for Generating an EAP-TLS Authentication Procedure

The following example routine creates in Microsoft SQL Server a procedure named **CSNTFindUser**, the default procedure that ACS uses for EAP-TLS authentication. Table and column names that could vary for your database schema appear in variable text. For more information about data type definitions, procedure parameters, and procedure results, see ODBC Database, page 13-34.

```
if exists (select * from sysobjects where id = object_id(`dbo.CSNTFindUser') and
sysstat & 0xf = 4) drop procedure dbo.CSNTFindUser
GO

CREATE PROCEDURE CSNTFindUser
@username varchar(64)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username )
SELECT 0,csntgroup,csntacctinfo,"No Error"
FROM  users
WHERE  username  = @username
ELSE
```

```
SELECT 3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTFindUser TO ciscosecure
GO
```

PAP Authentication Procedure Input

Table 13-1 details the input that ACS provides to the stored procedure that supports PAP authentication. The stored procedure should accept the named input values as variables.

Table 13-1 PAP Stored Procedure Input

Field	Type	Explanation
CSNTusername	String	0-64 characters
CSNTpassword	String	0-255 characters

The input names are for guidance only. Procedure variables that are created from them can have different names; however, you must define them in the procedure in the order shown: the username must precede the password variable.

PAP Procedure Output

The stored procedure must return a single row that contains the nonnull fields.

Table 13-2 lists the procedure results that ACS expects as output from stored procedure.

Table 13-2 PAP Stored Procedure Results

Field	Type	Explanation
CSNTresult	Integer	See Table 13-7.
CSNTgroup	Integer	The ACS group number for authorization. You use **0xFFFFFFFF** to assign the default value. Values other than 0-499 are converted to the default. **Note** The group that is specified in the CSNTgroup field overrides group mapping that is configured for the ODBC external user database.
CSNTacctInfo	String	0-16 characters. A customer-defined string that ACS adds to subsequent account log file entries.
CSNTerrorString	String	0-255 characters. A customer-defined string that ACS writes to the *CSAuth* service log file if an error occurs.

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The *CSNTerrorString* file is logged only after a failure (if the result is greater than or equal to 4).

Note If the ODBC database returns data in **recordset** format rather than in parameters, the procedure must return the result fields in the order previously listed.

CHAP/MS-CHAP/ARAP Authentication Procedure Input

ACS provides a single value for input to the stored procedure that supports CHAP/MS-CHAP/ARAP authentication. The stored procedure should accept the named input value as a variable.

Note Because ACS performs authentication for CHAP/MS-CHAP/ARAP, the user password is not an input (Table 13-3).

Table 13-3 CHAP Stored Procedure Input

Field	Type	Explanation
CSNTusername	String	0-64 characters

The input name is for guidance only. A procedure variable that is created from it can have a different name.

CHAP/MS-CHAP/ARAP Procedure Output

The stored procedure must return a single row that contains the nonnull fields.

Table 13-4 lists the procedure results that ACS expects as output from a stored procedure.

Table 13-4 CHAP/MS-CHAP/ARAP Stored Procedure Results

Field	Type	Explanation
CSNTresult	Integer	See Table 13-7 Result Codes.
CSNTgroup	Integer	The ACS group number for authorization. You use **0xFFFFFFFF** to assign the default value. Values other than 0-499 are converted to the default. **Note** The group that is specified in the CSNTgroup field overrides group mapping that is configured for the ODBC external user database.
CSNTacctInfo	String	0-15 characters. A customer-defined string that ACS adds to subsequent account log file entries.
CSNTerrorString	String	0-255 characters. A customer-defined string that ACS writes to the *CSAuth* service log file if an error occurs.
CSNTpassword	String	0-255 characters. ACS authenticates the password. **Note** If the password field in the database is defined by using a **char** datatype rather than **varchar**, the database might return a string that is 255 characters long; regardless of actual password length. We recommend using the **varchar** datatype for the CHAP password field in your ODBC database.

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The *CSNTerrorString* file is logged only after a failure (if the result is greater than or equal to 4).

Note If the ODBC database returns data in **recordset** format rather than in parameters, the procedure must return the result fields in the order previously listed.

EAP-TLS Authentication Procedure Input

ACS provides a single value for input to the stored procedure that supports EAP-TLS authentication. The stored procedure should accept the named input value as a variable.

Note Because ACS performs authentication for EAP-TLS, the user password is not an input (Table 13-3).

Table 13-5 EAP-TLS Stored Procedure Input

Field	Type	Explanation
CSNTusername	String	0-64 characters

The input name is for guidance only. A procedure variable that is created from it can have a different name.

EAP-TLS Procedure Output

The stored procedure must return a single row that contains the nonnull fields.

Table 13-4 lists the procedure results that ACS expects as output from stored procedure.

Table 13-6 EAP-TLS Stored Procedure Results

Field	Type	Explanation
CSNTresult	Integer	See Table 13-7 Result Codes.
CSNTgroup	Integer	The ACS group number for authorization. You use **0xFFFFFFFF** to assign the default value. Values other than 0-499 are converted to the default. **Note** The group that is specified in the CSNTgroup field overrides group mapping that is configured for the ODBC external user database.
CSNTacctInfo	String	0-15 characters. A customer-defined string that ACS adds to subsequent account log file entries.
CSNTerrorString	String	0-255 characters. A customer-defined string that ACS writes to the *CSAuth* service log file if an error occurs.

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The *CSNTerrorString* file is logged only after a failure (if the result is greater than or equal to 4).

Note If the ODBC database returns data in **recordset** format, rather than in parameters, the procedure must return the result fields in the order previously listed.

Result Codes

You can set the result codes that are listed in Table 13-7.

Table 13-7 Result Codes

Result Code	Meaning
0 (zero)	Authentication successful
1	Unknown username
2	Invalid password
3	Unknown username or invalid password
4+	Internal error—authentication not processed

The SQL procedure can decide among 1, 2, or 3 to indicate a failure, depending on how much information that you want the failed authentication log files to include.

A return code of 4 or higher results in an authentication error event. These errors do not increment per-user failed attempt counters. Additionally, error codes are returned to the AAA client so it can distinguish between errors and failures and, if configured to do so, fall back to a backup AAA server.

Successful or failed authentications are not logged; general ACS logging mechanisms apply. In the event of an error (**CSNTresult** equal to or less than 4), the contents of the **CSNTerrorString** are written to the Windows Event Log under the Application Log.

Configuring a System Data Source Name for an ODBC External User Database

On the computer that is running ACS, you must create a system DSN for ACS to communicate with the relational database.

To create a system DSN for use with an ODBC external user database:

Step 1 Using the local administrator account, log in to the computer that is running ACS.

Step 2 In the Windows Control Panel, double-click the **ODBC Data Sources** icon.

Step 3 Choose **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

Tip If the Control Panel is not expanded on the **Start** menu, choose **Start > Settings > Control Panel**, double-click **Administrative Tools**, and then double-click **Data Sources (ODBC)**.

The ODBC Data Source Administrator window appears.

Step 4 Click the **System DSN** tab.

Step 5 Click **Add**.

Step 6 Select the driver that you use with your new DSN, and then click **Finish**.

A dialog box displays fields that require information that is specific to the ODBC driver that you selected.

Step 7 Type a descriptive name for the DSN in the **Data Source Name** box.

Step 8 Complete the other fields that the ODBC driver that you selected requires. These fields might include information such as the IP address of the server on which the ODBC-compliant database runs.

Step 9 Click **OK**.

The name that you assigned to the DSN appears in the System Data Sources list.

Step 10 Close the ODBC Data Source Administrator window and the Windows Control Panel.

The system DSN that ACS will use for communication with the relational database is created on the computer that is running ACS.

Configuring an ODBC External User Database

Creating an ODBC database configuration provides ACS with information that it uses to pass authentication requests to an ODBC-compliant relational database. This information reflects the way that you have implemented your relational database, and does not dictate how your relational database is configured or functions. For information about your relational database, refer to your relational documentation.

Note Before performing this procedure, you should have completed the steps in Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 13-36.

To configure ACS for ODBC authentication:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 3 Click **External ODBC Database**.

Step 4 If you are creating a configuration:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for ODBC authentication in the box provided, or accept the default name in the box.

c. Click **Submit**.

ACS lists the new configuration in the External User Database Configuration table.

Step 5 Click **Configure**.

Step 6 From the System DSN list, select the DSN that is configured to communicate with the ODBC-compliant relational database that you want to use.

Note If you have not configured the computer that is running ACS with a DSN for the relational database, do so before completing these steps. For more information about creating a DSN for ACS ODBC authentication, see Configuring a System Data Source Name for an ODBC External User Database, page 13-43.

Step 7 In the **DSN Username** box, type the username that is required to perform transactions with your ODBC database.

Step 8 In the **DSN Password** box, type the password that is required to perform transactions with your ODBC database.

Step 9 In the **DSN Connection Retries** box, type the number of times that ACS should try to connect to the ODBC database before timing out. The default is 3.

Note If you have connection problems when Windows starts, increase the default value.

Step 10 To change the ODBC worker thread count, in the **ODBC Worker Threads** box, type the number of ODBC worker threads. The maximum thread count is 10. The default is 1.

Note Increase the ODBC worker thread count only if the ODBC driver that you are using is certified thread safe. For example, the Microsoft Access ODBC driver is not thread safe and can cause ACS to become unstable if multiple threads are used. Where possible, ACS queries the driver to find out if it is thread safe. The thread count to use is a factor of how long the DSN takes to execute the procedure and the rate at which authentications are required.

Step 11 From the DSN Procedure Type list, select the type of output that your relational database provides. Different databases return different output:

- **Returns Recordset**—The database returns a raw record set in response to an ODBC query. Microsoft SQL Server responds in this manner.
- **Returns Parameters**—The database returns a set of named parameters in response to an ODBC query. Oracle databases respond in this manner.

Step 12 To support ASCII, PAP, or PEAP (EAP-GTC) authentication with the ODBC database:

a. Check the **Support PAP authentication** check box.

b. In the **PAP SQL Procedure** box, type the name of the PAP SQL procedure routine that runs on the ODBC server. The default value in this box is **CSNTAuthUserPap**. If you named the PAP SQL procedure something else, change this entry to match the name given to the PAP SQL procedure. For more information and an example routine, see Sample Routine for Generating a PAP Authentication SQL Procedure, page 13-38.

Note If you enabled PAP authentication, the PAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the **PAP SQL Procedure** box. If it does not, be certain to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 13 To support CHAP, MS-CHAP, ARAP, EAP-MD5, or LEAP authentication with the ODBC database:

a. Check the **Support CHAP/MS-CHAP/ARAP Authentication** check box.

b. In the **CHAP SQL Procedure** box, type the name of the CHAP SQL procedure routine on the ODBC server. The default value in this box is **CSNTExtractUserClearTextPw**. If you named the CHAP SQL procedure something else, change this entry to match the name given to the CHAP SQL procedure. For more information and an example routine, see Sample Routine for Generating an SQL CHAP Authentication Procedure, page 13-39.

Note If you enabled CHAP/MS-CHAP/ARAP authentication, the CHAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the **PAP SQL Procedure** box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 14 To support EAP-TLS authentication with the ODBC database:

a. Check the **Support EAP-TLS Authentication** check box.

b. In the **EAP-TLS SQL Procedure** box, type the name of the EAP-TLS SQL procedure routine on the ODBC server. The default value in this box is **CSNTFindUser**. If you named the EAP-TLS SQL procedure something else, change this entry to match the name given to the EAP-TLS SQL procedure. For more information and an example routine, see Sample Routine for Generating an EAP-TLS Authentication Procedure, page 13-39.

Note If you enabled EAP-TLS authentication, the EAP-TLS authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the **EAP-TLS SQL Procedure** box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 15 Click **Submit**.

ACS saves the ODBC configuration that you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 16-3. For more information about configuring user accounts to authenticate by using this database, see Chapter 7, "User Management."

LEAP Proxy RADIUS Server Database

For ACS-authenticated users who access your network via Cisco Aironet devices, ACS supports PAP based MAC Exception Handling, LEAP, and EAP-FAST (phase zero and phase two) authentication with a proxy RADIUS server. Other authentication protocols are not supported with LEAP Proxy RADIUS Server databases. This feature is useful if your own RADIUS-based user database can support MS-CHAP but not LEAP/EAP-FAST. ACS manages the LEAP/EAP-FAST protocol handling and forwards just the MS-CHAP authentication to your server.

Note Authentication protocols not supported with LEAP Proxy RADIUS Server databases might be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-7.

ACS uses MS-CHAP Version 1 for LEAP Proxy RADIUS Server authentication. With LEAP Proxy, only the MS-CHAP authentication is proxied to the remote server in a separate RADIUS access request. To manage your proxy RADIUS database, refer to your RADIUS database documentation.

You can use the LEAP proxy RADIUS server authentication to authenticate users against existing Kerberos databases that support MS-CHAP authentication. You can use the LEAP Proxy RADIUS Server database to authenticate users with any third-party RADIUS server that supports MS-CHAP authentication.

Note The third-party RADIUS server must return Microsoft Point-to-Point Encryption (MPPE) keys in the Microsoft RADIUS vendor-specific attribute (VSA) `MS-CHAP-MPPE-Keys (VSA 12)`. If the third-party RADIUS server does not return the MPPE keys, the authentication fails and is logged in the Failed Attempts log.

ACS supports RADIUS-based group specification for users who are authenticated by LEAP Proxy RADIUS Server databases. The RADIUS-based group specification overrides group mapping. For more information, see RADIUS-Based Group Specification, page 17-8.

ACS supports group mapping for unknown users who are authenticated by LEAP Proxy RADIUS Server databases. Group mapping is only applied to an unknown user if RADIUS-based group specification did not occur. For more information about group mapping of users who are authenticated by a LEAP Proxy RADIUS Server database, see Group Mapping by External User Database, page 17-1.

Configuring a LEAP Proxy RADIUS Server External User Database

You should install and configure your proxy RADIUS server before configuring ACS to authenticate users with it. For information about installing the proxy RADIUS server, refer to the documentation that is included with your RADIUS server.

To configure LEAP proxy RADIUS authentication:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 3 Click **LEAP Proxy RADIUS Server**.

If no LEAP Proxy RADIUS Server configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

Step 4 If you are creating a configuration:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the LEAP Proxy RADIUS Server in the box provided, or accept the default name in the box.

c. Click **Submit**.

ACS lists the new configuration in the External User Database Configuration table.

Step 5 Under External User Database Configuration, select the name of the LEAP Proxy RADIUS Server database that you configure.

Note If only one LEAP Proxy RADIUS Server configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

Step 6 Click **Configure**.

Step 7 In the following boxes, type the required information:

- **Primary Server Name/IP**—IP address of the primary proxy RADIUS server.
- **Secondary Server Name/IP**—IP address of the secondary proxy RADIUS server.
- **Shared Secret**—The shared secret of the proxy RADIUS server. This must be identical to the shared secret with which the proxy RADIUS server is configured.
- **Authentication Port**—The UDP port over which the proxy RADIUS server conducts authentication sessions. If the LEAP Proxy RADIUS server is installed on the same Windows server as ACS, this port should not be the same port that ACS uses for RADIUS authentication. For more information about the ports that ACS uses for RADIUS, see RADIUS, page 1-3.
- **Timeout (seconds):**—The number of seconds that ACS waits before sending notification to the user that the authentication attempt has timed out.
- **Retries**—The number of authentication attempts ACS makes before failing over to the secondary proxy RADIUS server.
- **Failback Retry Delay (minutes)**—The number of minutes after which ACS attempts authentications by using a failed primary proxy RADIUS server.

Note If the primary and the secondary servers fail, ACS alternates between the servers until one responds.

Step 8 Click **Submit**.

ACS saves the proxy RADIUS token server database configuration that you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 16-3. For more information about configuring user accounts to authenticate by using this database, see Chapter 7, "User Management."

Token Server User Databases

ACS supports the use of token servers for the increased security that one-time passwords (OTPs) provide.

This section contains the following topics:

- About Token Servers and ACS, page 13-49
- RADIUS-Enabled Token Servers, page 13-49
- RSA SecurID Token Servers, page 13-53

About Token Servers and ACS

ACS provides ASCII, PAP, and PEAP (EAP-GTC) authentication by using token servers. Other authentication protocols are not supported with token server databases.

Note Authentication protocols that are not supported with token server databases might be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-7.

Requests from the AAA client are first sent to ACS. If ACS has been configured to authenticate against a token server and finds the username, it forwards the authentication request to the token server. If it does not find the username, ACS checks the database that is configured to authenticate unknown users. If the request for authentication is passed, the appropriate authorizations are forwarded to the AAA client along with the approved authentication. ACS then maintains the accounting information.

ACS acts as a client to the token server. For all token servers except RSA SecurID, ACS acts as a client by using the RADIUS interface of the token server. For more information about ACS support of token servers with a RADIUS interface, see RADIUS-Enabled Token Servers, page 13-49.

For RSA SecurID, ACS uses an RSA proprietary API. For more information about ACS support of RSA SecurID token servers, see RSA SecurID Token Servers, page 13-53.

Token Servers and ISDN

ACS supports token caching for ISDN terminal adapters and routers. One inconvenience of using token cards for OTP authentication with ISDN is that each B channel requires its own OTP. Therefore, a user must enter at least 2 OTPs, plus any other login passwords, such as those for Windows networking. If the terminal adapter supports the ability to turn on and off the second B channel, users might have to enter many OTPs each time the second B channel comes into service.

ACS caches the token to help make the OTPs easier for users. Therefore, if a token card is being used to authenticate a user on the first B channel, you can set a specified period during which the second B channel can come into service without requiring the user to enter another OTP. To lessen the risk of unauthorized access to the second B channel, you can limit the time that the second B channel is up. Furthermore, you can configure the second B channel to use the CHAP password that is specified during the first login to further lessen the chance of a security problem. When the first B channel is dropped, the cached token is erased.

RADIUS-Enabled Token Servers

This section describes support for token servers that provide a standard RADIUS interface.

This section contains the following topics:

- About RADIUS-Enabled Token Servers, page 13-50
- Token Server RADIUS Authentication Request and Response Contents, page 13-50
- Configuring a RADIUS Token Server External User Database, page 13-50

About RADIUS-Enabled Token Servers

ACS supports token servers by using the RADIUS server that is built into the token server. Rather than using a vendor-proprietary API, ACS sends standard RADIUS authentication requests to the RADIUS authentication port on the token server. This feature enables ACS to support any IETF RFC 2865-compliant token server.

You can create multiple instances of RADIUS token servers. For information about configuring ACS to authenticate users with one of these token servers, see Configuring a RADIUS Token Server External User Database, page 13-50.

ACS provides a means for specifying a user group assignment in the RADIUS response from the RADIUS-enabled token server. Group specification always takes precedence over group mapping. For more information, see RADIUS-Based Group Specification, page 17-8.

ACS also supports mapping users who are authenticated by a RADIUS-enabled token server to a single group. Group mapping only occurs if group specification does not occur. For more information, see Group Mapping by External User Database, page 17-1.

Token Server RADIUS Authentication Request and Response Contents

When ACS forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- `User-Name` (RADIUS attribute 1)
- `User-Password` (RADIUS attribute 2)
- `NAS-IP-Address` (RADIUS attribute 4)
- `NAS-Port` (RADIUS attribute 5)
- `NAS-Identifier` (RADIUS attribute 32)

ACS expects to receive one of the following three responses:

- **access-accept**—No attributes are required; however, the response can indicate the ACS group to which the user should be assigned. For more information, see RADIUS-Based Group Specification, page 17-8.
- **access-reject**—No attributes required.
- **access-challenge**—Attributes required, per IETF RFC, are:
  - `State` (RADIUS attribute 24)
  - `Reply-Message` (RADIUS attribute 18)

Configuring a RADIUS Token Server External User Database

Use this procedure to configure RADIUS Token Server external user databases.

Before You Begin

You should install and configure your RADIUS token server before configuring ACS to authenticate users with it. For information about installing the RADIUS token server, refer to the documentation included with your token server.

To configure ACS to authenticate users with a RADIUS Token Sever:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 3 Click **RADIUS Token Server**.

The Database Configuration Creation table appears. If at least one RADIUS token server configuration exists, the External User Database Configuration table also appears.

Step 4 If you are creating a configuration:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the RADIUS-enabled token server in the box provided, or accept the default name in the box.

c. Click **Submit**.

ACS lists the new configuration in the External User Database Configuration table.

Step 5 Under External User Database Configuration, select the name of the RADIUS-enabled token server that you configure.

Note If only one RADIUS-enabled token server configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

Step 6 Click **Configure**.

Step 7 In the RADIUS Configuration table, type the required information in the following boxes:

- **Primary Server Name/IP**—The hostname or IP address of the primary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Secondary Server Name/IP**—The hostname or IP address of the secondary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Shared Secret**—The shared secret of the RADIUS server. This must be identical to the shared secret with which the RADIUS token server is configured.
- **Authentication Port**—The UDP port over which the RADIUS server conducts authentication sessions. If the RADIUS token server is installed on the same Windows server as ACS, this port should not be the same port that ACS uses for RADIUS authentication. For more information about the ports that ACS uses for RADIUS, see RADIUS, page 1-3.

Note For ACS to send RADIUS OTP messages to a RADIUS-enabled token server, you must ensure that gateway devices between the RADIUS-enabled token server and ACS allow communication over the UDP port that is specified in the **Authentication Port** box.

- **Timeout (seconds):**—The number of seconds that ACS waits for a response from the RADIUS token server before retrying the authentication request.
- **Retries**—The number of authentication attempts that ACS makes before failing over to the secondary RADIUS token server.

- **Failback Retry Delay (minutes)**—The number of minutes that ACS sends authentication requests to the secondary server when the primary server has failed. When this duration elapses, ACS reverts to sending authentication requests to the primary server.

Note If the primary and the secondary servers fail, ACS alternates between the servers until one responds.

Step 8 If you want to support token users who perform a shell login to a TACACS+ AAA client, you must configure the options in the TACACS+ Shell Configuration table. Perform one of the following procedures:

- If you want ACS to present a custom prompt for tokens, select **Static (sync and async tokens)**, and then type in the **Prompt** box the prompt that ACS will present.

  For example, if you type **Enter your PassGo token** in the **Prompt** box, users receive an **Enter your PassGo token** prompt rather than a password prompt.

Note If some tokens that are submitted to this server are synchronous tokens, you must click the **Static (sync and async tokens)** option.

- If you want ACS to send the token server a password to trigger a challenge, select **From Token Server (async tokens only)**, and then, in the **Password** box, type the password that ACS will forward to the token server.

  For example, if the token server requires the string **challengeme** in order to evoke a challenge, you should type **challengeme** in the **Password** box. Users will receive a username prompt and a challenge prompt.

Tip Most token servers accept a blank password as the trigger to send a challenge prompt.

Note You should only click the **From Token Server (async tokens only)** option if all tokens that are submitted to this token server are asynchronous tokens.

Step 9 Click **Submit**.

ACS saves the RADIUS token server database configuration that you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 16-3. For more information about configuring user accounts to authenticate by using this database, see Chapter 7, "User Management."

RSA SecurID Token Servers

ACS supports ASCII, PAP, and PEAP (EAP-GTC) authentication for RSA SecurID token servers. Other authentication protocols are not supported with RSA SecurID external user databases.

Note Authentication protocols not supported with RSA SecurID databases might be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-7.

ACS supports mapping users who are authenticated by a RSA token server to a single group. For more information, see Group Mapping by External User Database, page 17-1.

ACS supports PPP (ISDN and async) and Telnet for RSA SecurID token servers by acting as a token-card client to the RSA SecurID token server. To use this client you must install the RSA token-card client software on the computer that is running ACS. The following procedure includes the steps that you follow to install the RSA client correctly on the computer that is running ACS.

Configuring an RSA SecurID Token Server External User Database

ACS supports the RSA SecurID token server custom interface for authentication of users. You can create only one RSA SecurID configuration within ACS.

Before You Begin

You should install and configure your RSA SecurID token server before configuring ACS to authenticate users with it. For information about installing the RSA SecurID server, refer to the documentation for your token server.

Ensure that you have the applicable RSA ACE Client.

To configure ACS to authenticate users with an RSA token server:

Step 1 Install the RSA client on the computer that is running ACS:

a. With a username that has administrative privileges, log in to the computer that is running ACS.

b. Run the Setup program of the ACE Client software, following the setup instructions that RSA provides.

Note Do not restart Windows when installation is complete.

c. Locate the ACE Server data directory, for example, `/sdi/ace/data`.

d. Get the file named `sdconf.rec` and place it in the following Windows directory: `%SystemRoot%\system32`.

For example:

`\winnt\system32`

e. Ensure that the ACE server hostname is in the Windows local host file:

`\`*Windows directory*`\system32\drivers\etc\hosts`

f. Restart the computer that is running ACS.

g. Verify connectivity by running the Test Authentication function of your ACE client application. You can run this from the Control Panel.

Step 2 In the navigation bar, click **External User Databases**.

Step 3 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 4 Click **RSA SecurID Token Server**.

If no RSA SecurID token server configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 5 If you are creating a configuration:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the RSA SecurID token server in the box provided, or accept the default name in the box.

c. Click **Submit**.

ACS lists the new configuration in the External User Database Configuration table.

Step 6 Click **Configure**.

ACS displays the name of the token server and the path to the authenticator dynamic link library (DLL). This information confirms that ACS can contact the RSA client. You can add the RSA SecurID external user database to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 16-3. For more information about configuring user accounts to authenticate by using this database, see Chapter 7, "User Management."

Deleting an External User Database Configuration

If you no longer need a particular external user database configuration, you can delete it from ACS.

To delete an external user database configuration:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 3 Click the external user database type for which you want to delete a configuration.

The External User Database Configuration table appears.

Step 4 If a list appears in the External User Database Configuration table, select the configuration to delete. Otherwise, proceed to Step 5.

Step 5 Click **Delete**.

A confirmation dialog box appears.

Step 6 Click **OK** to confirm that you want to delete the selected external user database configuration.

The external user database configuration that you selected is deleted from ACS.

Posture Validation

This chapter contains the following topics:

- What is Posture Validation?, page 14-1
- Network Access Control Overview, page 14-1
- Posture Validation in ACS, page 14-4
- Configuring Policies, page 14-17 (including internal, external, and audit server)
- How Posture Validation Fits into Profile-Based Policies, page 14-27

What is Posture Validation?

The term *posture* is used to refer to the collection of attributes that play a role in the conduct and "health" of the endpoint device that is seeking access to the network. Some of these attributes relate to the endpoint device-type and operating system; other attributes belong to various security applications that might be present on the endpoint, such as antivirus (AV) scanning software.

Posture validation, or posture assessment, refers to the act of applying a set of rules to the posture data to provide an assessment (posture token) of the level of trust that you can place in that endpoint. The posture token is one of the conditions in the authorization rules for network access. Posture validation, together with the traditional user authentication, provides a complete security assessment of the endpoint device and the user.

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, supports posture validation when ACS is deployed as part of a broad Cisco Network Access Control (NAC) solution.

Network Access Control Overview

NAC is a set of technologies and solutions built on an industry initiative led by Cisco Systems. It uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources; thereby limiting damage from emerging security threats. Customers using NAC can allow network access only to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can restrict the access of noncompliant devices.

This section contains the following topics:

- Benefits of NAC, page 14-2
- NAC Architecture Overview, page 14-2

- Posture Tokens, page 14-3

For more information about the NAC solution, see http://www.cisco.com/go/nac

Benefits of NAC

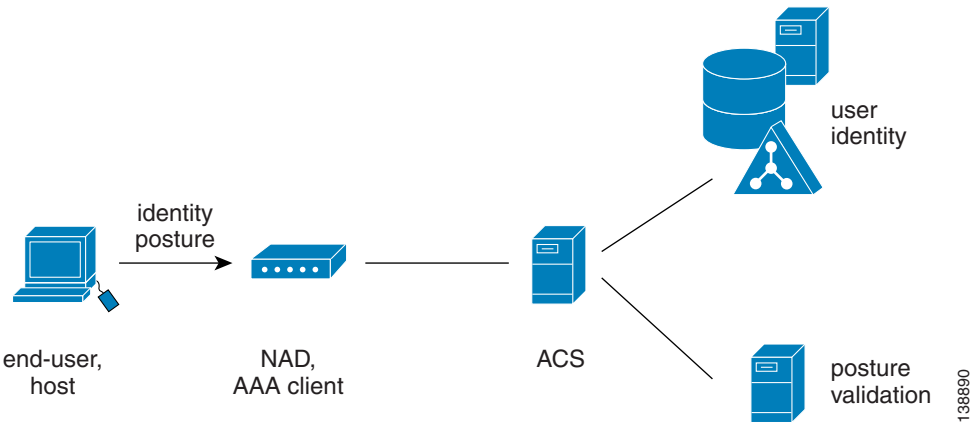
NAC:

- **Dramatically improves any network's security**—NAC ensures that all endpoints conform to the latest security policy; regardless of the size or complexity of the network. With NAC in place, you can focus operations on prevention, rather than on reaction. As a result, you can proactively protect against worms, viruses, spyware, and malicious software before they are introduced into your network.
- **Extends the value of your existing investments**—Besides being integrated into the Cisco network infrastructure, NAC enjoys broad integration with antivirus, security, and management solutions from dozens of leading manufacturers.
- **NAC provides deployment scalability and comprehensive span of control**—NAC provides admission control across all access methods (LAN, WAN, wireless, and remote access).
- **Increases enterprise resilience**—NAC prevents noncompliant and rogue endpoints from affecting network availability.
- **Reduces operational expenses**—NAC reduces the expense of identifying and repairing noncompliant, rogue, and infected systems.

NAC Architecture Overview

Figure 14-1 shows the components of a typical NAC deployment.

Figure 14-1 Components of a Typical NAC Deployment



Typical NAC components are:

- **End-user or host**—Also known as the endpoint. The endpoint is a device such as a PC, workstation or server that is connected to a switch, access point, or router through a direct connection. In a NAC deployment, the host that is running the Cisco Trust Agent (CTA) application, collects posture data from the computer and from any NAC-compliant applications that are installed on the computer. For more information about posture credentials, see Posture Validation Attribute Data Types, page 14-8.

Examples of NAC-compliant applications are the Cisco Security Agent and anti-virus programs from Network Associates, Symantec, or Trend Micro. These applications provide CTA with attributes about themselves, such as the version number of a virus definition file.

A NAC agentless host (NAH) is an endpoint that is not running the Cisco CTA application.

- **Network Access device (NAD)**—In a NAC deployment the AAA client is called a NAD. The NAD is a Cisco network access device, such as a router or switch, which acts as a NAC enforcement point.
- **ACS**—ACS performs the validation of the endpoint device by using internal policies, external policy servers, or both, to which the posture credentials are forwarded.
- **External posture validation servers**—These perform posture validation and return a posture token to ACS. In a NAC deployment with agentless hosts, you can configure ACS to invoke the services of a special type of posture validation server, called an audit server. An audit server uses out-of-bound methods, such as port scans, to validate the health of the endpoint device, and reports the result as a posture token to ACS.
- **Remediation servers**—Provide repair and upgrade services to hosts that do not comply with network admission requirements.

Posture Tokens

Posture tokens represent the state of an endpoint device or a NAC-compliant application that is installed on the computer. A token that is associated with the state of the computer is a system posture token (SPT). A token that is associated with the state of a NAC-compliant application is an application posture token (APT).

APTs are the result of applying a policy to the credentials that are received in a posture-validation request. ACS determines the SPT of each request by comparing the APTs from all policies that are applied to the request. The most severe APT becomes the SPT.

Table 14-1 describes the six predefined, non-configurable posture tokens, used for system and application posture tokens. They are listed in order from least to most severe.

Table 14-1 ACS Posture Tokens

Token	Description
Healthy	The endpoint device complies with the currently required credentials so you do not have to restrict this device.
Checkup	The endpoint device is within the policy but does not have the latest security software; update recommended. Use to proactively remediate a host to the `Healthy` state.
Transition	The endpoint device is in the process of having its posture checked and is given interim access pending a result from a full posture validation. Applicable during host boot where all services may not be running or while audit results are not yet available.
Quarantine	The endpoint device is out of policy and needs to be restricted to a remediation network. The device is not actively placing a threat on other hosts; but is susceptible to attack or infection and should be updated as soon as possible.
Infected	The endpoint device is an active threat to other hosts; network access should be severely restricted and placed into remediation or totally denied all network access.
Unknown	The posture credentials of the endpoint device cannot be determined. Quarantine the host and audit, or remediate until a definitive posture can be determined.

From the perspective of ACS, the actions that you set in your authorization rule determine the meaning of an SPTe. These actions associate a token with RADIUS authorization components (RACs), DACLs, or both. The authorization rule may also specify a user group as part of the condition. For details on configuring RACs, see Adding RADIUS Authorization Components, page 5-9. For details on setting up your authorization rules as part of network access profiles, see Setting Up a Profile, page 15-3.

Posture validation requests resulting in an SPT for which access is not strictly denied are logged in the Passed Authentications log. Posture validation requests resulting in an SPT for which access is denied are logged in the Failed Attempts log. For more information on logging and reports, see Posture-Validation Attributes in Logs, page 11-3.

ACS only uses APTs to determine the SPT; but the endpoint device receiving the results of the posture validation can use them based on their meanings to the relevant NAC-compliant application.

Posture Validation in ACS

This section provides overview information on posture validation and NAC support in ACS.

- Configuring NAC in ACS, page 14-4
- Posture Validation Process, page 14-6
- Policy Overview, page 14-7
- Internal Policies, page 14-9
- External Policies, page 14-11
- NAH Policies, page 14-14

Configuring NAC in ACS

This section provides an overview of the steps to configure posture validation in ACS, with references to more detailed procedures for each step.

Note Design your posture policies by using the Posture Validation tab and then assign those policies to profiles by using the Posture Validation link inside the Network Access Profiles tab.

Before You Begin

Before ACS can perform posture validation, you must complete several configuration steps. An overview of the steps follows. For information on finding detailed instructions on Cisco.com, see Network Access Control Overview, page 14-1.

To implement posture validation:

Step 1 Install a server certificate. ACS requires a server certificate for NAC because an EAP tunnel protects NAC communication with an end-user client. You can use a certificate that is acquired from a third-party certificate authority (CA) or you can use a self-signed certificate.

For detailed steps about installing a server certificate, see Installing an ACS Server Certificate, page 10-25. For detailed steps about generating and installing a self-signed certificate, see Generating a Self-Signed Certificate, page 10-34.

Note If you use a self-signed certificate, you may need to export the certificate from ACS and import it as a trusted root CA certificate into local storage on the endpoint computers.

Step 2 For posture credentials from a third-party vendor, you must import the corresponding NAC attribute definition file (ADF). For detailed steps on importing and ADF, see Import Vendor Attribute-Value Pairs (AVPs), page 15-36.

Step 3 To set up external policies or use external policy audit servers, you should plan on configuring ACS to communicate with the external server over HTTPS; although ACS also supports HTTP communication.

ACS authenticates the audit servers and posture validation servers by using certificates. You must choose the certificate from ACS or configure the Certificate Trust List (CTL). If the external servers use a different CA than the CA that issued the ACS server certificate, then you must configure the CTL. For detailed steps, see Editing the Certificate Trust List, page 10-27.

If your external server uses a self-signed certificate, you do not need to alter the CTL.

Tip You must add your audit vendor to the ACS internal dictionary by using the `CSUtil.exe` command before you can configure an external posture validation audit server. For detailed instructions, see Importing External Audit Posture-Validation Servers, page D-33.

Step 4 Enable the Passed Authentications log. ACS uses this log to log all posture validation credentials whenever access is not strictly denied. If the requests were denied, then ACS logs the results in the Failed Attempts log. When you enable the Passed Authentications log, be sure to move NAC-related attributes to the Logged Attributes column on the Passed Authentications File Configuration page.

For detailed steps about configuring this type of log, see Configuring a CSV Log, page 11-14.

Step 5 Configure the Failed Attempts log to include NAC attributes. Posture validation requests that were denied are logged to the Failed Attempts log. Including NAC attributes in this log can help you debug errors in your NAC implementation. For example, if none of the posture validation rules is matched, the request is logged here. Using the Failed Attempts log, you can see the contents of the attributes that are received in the request from the endpoint and sent in the reply to the endpoint.

For detailed steps about configuring this type of log, see Configuring a CSV Log, page 11-14.

Step 6 On the Global Authentication Setup page, enable posture validation by selecting **Allow Posture Validation** under EAP. Complete the steps for layer 2 or layer 3 support.

For detailed steps, see Configuring Authentication Options, page 10-19.

Step 7 If you have not already configured the AAA clients supporting NAC in the Network Configuration section, do so now.

For detailed steps, see Adding AAA Clients, page 4-11.

Step 8 From **Network Access Profiles**, set up the user groups that you want to use for posture validation. You are likely to want a separate user group for each possible SPT; therefore, select six user groups. If possible, choose groups that have not been configured to authorize users. Additionally, consider using groups that are widely separated from groups that authorize users. For example, assuming that the lowest numbered groups have been used for user authorization, consider using groups 494 through 499.

Step 9 For detailed steps on setting up profiles, see Setting Up a Profile, page 15-3.

Tip To avoid confusion between groups that are intended to authorize users and groups that are intended to authorize endpoints, consider renaming the groups with an easily understood name. For example, if you selected group 499 to contain authorizations that are related to the Unknown SPT, you could rename the group **NAC Unknown**. For detailed steps, see Renaming a User Group, page 6-40.

Step 10 For each posture validation rule, assign a posture token and an SPT, which you can later associate with a profile that contains downloadable IP ACL sets and/or RACs that limit network access appropriately.

For detailed steps on creating rules, see Creating an Internal Policy, page 14-18. For detailed steps, see Adding a Downloadable IP ACL, page 5-15 (and Adding RADIUS Authorization Components, page 5-9.) To associate posture rules to profiles, see Setting Up a Profile, page 15-3.

Step 11 For each profile, you can create several different posture validation policies that contain any number of rules to validate your endpoint device. You can:

a. Create a policy and its associated rules, including configuring mandatory credential types and policies.

   For detailed steps, see Configuring Policies, page 14-17.

b. Use **Network Access Profiles** to assign posture validation policies to profiles to validate your endpoint devices.

   For detailed steps, see Setting Up a Profile, page 15-3.

Posture Validation Process

ACS evaluates the posture attributes received from an endpoint computer. The following overview describes the steps and systems involved in posture validation. Details about various concepts, such as posture tokens and policies, are provided in topics that follow.

1. Following a network event (for example, **EoLAN Hello**=802.1 or traffic captured ny the EoU ACL on the NAD), the NAD initiates an EAP conversation with the endpoint and forwards EAP messages from the endpoint to ACS.
2. ACS establishes a secure conversation with the host by using PEAP or EAP-FAST (depending on the ACS configuration and endpoint support).
3. (EAP-FAST only and optional) ACS authenticates the end user.
4. ACS queries the endpoint for posture attributes. In response, the endpoint sends posture attributes to ACS.
5. ACS performs the evaluation of the posture attributes internally and/or uses external posture validation servers. The evaluation results in a set of application posture tokens (APTs). ACS then evaluates the system posture token (SPT) by using the most severe APT.
6. Based on authorization rules that you set in Network Access Profiles, ACS sends the endpoint computer the system posture token and the results of each policy that is applied to the posture validation request, and then ends the EAP session. Based on the evaluation that ACS grants the client network access based on access limitations; or the noncompliant device can be denied access, placed in a quarantined network segment, or given restricted access to computing resources.

You can set up many types of restrictions in authorization rules by using various RADIUS attributes in the RAC (which might be combined with the user's group), downloadable ACL, and url-redirect or `status-query-timeout`.

7. ACS sends the AAA client the RADIUS attributes as configured in the shared RAC, including ACLs and attribute-value pairs that are configured in the Cisco IOS/PIX 6.0 RADIUS attribute `cisco-av-pair`.
8. ACS logs the results of the posture validation request. If the request was not denied, ACS logs the results in the Passed Authentications log (if enabled). If the request was denied (for instance by the authorization policy or if no posture validation rule with matched required credential types was present), then ACS logs the results in the Failed Attempts log.

   The endpoint handles the results of the posture validation request according to its configuration. The AAA client enforces network access as dictated by ACS in its RADIUS response. By configuring profiles, you define authorizations and, therefore, network access control, based on the system posture token that is determined as a result of posture validation.

Policy Overview

You can use ACS to set up internal or external posture validation policies that return a posture token and an action after checking the rules that you (or the external server) set for the policy.

Policies are reusable; that is, you can associate a single policy with more than one network access profile. For example, if your NAC implementation requires two profiles, one for endpoints using NAI software and one for endpoints using Symantec software, you may need to apply the same rules about the operating system of the endpoint; regardless of which anti-virus application is installed. You can create a single policy that enforces rules about the operating system and associate it with the Symantec and the NAI server information.

The results of applying a policy are:

- **Posture Assessment**—The credential type and, therefore, the NAC-compliant application to which the policy evaluation result applies.
- **Token**—One of six predefined tokens that represents the posture of the endpoint and, specifically, the application that the result credential type defines.
- **Notification String**—An optional text string that is sent in the posture validation response to the application that the posture assessment defines.

About Posture Credentials and Attributes

For posture validation, credentials are the sets of attributes sent from the endpoint to ACS. Also known as inbound attributes, these attributes contain data that is used during posture validation to determine the posture of the computer. ACS considers attributes from each NAC-compliant application and from CTA to be different types of credentials.

With policies that ACS creates for validation, the rules that you create use the content of inbound attributes to determine the APT returned by applying the policy. With policies that are created for validation by an external server, ACS forwards the credential types that you specify to the external NAC server. In either case, the contents of inbound attributes provide the information that is used to determine posture and, thus, to control network admission for the computer.

ACS uses NAC attributes in its response to the endpoint. These attributes are called outbound attributes. For example, APTs and the SPT are sent to the endpoint in attributes.

Credential types are uniquely identified by two identifiers: vendor ID and application ID. The vendor ID is the number that is assigned to the vendor in the IANA Assigned Numbers RFC. For example, vendor ID 9 corresponds to Cisco Systems, Inc. Vendors assign numbers to the NAC applications that they provide. For example, with Cisco Systems, Inc., applications, application ID 1 corresponds to CTA. In the HTML interface, when you specify result credential types for a policy, credential types are identified by the names that are assigned to the vendor and application. For example, the credential type for CTA is Cisco:PA (where PA refers to posture agent, another term for CTA). In a posture validation response, ACS would use the numeric identifiers 9 and 1, which are the identifiers for Cisco and CTA, respectively.

Attributes are uniquely identified by three identifiers: vendor ID, application ID, and attribute ID. For each unique combination of vendor and application, there are set of attributes that each have numbers as well. When ACS communicates with an endpoint, the identifiers are numerical. In the HTML interface, when you define rules for internal policies, attributes are identified by the names that are assigned to vendor, application, and attribute. For example, the CTA attribute for the version of the operating system is Cisco:PA:OS-Version. The data that ACS receives identifies the attribute with the numeric identifiers 9, 1, and 6, which are the identifiers for Cisco, CTA, and the sixth attribute of CTA, respectively.

For more information about attributes, including data types and operators that are used in rules for internal policies, see Posture Validation Attribute Data Types, page 14-8. We recommend that you use RDBMS Synchronization to add and configure custom RADIUS vendors; however, you can use `CSUtil.exe` to accomplish the same custom RADIUS vendor and VSA configurations that you can accomplish by using RDBMS Synchronization. For information about using `CSUtil.exe` to export, add, or delete posture validation attributes, see Posture-Validation Attributes, page D-28.

Extended Attributes

You use extended attributes to configure conditions that support Linux clients, and are specific for different Linux packages. For example, you can configure a condition for the version of the **openssl** package.

You input values for these Linux packages in the Entity field. When you input an extended attribute from the attribute drop-down list, the entity field is enabled. You can then select an entity from the drop-down list.

For example, if you select the *`Cisco:Host:Package:Version`* attribute, which is an extended attribute, the Entity drop-down list displays all the Linux packages that are configured in the system (ACS).

You can add or delete extended attributes by using `CSUtil.ese`. For more details, see Posture-Validation Attributes, page D-28.

Posture Validation Attribute Data Types

Posture validation attributes can be one of the following data types:

- **boolean**—The attribute can contain a value of 1 or 0 (zero). In the HTML interface, when you define a rule element with a boolean attribute, the words `false` and `true` are valid input. Valid operators are `=` (equal to) and `!=` (not equal to). When a rule element using a Boolean attribute is evaluated, `false` corresponds to a value of 0 (zero) and `true` corresponds to 1.

  For example, if a rule element for a Boolean attribute requires that the attribute is not equal to `false` and the attribute in a specific posture validation request was 1, ACS would evaluate the rule element to be true; however, to avoid confusion, you can express the rule element more clearly by requiring that the attribute is equal to `true`.

- **string**—The attribute can contain a string. Valid operators are `=` (equal to), `!=` (not equal to), `contains`, `starts-with`, and `regular-expression`.

- **integer**—The attribute can contain an integer, including a signed integer. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), >= (greater than or equal to). Valid input in rule elements is an integer between -65535 and 65535.
- **unsigned integer**—The attribute can contain only an integer without a sign. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid input in rule elements is a whole number between 0 and 4294967295.
- **ipaddr**—The attribute can contain an IPv4 address. Valid operators are = (equal to), != (not equal to), and `mask`. Valid format in rule elements is dotted decimal format. If the operator is `mask`, the format is the `mask`/`IP`. For more information, see Internal Policy Configuration Options, page 14-10.
- **date**—The attribute can contain a date. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), >= (greater than or equal to), and `days-since-last-update`. Valid format in rule elements:

  mm/*dd*/*yyyy*
  hh:*mm*:*ss*

- **version**—The attribute can contain an application or data file version. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid format in rule elements:

  n.*n*.*n*.*n*

  where each *n* can be an integer from 0 to 65535.
- **octet-array**—The attribute can contain data of arbitrary type and variable length. Valid operators are = (equal to) and != (not equal to). Valid input in rule elements is any hexadecimal number, such as 7E (the hexadecimal equivalent of 126).

Internal Policies

This section contains the following topics:

- About Internal Policies, page 14-9
- About Rules, Rule Elements, and Attributes, page 14-10
- Internal Policy Configuration Options, page 14-10

About Internal Policies

Internal policies comprise one or more rules that you define in ACS. When ACS applies an internal policy, it uses the policy rules to evaluate credentials that are received with the posture validation request. Each rule is associated with an APT, a credential type, and an action. The credential type determines which NAC-compliant application with which the APT and action are associated.

ACS applies each rule in the order they appear on the Posture Validation Policies page (from top to bottom), resulting in one of the following two possibilities:

- **A configurable rule matches**—When all elements of a rule are satisfied by the credentials that are received in a posture validation request, the result of applying the policy is the condition, posture assessment, and notification string that are associated with the rule. ACS does not evaluate the credentials with any additional rules.
- **No configurable rule matches**—When the attributes that are included in the posture validation request satisfy no policy rules, ACS uses the condition, posture assessment, and notification string that are associated with the default rule as the result of the policy.

Note Applying a policy to a posture validation request always results in a match, to one of the configurable rules or to the default rule.

When you specify the order of rules in a policy, determine the likelihood of each rule to be true and then order the rules so that the rule most likely to be true is first and the rule least likely to be true is last. Doing so makes rule processing more efficient; however, determining how likely a rule is to be true can be challenging. For example, one rule may be true for the posture of twice as many endpoints as a second rule, but posture validation may occur more than twice as often for endpoints whose posture matches the second rule; therefore, the second rule should be listed first.

About Rules, Rule Elements, and Attributes

A rule is a set of one or more rule elements. A rule element is a logical statement which comprises:

- A posture validation attribute
- An operator or posture token
- A value or notification string

ACS uses the operator to compare the contents of an attribute to the value. Each rule element of a rule must be true for the whole rule to be true. In other words, all rule elements of a rule are joined with a Boolean AND.

For detailed descriptions of rules, see Setting Up a Profile, page 15-3.

Internal Policy Configuration Options

You can specify the rules that a policy comprises, including their order from the Internal Posture Validation Setup pages. The options for configuring a internal policy are as follows:

- **Name**—Specifies the name by which to identify the policy. When selecting a policy, you select it by name, and the description is not viewable on the policy selection page; therefore, you should make the name as useful as possible.

  Note The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the left bracket ([), the right bracket (]), the comma (,), and the slash (/).

- **Description**—Specifies a text description of the policy, up to 255 characters. In the **Description** box you enter details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules. Because you can apply the same policy to more than one profile, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which servers use it.
- **Posture Validation Rules**—Lists rules that you define in the order in which ACS uses them to evaluate the posture validation request. Each rule appears as a separate row in the table and is identified by its rule elements, which appear as a blue link in the Posture Validation Rules page. You can order the rules in this table by selecting the option directly to the left of a rule and clicking **Up** and **Down** to position it as needed. For more information about the order of rules, see About Internal Policies, page 14-9.

The Posture Validation Rules table contains:

- **Condition**—Specifies a vendor and application; the credential type. If the rule is true, the credential type determines the application to which the token in the corresponding Token list is associated. For example, CTA appears on the list as `Cisco:PA`. For more information about credential types, see About Posture Credentials and Attributes, page 14-7.
- **Posture Assessment**—Specifies the vendor and application, and a token (an APT). If the rule is true, the Token list determines the APT that is associated with the vendor and application that is selected in the corresponding Posture Assessment list. For more information about tokens, see Posture Tokens, page 14-3.
- **Notification String**—Specifies a text message that is sent to the application that the Result Credential Type list indicates. The vendor determines use of the text message. Some NAC-compliant applications do not implement the use of the Notification String box.

- **Default Rule**—If no configurable rule is true, the Default Rule specifies the posture assessment, token, and notification string (if specificed) that ACS uses as the result of applying the policy.

Note Under Default Rule, the meanings of the Posture Assessment list, Token list, and Notification String box are identical to the options of the same name in the Posture Validation Rules table; except that the default rule is automatically true, provided that no rule in the Posture Validation Rules table is true.

External Policies

This section contains the following topics:

- About External Policies, page 14-11
- External Policy Configuration Options, page 14-12

About External Policies

External policies are policies that are defined by an external NAC server, usually from an anti-virus vendor and a set of credential types to be forwarded to the external database. You also have the option of defining a secondary external NAC server. The presence of a secondary server allows The secondary or failover to evaluate any policies from the primary server.

ACS does not determine the result of applying an external policy; instead, it forwards the selected credentials to the external NAC server and expects to receive the results of the policy evaluation: an APT, a result credential type, and an action.

Each external policy that is associated with a external server must return a result; otherwise, ACS rejects policy validation requests that are evaluated with a profile whose external policies do not return a result. For example, if ACS evaluates a posture validation request by using a profile that has 10 internal policies and one external policy, but the external NAC servers associated with the external policy are not online, it is irrelevant that the 10 internal policies all return SPTs. The failure of the single external policy causes ACS to reject the posture validation request.

External Policy Configuration Options

On the External Posture Validation Setup page you can specify a NAC server (and an optional second NAC server) that ACS relies upon to apply the policy and configure the set of credential types that ACS forwards. The options for configuring an external policy are as follows:

- **Name**—Specifies the name by which to identify the policy.

  Note The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the left bracket ([), the right bracket (]), the comma (,), and the slash (/).

- **Description**—Specifies a text description of the policy, up to 255 characters. For each profile using the policy, the text you type in the **Description** box appears beside the policy. Use the Description box to provide details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules.

  Because you can apply the same policy to more than one profile, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which profiles use it.

- **Server Configuration**—You must specify a primary server. You can specify a secondary server for failover operation. For each posture validation request to which an external policy is applied, ACS attempts to use the first enabled server configuration in the policy that is enabled. If the first enabled server is the primary server and ACS cannot reach the primary server or the primary server fails to respond to the request, ACS will use the secondary server, if it is configured and enabled.

  For the primary and secondary server configurations, each have:

  – **URL**—Specifies the HTTP or HTTPS URL for the server. The format for URLs is:

    `[http[s]://]`*host*`[:`*port*`]/`*resource*

    where *host* is the hostname or IP address of the NAC server, *port* is the port number used, and *resource* is the rest of the URL, as required by the NAC server itself. The URL varies depending upon the server vendor and configuration. For the URL that your NAC server requires, refer to your NAC server documentation.

    The default protocol is HTTP. URLs beginning with the hostname are assumed to be using HTTP. To use HTTPS, you must specify the URL beginning with `https://` and you must import a self-generated CA certificate into ACS for this policy server. See ACS Certificate Setup, page 10-25.

    If the port is omitted, the default port is used. The default port for HTTP is port 80. The default port for HTTPS is port 443.

    If the NAC server hostname is *antivirus1*, which uses port 8080 to respond to HTTP requests for the service provided *policy.asp*, a script kept in a web directory called *cnac*, valid URLs would be:

    ```
    http://antivirus1:8080/cnac/policy.asp
    antivirus1:8080/cnac/policy.asp
    ```

    If the same server used the default HTTP port, valid URLs would be:

    ```
    http://antivirus1/cnac/policy.asp
    http://antivirus1:80/cnac/policy.asp
    antivirus1/cnac/policy.asp
    antivirus1:80/cnac/policy.asp
    ```

If the same server used HTTPS on the default port, valid URLs would be:

```
https://antivirus1/cnac/policy.asp
https://antivirus1:443/cnac/policy.asp
```

- **Username**—Specifies the username by which ACS submits forwarded credentials to the server. If the server is not password protected, the values in the Username and Password boxes are ignored.
- **Password**—Specifies the password for the username in the Username box.
- **Timeout (Sec)**—The number of seconds that ACS waits for a reply from a server after it forwards the credentials.

  If a secondary server is configured, requests to the primary server that time out are forwarded to the secondary server.

  If no secondary server is configured or if a request to the secondary server also times out, ACS cannot apply the external policy and the posture validation request is rejected.

  For each posture validation request, ACS always tries the primary server first, regardless of whether previous requests timed out.
- **Trusted Root CA**—The certificate authority (CA) that issued the server certificate that the uses server. If the protocol is HTTPS, ACS forwards credentials to a server only if the CA that is specified on this list issued the certificate that it presents. If ACS cannot forward the request to the primary or secondary NAC server because the trusted root CAs did not issue the server certificates, the external policy cannot be applied and, therefore, the posture validation request is rejected.

  If the Trusted Root CA list does not contain the CA that issued a NAC server certificate, you must add the CA certificate to ACS. For more information, see Adding a Certificate Authority Certificate, page 10-27.

Note ACS does not check NAC server certificates against certificate revocation lists, regardless of whether you have configured a CRL issuer for the CA of the NAC server certificate.

Tip You must select the correct certificate type for the CA, not just the name of the CA. For example, if the server presents a VeriSign Class 1 Primary CA certificate and VeriSign Class 1 Public Primary CA is selected on the Trusted Root CA list, ACS does not forward the credentials to the server when HTTPS is in use.

- **Forwarding Credential Types**—Contains two lists for use in specifying which credential types are forwarded to the external server. The credentials are:
  - **Available Credentials**—Specifies the credential types that *are not* sent to the external server.
  - **Selected Credentials**—Specifies the credential types that *are* sent to the external server.

Tip You can add credential types by using the **CSUtil** command. For detailed instructions, see Importing External Audit Posture-Validation Servers, page D-33.

NAH Policies

This section contains the following topics:

- About External Audit Servers, page 14-14
- External Audit Server Configuration Options, page 14-16

About External Audit Servers

Audit servers are Cisco and third-party servers that determine posture information about a host without relying on the presence of a Posture Agent (PA). The Cisco PA is also known as the Cisco Trust Agent (CTA). Audit servers are used to assess posture validation with an organization's security policy. You can also define a secondary external audit server. The presence of a secondary audit server allows the second or failover server to evaluate any policies from the primary server when the primary server rejects a policy.

An audit policy is a set of processing rules for evaluating the posture of a NAH through an audit server. Audit policies are used to retrieve posture decisions for hosts that do not have an EAP supplicant. When a host accesses the network through a NAD that is acting as a NAC enforcement point, the NAD sends information to ACS so that ACS can trigger auditing. If ACS is configured correctly, it queries the audit server for the result (posture token) of the audit and then determines the authorization based on the audit result.

Your network-management security strategy may include external audit servers that work with ACS to control access to your network.

ACS will use the **GAME** protocol to communicate with audit servers. In each audit request, ACS forwards the following information to the audit server:

- `host id`
- `ip-address`
- `mac-address` (optional)

The name of the System-Posture-Token is dynamically sent (without requiring any configuration) to the device.

Table 14-2 defines the details required in applying the results of an audit.

Table 14-2 Audit Policy Requirements

Audit Policy	Description
auditServerConfiguration	A pointer to the audit server configuration that defines how to communicate with the audit server.
exemptionList	A list of MAC and/or IP addresses that are exempt from audit.
inverseExemptionFlag	If this flag is set, the meaning of the exemption list will be inversed. That is, only the hosts specified in the list will be audited; all others will be exempt.
exemptionToken	The token to assign to hosts who are exempt.
defaultInProgressToken	The token to use when the audit is in progress and we have no cached token.

Table 14-2 Audit Policy Requirements (continued)

Audit Policy	Description
staticAttributes	These name value pairs will be sent to the audit server when this policy is invoked. For this release, this list of attributes will be used to pass the policy name.
tokenMappings	The token to user group mapping. Note that this scheme assumes that there is only one audit policy per service.

How an External Audit Gets Triggered

An endpoint failure triggers an external audit. This failure occurs when the enforcement point detects that the endpoint is not responding as required. The enforcement point sends the `aaa:event` failure message to indicate that a device failure has occurred.

The current release of ACS supports this event type and provides configuration in the out-of-band posture policy about which event should activate the policy (may be more than one).

ACS must be able to recognize the following events that may or may not trigger an audit, depending on policy configuration:

- NAS detects lack of functioning CTA and sends NRH notification in the `aaa:event` attribute
- Endpoint device (or supplicant) is unable to respond to a posture request
- An explicit audit request from the device

Once ACS recognizes that an audit will occur, the audit server is queried. The audit server responds with results or an audit-in-progress message, which may contain a polling timeout hint to pass on to the NAD. At this point, ACS evaluates the enforcement policy for the given host based on the default APT that is associated with the posture validation policies. Part of the enforcement policy must be a session-timeout value that is used to trigger the NAD to reauthenticate the host. ACS receives the request and queries the audit server. This process repeats itself until the audit server responds with an APT. Once the audit response is received, enforcement policies are reevaluated and returned to the NAD.

The NAD caches the posture token that will be sent along with any subsequent access requests occurring during the host's session; for instance, as a result of session timeout (reauthentication). ACS uses this token for default policy evaluation during the audit for these subsequent authentications, thereby avoiding session downgrade for the connected host.

Exemption List Support

ACS supports an exemption list for audit activation. The exemption list contains a list of IP or MAC addresses to include or exclude from the audit. When a host is exempted, it is assigned an exemption token that determines its posture status. The exemption list is defined in the out-of-band audit policy. The IP list may contain single IP addresses or IP mask ranges. The MAC lists may be MAC ranges in the form of partial MAC strings that are matched with the hosts MAC address by using the *begins with* operator.

External Audit Server Configuration Options

Table 14-3 describes the external audit server settings.

Table 14-3 External Audit Server Options

Options	Description
Which Hosts Are Audited	
Audit all hosts	Audit all hosts that do not contain a posture agent.
Audit these hosts	Audit only the hosts for which you have provided host IP addresses and ranges (IP/Mask) or MAC addresses.
Do not audit these hosts	Exclude the hosts for which you have provided host IP addresses and ranges (IP/Mask) or MAC addresses and audit all other hosts.
Select a token for the hosts that will not be audited	Select a token from the drop-down list for hosts that are not audited.
Use These Audit Servers	
Audit server vendor	Vendor name in ADF file. See Importing External Audit Posture-Validation Servers, page D-33 if no audit servers appear in the drop-down box.
Primary & Secondary Server Configuration	
URL	URL of the audit server. Refer to your audit server documentation for format guidelines.
Username	Credential ACS needs to access the audit server.
Password	Credential ACS needs to access the audit server.
Timeout (sec)	Number of seconds ACS waits for a result from the audit server, including domain name resolution.
Trusted Root CA	If the URL you provide specifies the HTTPS protocol, select the certification authority that issued the audit server certificate installed on the primary server from the Trusted Root CA list.
Validate Certificate Common Name	Enable this option to compare the host name within the URL to the common name in the certificate. If they do not match, the SSL connection is closed, posture validation fails, and user access will be denied. Leave this check box unchecked to disable this feature.
Audit Host Settings	
Use this token while Audit Server does not yet have a posture validation result	Interim posture token sent from ACS to the NAD while waiting for a result.
Polling Intervals and Session-Timeout:	Select whether ACS should use timeout values that are sent by the audit server or use settings in the authorization policy. If you select **Use Settings in Authorization Policy for Session-Timeout**, you must specify a polling interval in the Polling Interval (seconds) field. You must also configure any RACs in the authorization policy to assign specfic timeout values for the final resulting tokens. See Configuring an Authorization Rule, page 15-44..

Table 14-3 External Audit Server Options (continued)

Options	Description
Which Hosts Are Audited	
Maximum amount of times the Audit Server should be polled	Select the maximum amount of times ACS should query the audit server for a result (posture token). Maximum of 10 times.
Policy string to be sent to the Audit Server	If the audit server supports named policy invocation, enter the name of policy here.

Configuring Policies

If you plan to use NAC in your network, you will need to define the manner in which posture validation will be performed. Policies are sets of rules that are used to determine a posture token for a posture validation request.

You can configure posture validation, also known as posture compliance, as:

- Internally within ACS. See Setting Up Posture Validation Policies, page 14-18.
- Externally by using the Host Credential Authorization Protocol (HCAP) protocol to one or more Posture Validation Servers (PVSs). See Setting Up an External Policy Server, page 14-24.
- Externally by using the GAME protocol to an audit server for NAC agentless host (NAH) support. See Setting Up an External Audit Posture Validation Server, page 14-25.

Table 14-4 describes the setup options for posture validation.

Table 14-4 Posture Validation Options

Component	Description	Notes
Internal Posture Validation	Policy requirements for the network are internally (or locally) validated within ACS.	NAC policies for the CTA, Windows, CSA, and anti-virus software applications are among recommended internal policies. See Creating an Internal Policy, page 14-18
External Posture Validation	Policies are validated by an outside posture validation server.	Externalizing the posture validation to an AV server allows you to handle proprietary AV posture credentials and anti-virus policy administration by an AV administrator separate from the ACS administrator.
External Audit Posture Validation	Cisco and third-party servers that determine posture information about a host without relying on the presence of a PA. These types of hosts are also referred to as *agentless*. Audit servers are used to assess posture validation with an organization's security policy.	The Cisco PA is also known as the CTA. If no CTA is on the host, then an audit server can be used.

Note You can perform internal and external posture validation at the same time; but not for the same NAC credential types (vendor-application combinations).

To configure a policy for internal or external posture validation:

Step 1 In the navigation bar, click **Posture Validation**.

Step 2 Select one of the components to set up your posture validation servers:

- **Internal Posture Validation Setup**—See Internal Policies, page 14-9 or Creating an Internal Policy, page 14-18
- **External Posture Validation Setup**—See External Policies, page 14-11 or Setting Up an External Policy Server, page 14-24
- **External Posture Validation Audit Setup**—See NAH Policies, page 14-14 or Setting Up an External Audit Posture Validation Server, page 14-25

Step 3 Complete the required steps to set up internal or external posture validation.

Setting Up Posture Validation Policies

This section contains the following topics:

- Creating an Internal Policy, page 14-18
- Cloning a Policy or Policy Rule, page 14-21
- NAH Policies, page 14-14
- Editing a Policy, page 14-20
- Deleting a Policy or Rule, page 14-23

Creating an Internal Policy

Use internal posture validation to write your own policies for access in your network. After you have created policies, you can then profile rules to use these policies.

You can select internal policies for more than one profile. To add the policy to a profile, use the Network Access Profiles page.

For descriptions of the options available on the Internal Posture Validation Setup page, see Internal Policy Configuration Options, page 14-10.

For details on how to set up your third-party component policies, see the related documentation on the Go NAC website on Cisco.com. For information on adding internal policies to your profiles, see Configuring Posture-Validation Policies, page 15-35.

Once you have set up at least one policy, you can use the clone rule option to save time by copying a policy and customizing it. For details on how to use cloning, see Cloning a Policy or Policy Rule, page 14-21.

To create your internal posture validation policy:

Step 1 Access the Internal Policy Validation Setup page:

a. In the navigation bar, click **Posture Validation**.

b. Click **Internal Posture Validation Setup**.

ACS displays a list of posture validation policies, if available.

c. Click **Add Policy**.

Step 2 In the **Name** box, type a descriptive name for the policy.

Step 3 In the **Description** box, type a useful description of the policy.

Step 4 Click **Submit**.

Step 5 Click **Add Rule**.

Step 6 Set conditions to define.

a. For each condition set that you want to add:

i. Select an attribute. For more information about attribute types, see Posture Validation Attribute Data Types, page 14-8.

ii. Select an entity (only available for extended attributes).

iii. Select an operator.

iv. Type a value.

v. Click **Enter** and then **Submit**.

For example, if you create a policy for the Cisco Security Agent (CSA) you might create the following condition sets:

- *Cisco:PA:PA-Version >= 2.0.0.0* AND *Cisco:PA:Machine-Posture-State = 1 with a Posture token=Healthy.*
- *Cisco:PA:PA-Version >= 2.0.0.0* AND *Cisco:PA:Machine-Posture-State = 2 with a Posture Token=Transition.*
- Match OR inside Condition and AND between Condition Sets to allow ACS to choose between tokens.

For more information about operators, see Internal Policy Configuration Options, page 14-10.

For information on CTA posture plugin attributes and values, see the Cisco Trust Agent documentation.

The condition set appears in the Conditions Sets table.

b. Select which Boolean condition to add to this condition set:

- **Match OR inside Condition and AND between Condition Set**—Select if you want to be less stringent with your conditions.
- **Match AND inside Condition and OR between Condition Sets**—Select if you want to be more secure with your posture validation.

c. Verify that the condition sets are configured as intended.

Tip If you want to change a condition set that you have already added, select the condition element, click **Remove**, and update its attribute, entity, operator, or value, then click **Enter**.

d. For the new rule, do each of the following:

i. Select a credential type.

ii. Select a token.

iii. Type an action (in the form of an notification string).

For more information about tokens, see Posture Tokens, page 14-3.

If the rule matches the posture validation request, ACS associates with the policy the result credential type, token, and action that you specify.

Tip If you want to create another condition set that is identical to one that is already created, click **Clone**. Then change the condition set as needed.

Step 7 Click **Submit**.

The Policy Validation Rules page appears again. The new condition set appears at the bottom of the Condition Sets table.

Tip You can return to the Posture Validation Rules page by clicking the rule.

Step 8 After you create the rules that define the policy, order the rules as needed. ACS applies a policy by attempting to match rules in the order that they appear on the Policy Validation Rules page, from top to bottom. Policy processing stops at the first successful rule match; so order is important. To move a rule:

a. Select the rule. To do so, click the radio button to the left of the rule.

b. Click the **Up** or **Down** button as needed until the rule is positioned properly.

Step 9 Configure the Default Rule at the bottom of the Posture Validation Rules page by clicking **Default**:

i. Select a credential type.

ii. Select a token.

iii. Type an action (in the form of an notification string).

When ACS applies this policy to a posture-validation request and none of the configurable rules matches the request, ACS associates the default credential type, token, and action that you specify with the policy.

Step 10 Click **Submit**.

The Posture Validation Rules page displays the new rule.

Step 11 Click **Done**.

The current configuration has been changed.

Step 12 Click **Apply and Restart** for your changes to take effect.

Editing a Policy

You can only edit a policy by accessing it through the Posture Validation pages.

To edit a policy or posture validation rule:

Step 1 In the navigation bar, click **Posture Validation**.

Step 2 Click **Internal Posture Validation Setup**.

Step 3 Click on the policy name of the rule that you want to edit.

The applicable policy rules page appears.

Step 4 To edit a policy:

a. Click **Add Rule** to add more condition sets.

b. To change a condition set that you have already added:

   i. Select the condition element.

   ii. Click **Remove.**

   iii. Update its attribute, entity, operator, or value; then click **Enter**.

c. To add a new condition:

   i. Select the attribute, entity, and operator from the drop-down lists.

   b. Enter a value.

   c. Click **Enter**.

d. Click **Clone** to copy an existing condition set or policy rule.

e. Click **Delete** to remove policy rule. You can also remove a condition set or an element from a condition set. See Deleting a Condition Component or Condition Set, page 14-23.

f. To move a rule:

   i. Select the rule by clicking the button to the left of the rule.

   ii. Click the **Up** or **Down** button as needed until the rule is positioned properly.

g. If you want to add or change a Boolean condition to this condition set, select one of the options:

   - **Match OR inside Condition and AND between Condition Set**—Select if you want to be less stringent with your conditions.
   - **Match AND inside Condition and OR between Condition Sets**—Select if you want to be more secure with your posture validation.

h. Click **Rename** to change the existing name.

   ACS creates a new policy. ACS stores the new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.

Step 5 When finished with editing, click **Submit**. Then click **Done**.

Step 6 Click **Apply and Restart** for your changes to take effect.

Cloning a Policy or Policy Rule

This option creates a policy or rule that is identical to the selected one. You can then easily modify the settings.

To clone an internal posture validation policy or policy rule:

Step 1 If you have not already done so, access the Internal Policy Validation Setup page. To do so:

a. In the navigation bar, click **Posture Validation**.

b. Click **Internal Posture Validation Setup**.

   ACS displays a list of posture validation policies.

c. Select a policy name from the list.

Tip If no policies are configured, click **Add Policy** and follow the instructions in Creating an Internal Policy, page 14-18.

Step 2 To make a copy of the current policy, click **Clone**.

For example, if you selected ***VPNmgt1*** as the policy, the copy would be ***Copy-of-VPNmgt1***.

Step 3 To make a copy of one of the policy rules inside the current policy, click the condition name. Then click **Clone**.

The Policy Validation Rule page appears again. The new condition set appears in the Condition Sets table.

Step 4 Click **Rename** to change the existing name to a more meaningful name or description.

ACS creates a new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.

Step 5 When you finish with editing, click **Submit**.

Step 6 Click **Done** if you are finished adding clones.

Step 7 Click **Apply and Restart** for your changes to take effect.

Renaming a Policy

Use the renaming feature to change the name or description of an existing or cloned policy to something more meaningful.

To rename a policy:

Step 1 If you have not already done so, access the Internal Policy Validation Setup page. To do so:

a. In the navigation bar, click **Posture Validation**.

b. Click **Internal Posture Validation Setup**.

ACS displays a list of posture validation policies.

c. Select a policy name from the list.

Step 2 Click **Rename** to change the existing policy name or make the description more meaningful.

Step 3 Enter the changes to the policy name or description. When you finish editing, click **Submit**.

ACS creates a new policy. ACS stores the new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.

Step 4 Click **Done**.

The renamed policy appears at the bottom of the Posture Validation Policies page.

Step 5 Click **Apply and Restart** for your changes to take effect.

Deleting a Policy or Rule

To delete a policy or rule:

Step 1 If you have not already done so, access the Internal Policy Validation Setup page. To Access the Internal Policy Validation Setup page:

a. In the navigation bar, click **Posture Validation**.

b. Click **Internal Posture Validation Setup**.

ACS displays a list of posture validation policies.

Step 2 To delete a rule or policy, select a policy name from the list of posture validation policies.

The Posture Validation Rules page appears.

Step 3 To delete an entire policy and all its rules, click **Delete**.

This deletes the policy from the policy validation list; but does not remove the policy from any profiles with which it may be associated. A warning message prompts you to cancel or click **OK**.

Step 4 To delete an element or condition set, see Deleting a Condition Component or Condition Set, page 14-23.

ACS deletes the policy rule. The policies page reappears and the policies table no longer lists the deleted policy. All profiles that were configured to use the policy no longer include the deleted policy.

Deleting a Condition Component or Condition Set

A condition component is the list of elements that a condition set comprises. To delete a condition component from a condition set or an entire condition set:

Step 1 If you have not already done so, access the Internal Policy Validation Setup page. To Access the Internal Policy Validation Setup page:

a. In the navigation bar, click **Posture Validation**.

b. Click **Internal Posture Validation Setup**.

ACS displays a list of posture validation policies.

Step 2 Select a policy name from the list of posture validation policies.

The Posture Validation Rules page appears.

Step 3 Select a blue link in the Condition list on the Posture Validation Rules page.

Step 4 To delete the entire condition set, click **Delete**. Then click **Done**.

Step 5 To delete a selected condition component from the set, select a blue link in the Condition Sets list, then click **Delete**. Click **Submit** when you have deleted all condition components desired.

ACS deletes the condition set or condition component.

Step 6 Click **Done**.

Setting Up an External Policy Server

This procedure describes how you can create an external policy.

Before You Begin

You can select external policies for more than one profile. To create external policies, use the External Posture Validation Setup pages. To add the policy to a profile, use the Network Access Profiles page. See Setting Up a Profile, page 15-3.

The external server that you use to access the External Policy Validation page does not limit which profiles can select the new external policy.

For descriptions of the options available on the External Policy Configuration page, see External Policy Configuration Options, page 14-12.

Step 1 After selecting **External Posture Validation Setup**, the External Posture Validation Servers page displays.

Step 2 Click **Add Server**.

The Add/Edit External Posture Validation Server page appears.

Step 3 Name the server and provide a description if necessary.

Step 4 Provide addressing information for the primary and secondary servers.

a. Select the **Primary Server configuration** check box.

Note If you do not select the **Primary Server Configuration** check box, ACS uses the secondary server configuration. If no secondary server configuration exists or if the secondary server is unreachable, the posture validation request is rejected.

b. Provide configuration details about the primary NAC server. For more information about the boxes and list in this area, see External Policy Configuration Options, page 14-12.

Step 5 (Optional) In the **Secondary Server configuration** pane:

a. Select the **Secondary Server configuration** check box

b. Enter configuration details about the secondary NAC server. For more information about the boxes and list in this area, see External Policy Configuration Options, page 14-12.

Step 6 Determine credentials to forward to the primary or secondary external server by moving the available credentials to the selected credentials column.

Step 7 Click **Submit** to save your changes.

Step 8 Click **Apply and Restart** to submit your changes to ACS.

Editing an External Posture Validation Server

You can edit an external posture validation server by accessing it through the Posture Validation pages.

To edit an external posture validation server:

Step 1 In the navigation bar, click **Posture Validation**.

Step 2 Click **External Posture Validation Setup**.

Step 3 Click the server name that you want to edit.

The Add/Edit External Posture Validation Server page appears.

Step 4 Edit the fields and click **Submit**.

Deleting an External Posture Validation Server

You can remove an external posture validation server by accessing it through the Posture Validation pages.

To delete an external posture validation server:

Step 1 In the navigation bar, click **Posture Validation**.

Step 2 Click **External Posture Validation Setup**.

Step 3 Click the server name that you want to delete.

The Add/Edit External Posture Validation Server page appears.

Step 4 Click **Delete**.

Setting Up an External Audit Posture Validation Server

Use this page to create, modify, and delete external posture validation audit servers. Policies are reusable; you can associate an audit policy with more than one network access profiles.

Before You Begin

You must add your audit vendor to the ACS internal dictionary by using the **CSUtil** command before you can configure an external posture validation audit server. For detailed instructions, see Importing External Audit Posture-Validation Servers, page D-33.

To configure an audit server for external posture validation:

Step 1 After selecting **External Posture Validation Audit Setup**, the External Posture Validation Audit Server page appears.

Step 2 Click **Add Servers**.

The Edit External Posture Validation Audit Setup page appears.

Step 3 Enter a name for the audit policy.

Step 4 Select which hosts to audit. Select one of the following options from the drop-down list:

- **Audit all hosts**—Audit all hosts that do not contain a posture agent.
  - **Audit these hosts**—Audit only the hosts for which you have provided Host IP addresses and ranges (IP/Mask) or MAC addresses.
  - **Do not audit these hosts**—Exclude the hosts for which you have provided Host IP addresses and ranges (IP/Mask) or MAC addresses and audit all other hosts.
- **Select a Posture Token for the hosts that will not be audited**—Select a token from the drop-down list for hosts that are not audited.

Step 5 Select your audit server vendor, and provide addressing information and credentials for accessing a primary and if you require a failover, a secondary audit server.

Tip If your audit vendor does not appear, it does not have an audit APT defined in the internal ACS dictionary. To add an audit vendor, see Importing External Audit Posture-Validation Servers, page D-33

Step 6 Set directives for interpreting the various results and states that the audit server returns. The directives include:

- **Use this Posture Token while the Audit Server does not yet have a posture validation result**—Select a token from the drop-down list. The in progress token is used before the audit server determines the actual posture of the NAC agentless host.
- **Polling Intervals and Session-Timeout**—This option specifies polling intervals sent by the audit server and is enabled by default.
- **Maximum amount of times the Audit Server should be polled**—Select the maximum amount of times that ACS should query the audit server for a result (posture token).
- **Policy string sent to be sent to the Audit Server**—If the audit server supports named policy invocation, enter the name of policy.

Step 7 Click **Submit** to save your external posture validation audit server setup.

Editing an External Posture Validation Audit Server

You can edit an external posture validation audit server by accessing it through the Posture Validation pages.

To edit an external posture validation server:

Step 1 In the navigation bar, click **Posture Validation**.

Step 2 Click **External Posture Validation Audit Setup**.

Step 3 Click the server name that you want to edit.

The External Posture Validation Audit Server page appears.

Step 4 Edit the fields and click **Submit**.

Deleting an External Posture Validation Server

You can remove an external posture validation audit server by accessing it through the Posture Validation pages.

To delete an external posture validation audit server:

Step 1 In the navigation bar, click **Posture Validation**.

Step 2 Click **External Posture Validation Audit Setup**.

Step 3 Click the server name that you want to delete.

The External Posture Validation Audit Server page appears.

Step 4 Click **Delete**.

How Posture Validation Fits into Profile-Based Policies

In order to understand the profile-based policy paradigm, you should understand network access profiles. A profile is essentially a classification of network access requests for applying a common policy. Profile-based policies include rules for authentication, authorization, and posture validation.

Authorization rules are no longer set in Posture Validation but in the Network Access Profiles tab. Using authorization in NAP, you can provision the same RADIUS attribute to have different values for different users, groups and profiles. The one-user-one-group-one-profile is now more flexible, by using profile-based policies instead.

After configuring posture validation rules, you must associate those rules to a network access profile. For detailed instructions, see Setting a Posture-Validation Policy, page 15-37.

For more detailed information on policy-based profiles, see Overview of NAPs, page 15-1.

CHAPTER 15

Network Access Profiles

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, includes Network Access Profile (NAP) support. This chapter describes NAPs and contains the following topics:

- Overview of NAPs, page 15-1
- Profile-based Policies, page 15-2
- Configuring Profile-Based Policies, page 15-3
- Setting Up a Profile, page 15-3
- NAP Administrative Tasks, page 15-7
- Using Profile Templates, page 15-13
- Configuring Policies for Profiles, page 15-27
- Policy Replication and Backup, page 15-48

Overview of NAPs

A NAP, also known as a *profile*, is a means to classify access requests for each deployed network service, according to the Authentication, Authorization, and Accounting (AAA) clients' IP addresses, membership in a NDG, protocol types, or other specific Remote Access Dial-In User Service (RADIUS) attribute values sent by the network device through which the user connects.

Typical organizations have various kinds of users who access the network in different ways and for different purposes. Correspondingly, you must apply different security policies to the different use cases. For example, you might have to apply a tighter and more limiting security policy to the wireless access points of your building's lobby area, versus the physically secured production plant. Or, you might have to treat remote access users who use a virtual private network (VPN) differently from users that log in from behind a firewall. Users who connect through certain subnetworks might be authenticated differently from other users. Wireless access is often treated more strictly than wired access, as is any form of remote access (dial, VPN, home wireless).

A profile is essentially a classification of network-access requests for applying a common policy. One example of use of a profile is to aggregate all policies that should be activated for a certain location in the network. The policies will be selected every time an access request is initiated from that network location. Another method is to aggregate all policies that handle the same device type, for example, VPNs or Access Points (APs).

ACS traverses the ordered list of active profiles and maps a RADIUS transaction to a profile by using a first-match strategy on the first access request of the transaction. If no matching profile is found, ACS reverts to the global configuration settings.

You use profiles to classify access requests by defining filters on the access-request payload (the RADIUS attributes that are sent in an access request). Each profile is associated with a set of policies to be applied.

When a packet is received, ACS evaluates the profile filters to classify the packet. When a profile matches, ACS applies the configuration and policies that are associated with the profile during packet processing.

In their simplest form, you use NAPs to identify each of your network services (wireless LAN (WLAN), VPN, dial-up). On a per-service basis you can configure:

- Supported authentication protocols (Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Extensible Authentication Protocol (EAP)).
- Databases (ACS, Active Directory (AD), or others).
- How each type of service is provisioned (session keys, timeouts, access control lists (ACLs)).

Profile-based Policies

After you set up a profile, you associate a set of rules or policies with it to reflect your organization's security policies. These associations are called *profile-based policies.* Profile-based policies include rules for authentication, authorization, and posture validation.

By defining profile-based policies, can redirect authentication to different directories (for example, wireless users need to authenticate to AD while the same users who access the network through VPN might need to authenticate to an Rivest, Shamir, and Adelman (RSA) One-Time Password (OTP) directory).

To configure policies for a profile:

Step 1 Use the **Authentication** link to set policies based on password protocols or identity storage.

Step 2 Use the **Posture Validation** link to identify the kind of application that you expect to install.

Step 3 Use the **Authorization** link to design the network result for each combination of user and posture assessment that is used.

ACS associates attributes according to the profile that was requested. The attributes that are returned in an `Access-Accept` message are a consolidation of attributes that are associated with a profile (such as `Tunnel-Type` for a VPN profile request) and session-specific attributes that are bound to the end-user (such as `Idle-Timeout` for example). The profile mapping is independent of the user identity, therefore each user can use multiple profiles, and has only one entry in the validating database.

See Configuring Policies for Profiles, page 15-27, for a description on how to configure profile-based policies in detail.

Configuring Profile-Based Policies

To create profile-based policies:

Step 1 Identify the network services that you want to control by using ACS (for example, VPN, Dial, WLAN, `ip-admission`).

Step 2 Set up a profile for each network service. Setting up a profile defines how ACS will recognize or identify requests for example, device IP, NDG, NAF, advanced filtering). For more information, see Setting Up a Profile, page 15-3.

Step 3 Define the authentication protocols and external databases that are required for the service. For more information, see Configuring Authentication Policies, page 15-27.

Step 4 Define the posture-validation policies or rules (optional–if network admission control (NAC) is part of the deployment). See Configuring Posture-Validation Policies, page 15-35 for more information.

Step 5 Define per-service provisioning components (Shared RADIUS authorization components (RACs) and downloadable access control lists (DACLs)). If required for a given service, create custom RACs and DACLS for those groups of users that require specific settings.

Step 6 Define the authorization mappings from group to RAC and DACL. Also include the system posture token (SPT) if NAC is in use. For more information, see Configuring an Authorization Rule, page 15-44

Step 7 Check the Network Access Restriction (NAR) policies for the selected user group. Accept or reject will be applied, depending on the result of the NAR evaluation. For more information, see Network Access Restrictions, page 5-17.

If access is granted (`access-accept`) ACS merges between user, user-group RAC and ACLs, and provisions a result to the AAA client. For more information, see Merging Attributes, page 15-47.

Setting Up a Profile

This section describes how to configure network-access profiles. Profiles are associated with RADIUS attributes. Each profile has a unique name and can be active or inactive.

This section describes the following topics:

- Defining User Access Requests, page 15-4
- NAFs, page 15-4
- Protocol Types, page 15-5
- Advanced Filtering, page 15-5

Defining User Access Requests

You use the Profile Setup Page to define how ACS classifies access requests. You can use one or all of the following classification methods:

- NAFs
- Protocol Types
- Advanced Filtering

You use these three conditions to determine how ACS classifies an access request and maps it to a profile. The profile is selected when all the selected conditions match. For each condition, the value **Any** always matches the condition. For example, if you create a NAF for wireless and then select the Aironet Protocol type, only devices with the protocol types in the wireless NAF will be selected for filtering.

You create a profile from scratch, or you can use one of the supplied s to populate some default values. See Using Profile Templates, page 15-13, for more information. The templates that are provided are particularly useful for NAC-enabled networks.

NAFs

NAFs provide a flexible way of applying network-access restrictions, and downloadable ACLs on network device names, NDGs, or their IP addresses. NAFs that are applied by IP address can use IP address ranges and wildcards. NAFs introduce a granular application of NARs and downloadable ACLs, both of which previously supported only the use of the same access restrictions or ACLs to all devices. You can use NAFs to define flexible network device restriction policies, a requirement common in large environments.

NAFs are groupings of AAA client configurations (which might represent multiple network devices), NDGs, or IP addresses of specific AAA client devices. For more information, see About Network Access Filters, page 5-3.

You can use a NAF to group (and name) a disparate set of devices; for example: *these devices comprise the abc network service*.

You can also use NAFs to differentiate user requests on the same type of device. For example, while you undertake an IOS upgrade of Aironet wireless APs is undertaken (perhaps to enable some new encryption protocol) you might require a separate NAP for upgraded and nonupgraded APs.

Therefore, you can use NAFs with greater flexibility when you define which devices in a given network service or NAP.

Note If you want to aggregate NDGs and use them as a filter to assign users to a profile, you must configure NAFs before you set up a profile.

Protocol Types

You use Protocol Types to classify a user request based on the type of protocol that is used to request access to the network. Protocol Types are a subset of the vendor specific attributes (VSAs) that RADIUS supports.

Note The Terminal Access Controller Access Control System (TACACS+) protocol for NAPs is not supported in ACS Release 4.0.

You can select the AAA client vendor types from the access requests that are allowed. See AAA Client Configuration Options, page 4-8.

Advanced Filtering

You can use Advanced Filtering to create rules based on specific RADIUS attributes and values (including `Cisco-AV- pairs`). It is based on a Boolean AND expression of RADIUS attributes.

You can enter multiple `rule-elements`, which are treated as an AND Boolean expression. Operators **contains**, **start with**, and **regular expression** only apply to string-type attribute values.

Note ACS supports Cisco IOS RADIUS AV pairs. Before you select an AV pair, confirm that your AAA client supports it. If you enter an AV pair that the AAA client does not support, the condition will always fail.

Use the Rule Elements Table to specify the rule elements that comprises a rule based on a RADIUS attribute. For more information about rules, see About Rules, Rule Elements, and Attributes, page 14-10.

The components of the Rule Elements Table are:

- **Attribute**—Lists all RADIUS attributes that you can use to specify rules. A number uniquely identifies each RADIUS attribute; for example, 001 is the number for `User-Name`, except for vendor-specific attributes. Vendor Specific Attributes (VSAs) use the number 026 as an identifier. The format is:

  Cisco AV-pair 026 / <vendor type> / <vendor attribute>, for example, 026/009/001 is a Cisco AV-pair attribute.

- **Operator**—Defines the comparison method by which ACS evaluates whether the rule element is true. The operators that are available in the Operator list vary depending on the type of attribute selected from the Attribute list. In addition to common operators, such as the right angle bracket (>), the left angle bracket (<), and the equal sign (=), the Operator list supports a few special operators. For information about special operators, see About Rules, Rule Elements, and Attributes, page 15-6.
- **Value**—Specifies the value to which ACS compares the contents of the attribute.
- **AV-pair Key**—This option is enabled when you select the Cisco AV-pair attribute and ACS compares the contents of the AV-pair key attribute from the access request.
- **AV-pair Value**—This option is enabled when you select the Cisco AV-pair attribute and ACS compares the contents of the AV-pair value attribute from the access request.
- **Enter button**—Adds the rule element that is defined in the Attribute, Operator, and Value options to the Rule Elements Table.

About Rules, Rule Elements, and Attributes

A rule is a set of one or more rule elements. A rule element is a logical statement that contains:

- A RADIUS attribute
- An operator
- A value

ACS uses the operator to compare the contents of an attribute to the value. Each rule element of a rule must be true for the whole rule to be true. In other words, all rule elements of a rule are joined with a Boolean AND.

Note The {026/009/001Cisco AV-pair attribute field is unique. When it is selected, the AV-pair key and an AV-pair value are activated. Enter values for the two fields. For example, AV-pair key is the name of AV-pair attribute (aaa:service) and AV-pair value is the attribute contents to be compared to (for example. `ip-admission`).

Rule Operators

When you construct a rule in ACS, you can only select an operator that is applicable to the type of attribute that you select.

ACS supports these operators:

- **= (equal to)**—The rule element is true if the value in the attribute is exactly equal to the value that you specify.
- **!= (not equal to)**—Evaluates to FALSE when the input request does not contain an attribute.

Tip Use of the **!=** operator can lead to confusion, especially with Boolean attributes. For example, if a rule element for a Boolean attribute requires that the attribute is not equal to `false` and the attribute in a specific posture-validation request was 1, ACS would evaluate the rule element to be `true`. To avoid confusion, you can express the rule element more clearly by requiring that the attribute is equal to `true`.

- **> (greater than)**—The rule element is true if the value in the attribute is greater than the value that you specify.
- **< (less than)**—The rule element is true if the value in the attribute is less than the value that you specify.
- **<= (less than or equal to)**—The rule element is true if the value in the attribute is less than or equal to the value that you specify.
- **>= (greater than or equal to)**—The rule element is true if the value in the attribute is greater than or equal to the value that you specify.
- **contains**—The rule element is true if a substring of the string type attribute matches the string that you specify. For example, the **contains** operator and a value of `sc` would match an attribute that contains the string `Cisco`, the string `scsi`, or the string `disc`.
- **starts-with**—The rule element is true if the beginning of the attribute value matches the string that you specify. For example, the **starts-with** operator and a value of `Ci` would match an attribute that contains the string `Cisco` or the string `Ciena`.

- **regular-expression**—The rule element is true if the attribute matches the regular expression that you specify. ACS supports the following regular expression operators:
  - **^ (caret)**—The ^ operator matches the start of a string. For example `^Ci` would match the string `Cisco` or the string `Ciena` but not `docile`.
  - **$ (dollar)**—The $ operator matches the end of a string. For example, `co$` would match the string `Cisco` or the string `Tibco` but not the string `console`.

For more information about **RegEx** syntax, see Regular Expression Basic Syntax Reference, page 11-14.

Configuring Advanced Filtering

To configure advanced filtering:

Step 1 Select an **Attribute** from the drop-down list.

Step 2 Select an **Operator** from the drop-down list.

Step 3 Select an **Entity** from the drop-down list (optional for Linux packages).

Step 4 Enter a **Value** for the Attribute.

Step 5 Click **Enter**.

Note The Rule Elements Table is populated with conditions when you select a profile template. See Using Profile Templates, page 15-13.

NAP Administrative Tasks

This section describes the following tasks:

- Adding a Profile, page 15-7
- Ordering Profiles, page 15-9
- Editing a Profile, page 15-9
- Cloning a Profile, page 15-9
- Deleting a Profile, page 15-10
- Processing Unmatched User Requests, page 15-10
- NAP Administration Pages, page 15-11

Adding a Profile

On the Profile Setup page, you can configure:

- Name of the profile
- Description

- Activation flag (determines whether this profile is active or inactive)
- Clone an existing profile

The Network Access Profiles Page page is initially empty. Once populated, you must set the list of profiles into an order with a priority sequence from top to bottom.

Use the Profile Setup Page to configure the profile name, description, add the classification, and all other parameters that are required to set up the profile.

To add a profile:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles Page appears.

Step 2 Click **Add Profile**.

The Profile Setup Page appears.

Step 3 In the **Name** box, type the name of the new profile.

Step 4 In the **Description** box, type a description of the new profile.

Step 5 To enable the profile, check the **Active** check box.

Step 6 Set the configuration parameters for the profile:

a. Classify (filter), a user request by choosing a NAF from the list of existing NAFs. Configure NAF objects in Shared Profile Components. See About Network Access Filters, page 5-3.

b. Use Protocol Types to choose one or more protocol types as a filter. The Protocol Types are a subset of the VSAs that NAS supports. See AAA Client Configuration Options, page 4-8

c. Choose Advance Filtering to create a specific rule that contains one or more RADIUS attributes and values. See Configuring Advanced Filtering, page 15-7

Step 7 Click **Submit.**

The Network Access Profiles Page appears. The Network Access Profile's first match is implemented to authenticate or authorize a client request, or both.

Step 8 Click the radio buttons to change the order of the profiles. Click the **Up** or **Down** to move the profile to the correct position.

Note You also click the **Up** and **Down** buttons to submit the information to ACS.

Step 9 Select **Deny access when no profile selected,** when no profile matches the request. The default selection, Grant access using global configuration, when no profile matches, reverts to the global ACS configuration settings of authorizing by user-groups.

Step 10 Click **Apply and Restart** for your changes to take effect.

Ordering Profiles

Since ACS applies a first-match principle when trying to match an access request with a profile, the order of the profiles in the list is significant.

To set the order of the profile:

Step 1 In the Network Access Profiles Page, click the radio buttons to select a profile.

Step 2 Click the **Up** or **Down** to move the profile to the position you want.

Note Click **Apply and Restart** for your changes to take effect.

Editing a Profile

To edit the profile configuration:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles Page appears.

Step 2 Click the **Name** to modify the filtering methods for the profile.

The Profile Setup Page appears,

or

Select the configuration policy to edit. The relevant policy configuration page appears.

Step 3 To save your profile configuration settings, return to the Network Access Profiles Page and click **Apply and Restart.**

Cloning a Profile

Cloning replicates all the following relevant components for a NAP:

- **Authentication references**—External databases.
- **Posture references**—Internal or external posture validation, and external audit server. For more information about posture references, see Setting Up Posture Validation Policies, page 14-18.
- **Authorization references**—RACs and DACLs.

Cloning a NAP does not copy the shared-profile components, or the internal and external posture-validation policies, that the profile references. The newly cloned profile *references* the same shared-profile components as the original profile. For example, components that are referenced by name (RACs, DACLs, NAFs) remain the same.

When you clone a NAP, it is initially inactive by default. This inactive state avoids ambiguity when ACS tries to match an access request to a profile. After you modify the cloned profile, you can change the status to the active state.

The Profile description, Active Flag, Protocol Selection, Advanced Filter, Authentication, and Authorization policies are all cloned (copied). Posture-validation policies (Internal/External/Audit Servers) are not copied, but are referenced by the newly created Profile.

The naming pattern for cloning is **Copy-of-**. For multiple cloning (cloning the cloned element) the prefix **Copy-(2)-of-** is given.

If the new name length exceeds 32 characters, it is truncated to 32 characters.

To clone a profile:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles Page appears.

Step 2 Click the **Name**.

The Profile Setup Page appears.

Step 3 Click **Clone**.

Step 4 A copy of the cloned profile appears in the Network Access Profiles Page.

Step 5 Modify the cloned profile.

Step 6 Click **Apply and Restart** for your changes to take effect.

Deleting a Profile

To delete a profile:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles Page appears.

Step 2 Click the **Name**.

The Profile Setup Page appears.

Step 3 Click **Delete**.

Step 4 A warning message appears.

Step 5 Click **OK** to delete the profile configuration.

Step 6 Click **Apply and Restart** for your changes to take effect.

Processing Unmatched User Requests

ACS global configuration settings serve two purposes:

- Defining the fallback behavior for a request that does not match a profile.
- Defining the baseline for NAPs (if you want to enable a protocol in the NAP authentication page, you must first enable it in the Global Authentication Settings page).

Although legacy global settings and NAPs are supported and are interoperable, we do not recommend both of them, except for the case that is described in this section.

We recommend that you use the Deny access when no profile selected option whenever the access request cannot be classified it is rejected.

We recommend that you use to use **Grant access using global configuration** when no profile matches, since ACS will revert to the configuration settings in the Global Authentication Page. The Unknown User policy determine how to proceed with the packet processing.

The only case where ACS fallback behavior and NAPs should be used is with TACACS+. NAPs does not currently support TACACS+. Using Grant access using global configuration option is the only way to use TACACS+ and NAP configuration with RADIUS.

When you use both, you must ensure that the fallback behavior using global configuration will not create a security flaw in the network.

NAP Administration Pages

This section describes the fields in the web pages that you use for NAP administration:

- Network Access Profiles Page, page 15-11
- Profile Setup Page, page 15-12
- Advanced Filtering–Rule Elements Table, page 15-12

Network Access Profiles Page

Field	Description
Name	Click to activate the configuration for the profile. Opens the Profile Setup Page.
Policies	Contains links to set up authentication, posture validation, and authorization policies. Choose the appropriate link in this column to set the policy for the profile.
Authentication	Controls the profile's authentication policy. Opens the Authentication Settings Page where you can select which protocols are permitted and the database that is used to validate user credentials.
Posture Validation	Use to configure posture-validation policies. Opens the Posture Validation Page.
Authorization	Use to map between a user-group and system posture token result, to a radius-profile tag and Access Control List (ACL) name. Opens the Authorization Rules for Profile Page.
Deny access when no profile matches	When this option is enabled and the access request does not match any profile, authentication fails and the access request is denied. If this option is not enabled, ACS reverts to the global configuration settings of authorizing by user-groups.
Grant access using global configuration, when no profile matches	When this option is enabled and the access request does not match any profile, authentication fails and the access request is granted based on the default configuration.
Add Profile	Click to open the Profile Setup Page to configure NAPs.

Field	Description
Add Template Profile	Click to create a profile from a selection of templates. You can use the templates to facilitate the construction of a profile. Opens the Create Profile from Template Page.
Up/Down	Use to change the order of the profiles. Click the **Up** or **Down** buttons submit and save the sort order to the database.
Radio Button	Use to sort the order of profiles. Click to activate the profile to reorder.
Apply and Restart	Restarts ACS and applies the modifications.

Profile Setup Page

Field	Description
Name	Enter the profile name.
Description	Displays the profile description
Active	Displays the profile status.
Network Access Filter	Use to create a filter for configuring a profile. based on NAFs. The default for the NAF is **Any**.
Protocol Types	The Protocol Types are a subset of the VSAs that NAS supports. Click **Allow Any Protocol Type** to allow any protocol type or click **Allow Selected Protocol Types** to select protocols. Click the arrows to move the available Protocol Types to the Selected list. The default for the Protocol Types is **Allow Any**.
Advanced Filtering	Use to set rules for advanced filtering. See Advanced Filtering–Rule Elements Table, page 15-12. If you do not specify values for advanced filtering, the default is **Any**.
Submit	Click to submit your modifications. Returns you to the Network Access Profiles Page.
Clone	Click to clone and create a copy of the NAP. See Cloning a Profile, page 15-9 for more information.
Delete	Click to delete a profile. A warning message appears.
Cancel	Returns you to the Network Access Profiles Page without implementing any changes that you have made.

Advanced Filtering–Rule Elements Table

This table contains:

Field	Description
Attribute	Select the RADIUS Attribute from the drop-down list.

Operator	When you construct a rule for advanced filtering, in ACS you can only select an operator that is applicable to the type of attribute that you select. Operators include: • **=** (equal to)—The rule element is true if the value in the attribute is exactly equal to the value that you specify. • **!=** (not equal to)—The rule element is true if the value in the attribute does not equal to the value that you specify. • **contains** — The rule element is true if the attribute contains a string and if any part of that string matches the string that you specify. • **starts wit**h —The rule element is true if the attribute contains a string and if the beginning of that string matches the string that you specify. • **regular expression** — The rule element is true if the attribute contains a string and if the string matches the regular expression that you specify.
Value	Enter a value for the attribute.
Cisco-av-pair	When you select the {026/009/001} cisco-av-pair attribute, enter an operator and values for the av-pair-key and av-pair-value.

Using Profile Templates

You use a *profile template* to construct a new profile. Instead of setting up a new profile from scratch, you can select a profile from a predefined set of profile templates. The templates include a preconfigured set of NAC samples that you can use as the basis for building NAC policies. After you name the new profile and select a profile template, default values are populated into the Profile Setup page. You can then customize the profile settings to the specific needs of your security policy.

When you select a predefined template, ACS creates a full-scale NAP, including profile authentication, posture validation, and authorization policies.

The following templates are available for creating a profile:

- NAC L3 IP
- NAC L2 IP
- NAC Layer 2 802.1x
- Microsoft IEEE 802.1x
- Wireless (NAC L2 802.1x)
- Authentication Bypass (802.1x fallback)
- NAC Agentless Host (EAP over User Datagram Protocol (UDP) fallback)

Shared-profile Components

Each template references a set of shared-profile components. Before creating a template, ACS verifies that the appropriate shared-profile components exist. If the shared-profile components were not configured, ACS uses a set of shared-profile components that were created especially for the selected template.

Prerequisites for Using Profile Templates

Before you can use a profile template, you must configure:

- At least one AAA client by using the RADIUS Internet Engineering Task Force (IETF) protocol.
- Certificate setup.
- Administrator accounts (if needed).
- Logging settings.
- Global Authentication Setup for templates, depending on the template.
- User-Level or Group-Level Downloadable ACLs in the Interface Configuration > Advanced Options, depending on the template.

ACS rules are constructed from attributes that reside in the ACS dictionaries. During installation, the ACS posture dictionary is initialized to include attributes that belong to the `cisco:pa`. (It is mandatory that this default set of attributes be supported by every Cisco Trust Agent (CTA) implementation.)

The internal posture-validation polices that the templates create are based on these sets of attributes.

In ACS, each template that is created references a set of reusable objects. Before creating the template, ACS verifies that the relevant reusable objects already exist. If they do not, ACS automatically creates the required objects for the template. Creation of profiles from templates will not fail if these objects do not exist beforehand. If the reusable objects exist for the selected template, ACS uses the relevant reusable objects.

Note You cannot delete an attribute if it is being used in a posture-validation policy.

Selecting a Profile Template

To select a profile template:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles Page appears.

Step 2 Click **Add Template Profile**.

The Create Profile from Template Page appears.

Select a template from the drop-down list.

Step 3 Enter and **Name** and **Description** for the Profile.

Step 4 Check the **Active** check box to activate the profile.

Step 5 To save your profile configuration settings, return to the Network Access Profiles Page and click **Apply and Restart.**

Create Profile from Template Page

This page contains:

Field	Description
Name	Enter a name for the profile template.
Description	Enter a description for the template profile.
Template	Select one of the templates from the drop-down list.
Active	Check to activate the profile.

NAC L3 IP

This template is used for access requests from a LAN Port IP by using Layer 3 posture validation.

Before you use this template enable:

1. Allow Posture Validation in Global Authentication Setup.
2. Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) authenticated in-band PAC provisioning in Global Authentication Setup.
3. EAP-FAST MS-CHAPv2 in Global Authentication Setup.
4. EAP-FAST Generic Token Card (GTC) in Global Authentication Setup.

Downloadable ACLs

Downloadable per-user ACL support is available for Layer 3 network devices that support downloadable ACLs. These includes Cisco PIX security appliances, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that you can apply per user or per group. This feature complements NAC support by enabling the enforcement of the correct ACL policy. When used in conjunction with NAFs, you can apply downloadable ACLs can differently per device, allowing you to tailor ACLs uniquely per user or per access device.

To create Layer 3 NAC profile from a template:

Step 1 Choose **Network Access Profiles.**

Step 2 Choose **Add Template Profile**.

Step 3 Select **NAC L3 IP** from the template drop-down list.

Step 4 Enter and **Name** and **Description** for the Profile.

Step 5 Check the **Active** check box to activate the profile.

Step 6 Click **Submit**.

Table 15-1 describes the Profile Sample in the NAC Layer 3 IP Sample Profile Template.

Table 15-1 NAC Layer 3 IP Profile Sample

Section	Property		Value		
NAP	Name		User configurable		
	Description		User configurable		
Profile	NAF		N/A		
	Protocol		N/A		
	Advance filter		([[26/9/1]Cisco av-pair]aaa:service = ip-admission) AND ([006]Service-Type != 10)		
Authentication	Protected Extensible Authentication Protocol (PEAP)		Allow Posture Only is checked		
	Credential Validation Database		N/A		
Posture Validation	Posture Validation Rule	Name	NAC-EXAMPLE-POSTURE-EXAMPLE		
		Required credential types	Cisco:PA		
		Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
		Selected external posture policies	N/A		
		System Posture Token configuration	System Posture Token	PA message	URL Redirect
			Healthy	Healthy	N/A
			Checkup	Checkup	N/A
			Transition	Transition	N/A
			Quarantine	Quarantine	N/A
			Infected	Infected	N/A
			Unknown	Unknown	N/A

Table 15-2 Authorization Rules for NAC Layer 3 IP Profile Template

Authorization Rules	User Group	System Posture Token	Shared RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC-SAMPLE-HEALTHY-ACL
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC-SAMPLE-QUARANTINE-ACL
Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Table 15-3 describes the posture-validation policies in the NAC Layer 3 IP Sample Profile Template.

Table 15-3 Posture Validation for NAC Layer 3 IP Sample

Section	Object		Value		
Internal posture policy	NAC-SAMPLE-CTA-POLICY		Condition	System Posture Token	Notification String
		Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0	Cisco:PA:Healthy	N/A
		Default	N/A	Cisco:PA:Quarantine	N/A

Table 15-4 describes the Shared Profile Components in the NAC Layer 3 IP Sample Profile Template.

Table 15-4 Shared Profile Components for NAC Layer 3 IP Sample

Type	Object	Value		
RADIUS Authorization Components	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [26/9/1]cisc-av-pair status-query-timeout=300 [029] Termination-Action RADIUS-Request (1)		
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [26/9/1]cisc-av-pair status-query-timeout=30 [029] Termination-Action RADIUS-Request (1)		
Downloadable IP ACLs	NAC-SAMPLE-HEALTHY-ACL	ACL Content Name	Content	NAF
	NAC-SAMPLE-QUARANTINE-ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)

NAC L2 IP

Before you use this template, choose **Enable EAP Configuration > Allow Posture Validation in Global Authentication Setup**.

You can use NAC Layer 2 IP on an access port on an edge switch to which an endpoint system or client is connected. The device (host or client) can be a PC, a workstation, or a server that is connected to the switch access port through a direct connection, an IP phone, a hub, or a wireless access point.

When NAC Layer 2 IP is enabled, UDP only works with IPv4 traffic. The switch checks the antivirus condition of the endpoint devices or clients and enforces access-control policies.

Advanced Filtering and Authentication properties are filled out with NAC-L2-IP Configuration automatically.

Table 15-5 describes the content of the Profile in the NAC Layer 2 IP Sample Profile Template.

Table 15-5 NAC Layer 2 IP Profile Sample

Section	Property		Value		
NAP	Name		User configurable		
	Description		User configurable		
Profile	NAF		N/A		
	Protocol		N/A		
	Advance filter		([[26/9/1]Cisco av-pair]aaa:service = ip-admission) AND ([006]Service-Type != 10)		
Authentication	PEAP		Allow Posture Only is checked		
	Credential Validation Database		N/A		
Posture Validation	Posture Validation Rule	Name	NAC-EXAMPLE-POSTURE-EXAMPLE		
		Required credential types	Cisco:PA		
		Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
		Selected external posture policies	N/A		
		System Posture Token configuration	System Posture Token	PA message	URL Redirect
			Healthy	Healthy	N/A
			Checkup	Checkup	N/A
			Transition	Transition	N/A
			Quarantine	Quarantine	N/A
			Infected	Infected	N/A
			Unknown	Unknown	N/A

Table 15-6 describes the content of the Authorization Rules in the NAC Layer 2 IP Sample Profile Template.

Table 15-6 Authorization Rules for NAC Layer 2 IP Profile Template

Authorization Rules	User-Group	System Posture Token	RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC-SAMPLE-HEALTHY-ACL
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC-SAMPLE-QUARANTINE-ACL
Default			NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL

Table 15-6 Authorization Rules for NAC Layer 2 IP Profile Template (continued)

Authorization Rules	User-Group	System Posture Token	RAC	DACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Table 15-7 describes the content of the posture-validation policies in the NAC Layer 2 IP Sample Profile Template.

Table 15-7 Posture Validation for NAC Layer 2 IP Sample

Section	Object		Value		
Internal posture policy	NAC-SAMPLE-POSTURE-RULE		Condition	System Posture Token	Notification String
		Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0	Cisco:PA:Healthy	N/A
		Default	N/A	Cisco:PA:Quarantine	N/A

ACS and AV Pairs

When you enable NAC Layer 2 IP validation, ACS provides NAC AAA services by using RADIUS. ACS gets information about the antivirus credentials of the endpoint system and validates the antivirus condition of the endpoint.

You can set these Attribute-Value (AV) pairs on ACS by using the RADIUS cisco-av-pair vendor-specific attributes (VSAs).

- **Cisco Secure-Defined-ACL**—Specifies the names of the downloadable ACLs on the ACS. The switch gets the ACL name through the Cisco Secure-Defined-ACL AV pair in this format:

  #ACL#-IP-name-number

  where *name* is the ACL name and *number* is the version number, such as 3f783768.

The Auth-Proxy posture code checks if the access-control entries (ACEs) of the specified downloadable ACL were previously downloaded. If it was not, the Auth-Proxy posture code sends an AAA request with the downloadable ACL name as the username so that the ACEs are downloaded. The downloadable ACL is then created as a named ACL on the switch. This ACL has ACEs with a source address of **Any** and does not have an implicit **Deny** statement at the end. When the downloadable ACL is applied to an interface after posture validation is complete, the source address is changed from any to the host source IP address. The ACEs are prepended to the downloadable ACL that is applied to the switch interface to which the endpoint device is connected.

If traffic matches the Cisco Secure-Defined-ACL ACEs, the appropriate NAC actions are taken.

- **url redirect and url-redirect-acl**—Specifies the local URL policy on the switch. The switches use these cisco-av-pair VSAs:

  — *url-redirect = <HTTP or HTTPS URL>*

  — *url-redirect-acl = switch ACL name or number*

These AV pairs enable the switch to intercept an HyperText Transfer Protocol (HTTP) or Secure HyperText Transfer Protocol (HTTPS) request from the endpoint device and forward the client web browser to the specified redirect address from which the latest antivirus files can be downloaded. The url-redirect AV pair on the ACS contains the URL to which the web browser will be redirected. The url-redirect-acl AV pair contains the name or number of an ACL which specifies the HTTP or HTTPS traffic to be redirected. The ACL must be defined on the switch. Traffic which matches a permit entry in the redirect ACL will be redirected.

These AV pairs might be sent if the host's posture is not healthy.

For more information about AV pairs that Cisco IOS software supports, see the documentation about the software releases that run on the AAA clients.

Default ACLs

If you configure NAC Layer 2 IP validation on a switch port, you must also configure a default port ACL on a switch port. You should also apply the default ACL to IP traffic for hosts that have not completed posture validation.

If you configure the default ACL on the switch and the ACS sends a host access policy to the switch, the switch applies the policy to traffic from the host that is connected to a switch port. If the policy applies to the traffic, the switch forwards the traffic. If the policy does not apply, the switch applies the default ACL. However, if the switch gets a host access policy from the ACS, but the default ACL is not configured, the NAC Layer 2 IP configuration does not take effect.

When ACS sends the switch an downloadable ACL that specifies a redirect URL as a policy-map action, this ACL takes precedence over the default ACL that is already configured on the switch port. The default ACL also takes precedence over the policy that is already configured on the host. If the default port ACL is not configured on the switch, the switch can still apply the downloadable ACL from the ACS.

You use this template for access requests from Layer 2 devices that do not have the 802.1x client installed. Media Access Control (MAC) Authentication Bypass is used for access requests to bypass the nonclient authentication process. Users are mapped to a User Group based on their identity.

Note Do not use the Populate from Global button; otherwise: this authentication field will be inherited from the Global Authentication Setup in System Configuration.

NAC Layer 2 802.1x

Before you use this template enable:

1. EAP-FAST in Global Authentication Setup
2. EAP-FAST Authenticated in-band PAC Provisioning in Global Authentication Settings
3. EAP-FAST MS-CHAPv2 in Global Authentication Setup

4. EAP-FAST GTC in Global Authentication Setup

Table 15-8 describes the content of the NAC L2 802.1x Sample Profile Template.

Table 15-8 NAC L2 802.1x Profile Sample

Section	Property	Value		
NAP	Name	User configured		
	Description	User configured		
Profile	NAF	N/A		
	Protocol	N/A		
	Advance filter	([006]Service-Type != 10) and (not exist [26/9/1]cisco-av-pair aaa:service)		
Authentication	EAP-FAST	**Allow EAP-FAST** is checked. **Allow authenticated in-band PAC provisioning** is checked. **Allow inner methods EAP-GTC** is checked. **Allow inner methods EAP-MS-CHAPv2** is checked. **Allow Stateless Session Resume** is checked. **Accept client on authenticated provisioning** is checked. **Posture Validation required** is checked.		
	Credential Validation Database	ACS Internal user database		
Posture Validation				
Posture validation Rule	Name	NAC-SAMPLE-POSTURE-RULE		
	Required credential types	Cisco:PA		
	Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
	Selected external posture policies	N/A		
	System Posture Token configuration	System Posture Token	PA message	URL
		Healthy	Healthy	N/A
		Checkup	Checkup	N/A
		Transition	Transition	N/A
		Quarantine	Quarantine	N/A
		Infected	Infected	N/A
		Unknown	Unknown	N/A

Table 15-9 describes the content of the Authorization Rules in the NAC Layer 802.1x Sample Profile Template.

Table 15-9 Authorization Rules for NAC Layer 2 801.x Profile Sample

Authorization Rules	User group	System Posture Token	RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L2-RAC	N/A
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L2-RAC	N/A
Default			NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Table 15-10 describes the content of the posture-validation policies in the NAC Layer 802.1x Sample Profile Template.

Table 15-10 Posture Validation for NAC Layer 2 802.1x Profile Sample

Section	Object		Value		
Internal posture policy	NAC-SAMPLE-CTA-POLICY		Condition	System Posture Token	Notification String
		Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0	Cisco:PA:Healthy	N/A
		Default	N/A	Cisco:PA:Quarantine	N/A

Table 15-11 describes the content of the Shared Profile Components in the NAC Layer 802.1x Sample Profile Template.

Table 15-11 Shared Profile Components for NAC Layer 2 802.1x Profile Template

Type	Object	Value
RADIUS Authorization Components	NAC-SAMPLE-HEALTHY-L2-RAC	[027] Session-Timeout = 36,000 [26/9/1] cisco-av-pair sec:pg=healthy_hosts [029] Termination-Action RADIUS-Request (1) [064] Tunnel-Type [T1] VLAN (13) [065] Tunnel-Medium-Type [T1] 802 (6) [081] Tunnel-Private-Group-ID = healthy
	NAC-SAMPLE-QUARANTINE-L2-RAC	[027] Session-Timeout = 3,600 [26/9/1]cisco-av-pair sec:pg=quarantine_hosts [029] Termination-Action RADIUS-Request (1) [064] Tunnel-Type [T1] VLAN (13) [065] Tunnel-Medium-Type [T1] 802 (6) [081] Tunnel-Private-Group-ID = quarantine

Microsoft IEEE 802.1x

Before you use this template, choose **Enable EAP Configuration > Allow EAP-MS-CHAPv2** in the Global Authentication Setup page.

Table 15-12 describes the Profile Sample in the Microsoft IEEE 802.1x Sample Profile Template.

Table 15-12 Microsoft IEEE 802.1x Profile Sample

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	([006]Service-Type != 10) and (not exist [26/9/1]cisco-av-pair aaa:service)
Authentication	PEAP	Allow EAP MS-CHAPv2 is checked
	Credential Validation Database	ACS Internal Users Database
Posture Validation	N/A	

Table 15-13 describes the Authorization Rules in the Microsoft IEEE 802.1x Sample Profile Template.

Table 15-13 Authorization Rules for Microsoft IEEE 802.1x Profile Sample

Authorization Rules	User Group	System Posture Token	RAC	DACL
Default	Deny = unchecked			
Include RADIUS attributes from user's group	Checked			
Include RADIUS attributes from user record	Checked			

Wireless (NAC L2 802.1x)

The templates for wireless (NAC L2 802.1x) are the same as the NAC L2 802.1x templates. See NAC Layer 2 802.1x, page 15-20 for more information.

Authentication Bypass

You can use the profile template that ACS provides to create a profile that matches a RADIUS request that will come from a switch. Once the profile is created an analysis of the RADIUS packet that comes from the Catalyst 6500 must be done to create an accurate match for the profile. The RADIUS request from the switch has a Service Type value of 10, just like NAC-L2-IP; but does not have a Cisco Attribute Value Pair (AVP) that contains the keywords service. Therefore, two entries are created in the Advanced Filtering box.

Note MAC-Authentication-Bypass is only supported on the Cisco Catalyst 6500 Cat OS in this release.

Table 15-14 describes the content of the Profile Sample in the Authentication Bypass Sample Profile Template.

Table 15-14 Authentication Bypass Sample Profile

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	(not exist [26/9/1]cisco-av-pair aaa:service) AND ([006]Service-Type = 10)
	Credential Validation Database	N/A

Table 15-14 Authentication Bypass Sample Profile (continued)

Section	Property	Value
Authentication	Protocols	MAC authentication bypass will be checked Default user-group will be set to **default group**
Posture Validation	N/A	

Table 15-15 describes the content of the Authorization Rules in the Authentication Bypass Sample Profile Template.

Table 15-15 Authorization Rules for Authentication Bypass Sample Profile

Authorization Rules	User Group	System Posture Token	RAC	DACL
Rule 1	Default-group	N/A	NAC-SAMPLE-QUARANTINE-L2-RAC	N/A
Default	Deny = checked			
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

NAC Agentless Host

This template is used for access requests for NAC Agentless Hosts (NAH), also known as agentless hosts. These requests use EAP over UDP (EoU).

Table 15-16 describes the Profile Sample in the NAH Sample Profile Template.

Table 15-16 NAH Sample Profile Template

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	([[26/9/1]Cisco av-pair]aaa:service = ip-admission) AND ([006]Service-Type = 10)
	Credential Validation Database	N/A
Posture Validation	N/A	

Table 15-16 NAH Sample Profile Template (continued)

Section	Property	Value			
Authorization	Rules	User-group	System Posture Token	RAC	DACL
		N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL
		N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
		N/A	Transition	NAC-SAMPLE-TRANSITION-L3-RAC	NAC_SAMPLE_TRANSITION_ACL
	Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
	Include RADIUS attributes from user's group	Unchecked			
	Include RADIUS attributes from user record	Unchecked			

Table 15-17 describes the Shared Profile Components in the NAH Sample Profile Template.

Table 15-17 Shared Profile Components for NAH Sample

Type	Object	Value
RADIUS Authorization Components	NAC-SAMPLE-TRANSITION-L3-RAC	[027] Session-Timeout = 60 [029] Termination-Action RADIUS-Request (1) A Session-Timeout can be overwritten if hinted by an audit server
	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [029] Termination-Action RADIUS-Request (1)
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [029] Termination-Action RADIUS-Request (1)

Table 15-17 Shared Profile Components for NAH Sample (continued)

Downloadable IP ACLs		ACL Content Name	Content	NAF
	NAC-_SAMPLE-_TRANSITION-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_HEALTHY-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC_-SAMPLE-_QUARANTINE-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)

Configuring Policies for Profiles

After you set up a profile, you associate a set of rules or policies with it, to reflect your organization's security policies. These associations are called profile-based policies. Configuration of a profile-based policy includes the creation of rules for:

- **Authentication**—A set of configuration policies that are related to authentication mechanisms.
- **Posture validation**—Define the manner in which posture validation will be performed (only if you plan to deploy NAC in your network).
- **Authorization**—Configure a set of authorization rules (optional).

A profile acts as a way to segment network access-requests and apply a common policy to those user requests.

Configuration of profile-based policies includes:

1. Configuring Authentication Policies, page 15-27
2. Configuring Posture-Validation Policies, page 15-35
3. Configuring Authorization Policies, page 15-43

Configuring Authentication Policies

Before you configure authentication policies:

- Set up the authentication protocols in the System Configuration section by using the Global Authentication Setup option. For more information, see Global Authentication Setup Page, page 10-20.

  Note We recommend that you check all authentication protocols in the Global Authentication Setup for NAC.

- Configure the External User Databases that you mapped to ACS user groups by the mapping rules that are defined in Database Group Mapping.

  Note The ACS internal database is the default selected database.

Authentication settings define what types of authentication protocols are allowed, the configuration for these protocols, and which databases are used to validate the credentials of the user for authentication. The authentication protocols are listed from weakest to most secure. The protocols that you select determine the flexibility of negotiation. The final result is to determine which protocol to use to authenticate.

Note For simple posture validation, you must check the **Allow Posture Validation** check box in the EAP Configuration section.

Populate from Global

You can populate the authenticating settings with the ACS global settings, and can then be customized. This method facilitates configuring the authentication settings each time you set up a new profile.

You should first configure the Global Authentication Setup, which serves as a central location for all of the EAP configuration settings in the active or inactive profiles.

EAP types, which are disabled in the Global Authentication Page, cannot be enabled in any of the ACS profiles. Every EAP type that is unchecked in the Global Authentication Page, will be automatically unchecked in all ACS (active and inactive) profiles.

To apply global settings:

Click **Populate from Global** to apply authentication settings that were set in the **System Configuration > Global Authentication Setup** window.

Authentication Protocols

You can configure all relevant parameters for authentication in the Authentication Settings Page. These parameters are applied during access request processing.

The following authentication protocols can be configured in the Authentication Settings Page:

- RADIUS Authentication protocols:
  - An option to allow or disallow authentication by using Password Authentication Protocol (PAP) protocol.
  - An option to allow or disallow authentication by using CHAP password protocol.
  - An option to allow or disallow authentication by using MS-CHAPv1 password protocol.
  - An option to allow or disallow authentication by using MS-CHAPv2 password protocol.
  - An option to allow or disallow authentication by using MAC-Authentication Bypass. For more information, see MAC-Authentication Bypass, page 15-29.

An option to allow or disallow a set of EAP types (outer and inner) to be used for EAP authentication, including the relevant setting for each EAP-type. See EAP Configuration, page 15-29, for more information.

- You can configure the following EAP protocols:
  - PEAP
  - EAP-FAST
  - EAP-Transport Layer Security (TLS)
  - EAP-Message Digest 5 (MD5)

- An ordered list of external database instances that you can use for authentication and user-group mapping.

If the password protocol is not enabled, then ACS rejects the access request.

If ACS and a client do not share any commonly enabled EAP-Type, then ACS rejects the access request.

When authentication is requested, ACS uses the ordered list of external databases that are defined for a specific profile.

MAC-Authentication Bypass

MAC Authentication Bypass is an identity-based network security feature that is configured on a port basis. A switch makes a RADIUS request to ACS with the MAC address of the endhost connecting to the switch. MAC authentication happens on the switch or device as a fallback that results from a 802.1x failure or an EAPoUDP failure, and hence bypasses these mechanisms. This feature is useful for allowing network access for hosts without 802.1x or EAPoUDP support. For example, devices such as printers or terminals that do not have an 802.1x client can use this feature to access to the network.

You can use this feature to map MAC addresses to user groups. If the list of defined addresses does not contain a MAC address, you can associate a fallback user group with the access request. Groups can be included in the profile's authorization policy and then be evaluated for network admission based on authorization rules.

The MAC address is sent in the Calling-Station-ID RADIUS attribute. The following defines how ACS identifies a **mac-authentication** request:

Service-Type = 10 (Call Check)

If the MAC-Authentication Bypass option is not selected, MAC authentication is not applied and the access request is rejected.

For more information on how to configure MAC Authentication Bypass, see Configuring MAC Authentication Bypass, page 15-31.

EAP Configuration

EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x, or RADIUS and supports multiple authentication types:

- PEAP (Protected EAP)
- EAP-FAST
- EAP-TLS (based on X.509 certificates)
- EAP-MD5: Plain Password Hash (CHAP over EAP)
- EAP-GTC: OTP Tokens

New extended EAP methods have been added to EAP for NAC:

- EAP-TLV: Carry posture credentials, adding posture AVPs, posture notifications.
- Status Query: You can use this new EAP method for securely querying the status of a peer without a full credential validation.
- EAPoUDP: use of EAP over UDP for Layer 3 transport.

Note LEAP (EAP-Cisco Wireless) is not supported when working with Network Access Profiles.

EAP-FAST

EAP-FAST 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

You can set the following inner methods for EAP- FAST;

- EAP-GTC: OTP Tokens
- EAP MS-CHAPv2
- EAP-TLS

Posture Validation Settings

Several organizations might be transitional to supply their hosts with CTA and some hosts might or might not have CTA installed. Cases might arise where you might want to enforce posture validation on machines with CTA; however, you do not want to fail authentication on those machines that are temporarily without CTA. When EAP-FAST is enabled with Required Posture Validation, you can select the Optional selection and supply a resulting SPT. You can use the SPT that is set here for setting Authorization settings. For a description of the tokens that are used in ACS, see Posture Tokens, page 14-3.

Note If posture-validation rules are not defined, the posture token returned is **Unknown**.

Credential Validation Databases

The Credential Validation Databases are databases that you use to validate users. The Available Databases are the configured External User Databases that are mapped to ACS user groups by the mapping rules defined in Databases Group Mapping. The ACS internal database appears, by default, as a selected database.

Note If you specify multiple databases for authentication, ACS will query each directory server in the order specified until it receives an authoritative response. You should put the most likely directory servers higher in the list to improve response times and user experience.

Setting Authentication Policies

To set authentication policies:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the relevant Authentication policy.

The Authentication Settings Page appears.

Step 3 Select **Populate from Global** to populate authentication settings from the ACS Global Authentication Settings. For more information, see Global Authentication Setup, page 10-19.

If you are not using the Global Authentication Setup settings:

Step 4 Configure the **Authentication Protocols** for the profile.

Step 5 Select the **EAP Configuration.** See EAP Configuration, page 15-29.

Step 6 Select the **EAP-FAST Configuration**. See EAP-FAST, page 15-30

Step 7 Select the **Credential Validation Databases.** See Credential Validation Databases, page 15-30.

Step 8 Click **Submit**.

The Network Access Profiles Page appears.

Step 9 Click **Apply and Restart** for your changes to take effect.

Configuring MAC Authentication Bypass

To configure the MAC authentication bypass:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the relevant Authentication policy.

Step 3 In the Authentication Settings Page, enable **Allow MAC-Authentication-Bypass**.

Step 4 Click **Submit**.

The Network Access Profiles Page appears.

Step 5 Choose the relevant Authentication policy.

Step 6 Select the **MAC Authentication Bypass Configuration** link.

The MAC Authentication Mapping Page appears.

Step 7 Click **Add**.

Step 8 Enter the **MAC Addresses** for the access requests that you want to group.

Step 9 Select a **User Group** from the drop-down list.

Step 10 Continue Adding MAC addresses and mappings to the list. (optional)

Step 11 Define the default mapping for MAC addresses that do not match by selecting a group from the drop-down list.

Step 12 Click **Submit.**

The Network Access Profiles Page appears.

Step 13 Click **Apply and Restart** for your changes to take effect.

Note Each NAP can hold up to 10,000 MAC addresses in the MAB page. Each NAP can hold up to 100 mappings (a map between list of one or more MAC addresses to a group), meaning you can have up to 100 lines of mappings from lists of MACs to user-groups. You can map up to 10,000 MAC Addresses to the same user-group in one NAP.

Authentication Settings Page

The Authentication Settings page contains:

Field	Description
Populate from Global	Use this option to populate the Authentication Settings with the ACS global Authentication settings. This method facilitates configuration of the authentication settings each time you set up a new profile.
Authentication Protocols	Select from PAP, CHAP, MS-CHAPv1,MS-CHAPv2
Allow PAP	Select to enable PAP. PAP uses clear-text passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	Select to enable CHAP. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with the Windows user database.
Allow MS-CHAPv1	Select to enable MS-CHAPv1.
Allow MS-CHAPv2	Select to enable MS-CHAPv2
Allow MAC-Authentication Bypass	Enable to configure the authentication process for a profile that receives a MAC address request.
MAC Authentication Bypass Configuration	Opens the MAC Authentication Mapping Page, page 15-34
EAP Configuration	Note: PEAP is a certificate-based authentication protocol. Authentication can occur only after you have completed the required steps on the ACS Certificate Setup page. Select he PEAP types. In most cases, all three boxes should be checked. When none is selected, PEAP will not be allowed for authentication.
Allow EAP-GTC (Cisco PEAP)	Select to enable EAP-GTC within PEAP authentication. Use for RSA Secure ID authentication.
Allow EAP-MS-CHAPv2 (MS PEAP)	Select to enable EAP-MS-CHAPv2 within PEAP authentication. Use for AD authentication.
Allow Posture validation	Select to enable the collection of posture data when using PEAP. This options uses EAP over UDP. **Note** This EAP configuration must be checked to use the Layer 3 NAC Profile Template.
Allow EAP-FAST	Select to enable EAP-FAST authentication, All other EAP-FAST-related options are irrelevant if unchecked. Some of the following settings must have corresponding settings on the PC based authentication agent (the EAP-FAST client).
Allow anonymous in-band PAC provisioning	If this check box is checked, ACS establishes a secure anonymous TLS handshake with the client to provision it with a so-called PAC by using phase zero of EAP-FAST, and using EAP-MS-CHAP as the inner method.

Field	Description
Allow authenticated in-band PAC provisioning	ACS uses secure sockets 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 are installed on ACS.
Accept client on authenticated provisioning	This option is only available when the Allow authenticated in-band PAC provisioning option is selected. This option should be checked to slightly shorten the protocol.
Require client certificate for provisioning	Select this option if the clients are configured with public key infrastructure' (PKI) certificates, which will be used to provision PACs
Allow Stateless session resume	Should normally be checked. Uncheck if you do not want ACS to provision authorization PACs for EAP-FAST clients, and always perform phase 2 of EAP-FAST.
Authorization PAC TTL minutes hours	You can use this setting to determine the expiration time of the user authorization PAC. When ACS receives an expired authorization PAC, it performs phase 2 EAP-FAST authentication. Enter a time in minutes or hours.
Allowed inner methods	These options determine which inner EAP methods run inside the EAP-FAST tunnel. For anonymous in-band provisioning, EAP-GTC and EAP-MS-CHAPv2 must be enabled for backward compatibility. In most cases, all the inner methods should be checked. **Note** ACS always starts the authentication process by using the first enabled EAP method. For example, if you select EAP-GTC and EAP-MS-CHAPv2, then the first enabled EAP method is EAP-GTC. ACS always runs the first enabled EAP method. For example, if you select EAP-GTC and EAP-MS-CHAPv2, then the first enabled EAP method is EAP-GTC.
EAP-GTC	This option uses a two-factor authentication; for example, OTP.
EAP-MS-CHAPv2	This option is used for AD authentication.
EAP-TLS	This option uses certificates for authentication.

Field	Description
Posture Validation	Determines the EAP-FAST posture-validation mode. Select one of the following posture-validation modes: • **None**—Authentication is performed; however, no posture-validation data is requested from the client and no SPT is returned. • **Required**—Authentication and posture validation are performed in the same authentication session. As a result, an SPT is returned. If this option is selected and posture credentials that are requested from the client are not received, authentication fails. If you are implementing NAC, this option should be enabled. • **Optional**—Client may not supply posture data. Sets a default SPT when a client cannot supply posture data to ACS. • **Use Token**—Select an SPT from the drop-down list to use as the default posture token. • **Posture Only**—Perform posture validation without running authentication inner methods within the authentication session. This option returns an SPT for posture validation.
EAP-TLS	Check this check box to enable EAP-TLS authentication. Note: EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.
EAP-MD5	Select to enable EAP-based Message Digest 5 hashed authentication.
Credential Validation Databases	Select the databases that you want to use to validate users. Select from the Available Databases list and use the arrows to move them into the Selected Databases list.

MAC Authentication Mapping Page

The MAC Authentication Mapping page contains:

Field	Description
MAC Addresses	Enter the MAC Addresses to map to a user group. These values should be comma-separated values. Two MAC address formats are accepted: **00-0D-60-FB-16-D3** or **000D.60FB.16D3**. MAC prefixes that serve as ranges are acceptable. For example, **00-0D-60-FB-16** or **000D.60** would match any MAC address that begins with these bytes. MAC prefixes must contain an even number of hexadecimal digits. MAC address matching is case sensitive.
User-Group	Select the group from the ACS-defined groups to which to apply the MAC Authentication policy.

Field	Description
If a MAC address is not defined or there is no matched mapping.	If the MAC addresses entered in the provided fields do not match any of the MAC addresses entered, select a group to which to assign the MAC address.
Add	Adds a MAC Address mapping field.
Delete	Deletes a MAC Address mapping field.
Submit	Click to submit your changes to the ACS database.
Cancel	Returns you to the Network Access Profiles Page.

Configuring Posture-Validation Policies

Use the Posture Validation Page to configure and delete posture-validation rules. Posture-validation rules define the way that ACS performs posture validation.

Each rule comprises a condition and actions. The condition contains a set of required credential types; while the action contains a list of internal posture-validation policies or external posture-validation servers that you can use for posture validation, or both. See Chapter 14, "Network Access Control Overview," for more information.

ACS interprets a posture-validation rule as:

If posture credentials contain data that was sent from the following plug-ins <required credential types>, then perform posture validation by using the following internal, external, or both internal and external posture validation methods <list of internal policies and external servers>.

ACS applies all the policies that associated with the selected posture-validation rule to derive application posture tokens (APT), which represent the state of the client (also known as the endpoint). ACS compares all derived APTs and uses the worst case posture token as the SPT, which symbolizes the overall posture of the client.

Audit servers are Cisco and third-party servers that determine posture information about a client without relying on the presence of a NAC-compliant Posture Agent (PA). These types of clients are also referred to as NAC Agentless Hosts (NAH). Audit servers are used to assess posture validation with an organization's security policy. For more information, see Setting a Posture-Validation Policy, page 15-37.

The Cisco PA is also known as the Cisco Trust Agent (CTA).

Each rule contains:

- Name (posture-validation policy) for identification.
- Required credential types that define the credential types that activate this rule.
- Internal policies and external servers that execute to calculate the posture token.
- Posture Agent (PA) messages that return to the client for each SPT.
- URL redirect that is sent to the AAA client for each SPT.

Note ACS supports up to 100 rules per policy.

The posture rules are evaluated in a first-match strategy. A posture-validation policy can have zero or more ordered posture-validation rules and is selected by using the first rule that matches.

This section contains the following information about configuring posture-validation policies:

- URL Redirect Policy, page 15-36
- Import Vendor Attribute-Value Pairs (AVPs), page 15-36
- Setting a Posture-Validation Policy, page 15-37
- Deleting a Posture Validation Rule, page 15-40
- Audit Server Functionality, page 15-40
- System Posture Token Configuration, page 15-40
- Mapping an Audit Server to a Profile, page 15-40
- Posture Validation for Agentless Hosts, page 15-41
- Configuring Fail Open, page 15-41
- Runtime Behavior, page 15-43

URL Redirect Policy

The URL Redirect policy provides a mechanism to redirect all HTTP or HTTPS traffic to a remediation server that allows a noncompliant host to perform the necessary upgrade actions to become compliant. The policy comprises:

- A URL that points to the remediation server.
- An ACL on the switch that causes all HTTP or HTTPS packets from the host other than those destined to the remediation server address to be captured and redirected to the switch software for the necessary HTTP redirection.

The ACL name for the host policy, the redirect URL and the URL redirect ACL are conveyed by using RADIUS Attribute-Value objects.

Import Vendor Attribute-Value Pairs (AVPs)

ACS does not include any non-Cisco attributes by default. Therefore, you must import a NAC Attribute Definition File (ADF) from each vendor application that you would like to validate in your NAC posture-validation policies. The attributes that are added can be used to create conditions for internal policies.

NAC introduces the ability to authorize network hosts not only based upon user or machine identity; but also upon a host's posture validation. The posture validation is determined by comparing the host's credentials to a posture-validation policy which you create from attribute-value pairs (AVPs), which are defined by Cisco and other vendors who are NAC partners. Since the range of NAC attributes extends across many vendors and applications, you must import the non-Cisco attributes.

To import a NAC attribute definition file:

Step 1 Obtain one or more ADFs for the NAC-compatible applications that you want to validate with ACS.

Step 2 Place the ADFs in the same directory as the ACS utility, **CSUtil.exe** <*ACS Install Dir\bin*>, or a directory that is accessible by **CSUtil.exe**.

Step 3 On the host that is running ACS, open a **cmd** command prompt and navigate to the directory that contains `CSUtil.exe`.

Step 4 Add the AVPs to ACS by using the command:

CSUtil.exe -addAVP ***filename.adf***

For details on CSUtil, see CSUtil Command Syntax, page D-2.

Step 5 After successfully adding the AVPs, restart CSAdmin, CSLog, and CSAuth.

Setting a Posture-Validation Policy

A posture-validation policy can have one or more posture-validation rules. When ACS uses a posture-validation policy to evaluate a posture-validation request, the first match is implemented. The selected rules determines which internal and external policies will be activated for the request.

You can configure posture-validation policies that might be associated with a rule in Internal or External Posture Validation Setup, as applicable.

To add an internal posture-validation policy, external posture-validation server, or both, to a profile:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose **Posture Validation** for the selected profile.

Step 3 The Posture Validation page appears. See Posture Validation Page, page 15-38.

Step 4 Click **Add Rule**. The Posture Validation Rule Page appears, see Posture Validation Rule Page, page 15-39.

Step 5 Enter a Name for the rule.

Step 6 Choose the **Required Credential Types**.

Use the arrows to move the Required Credential Types from the from the **Available Credentials** to the **Selected Credentials**.

Step 7 Check the appropriate check boxes to enable Internal Posture Validation Policies and External Posture Validation Servers.

Step 8 Use the **System Posture Token Configuration** Table to set PA Messages and URL Redirects for the System Posture Token. (optional)

Step 9 Click **Submit**.

Step 10 In the Posture Validation Page click **Done**.

The Network Access Profiles Page appears.

Step 11 Select **Apply and Restart** for your changes to take effect.

Step 12 Click **Cancel** to return to the posture-validation policy.

Posture Validation Page

Use this page to add or modify a posture-validation rule.

Field	Description
Rule Name	Displays the name for the posture-validation rule. Highlight the name to modify the rule.
Required Credential Types	A posture-validation rule can have one or more required credential types. ACS determines whether to use the rule to evaluate a posture-validation request by comparing the credentials that it received in the request to the required credential types that are associated with the rule. If the request includes each of the credential types specified, ACS uses the rule to evaluate the request. If the required credentials do not match, ACS successively tries to match the next sequential rule. If no rule matches, the user request fails and access is denied. Required Credential Types are those that appear in the Selected Credentials list. Use the left and right arrow buttons to move highlighted credentials from one list to the other. The lists are: • The Available Credentials list displays the credential types that ACS does not require in a posture-validation request in order to use this posture-validation rule to evaluate the posture-validation request. • The Selected Credentials list displays the credential types that ACS does require in a posture-validation request in order to use this posture-validation rule to evaluate the posture-validation request.
Associate With	A posture-validation policy can have one or more posture-validation rules that are associated with it. When ACS evaluates a posture-validation request, it applies each of the internal policies and external server's policies that are associated with the rule to the attributes that are received in the request. The policies that are associated with a rule are selected in the Posture Validation Rule configuration page.
Up/Down	Click the radio button to select the rule you want to reorder. Click the **Up** and **Down** buttons to set the order.
Add Rule	Opens the Posture Validation Rule Page on which you create a new posture-validation rule.
Select Audit	NAC-compliant AAA clients can handle NAC for computers that do not respond to attempts to start a posture-validation session with CTA by querying an audit server. If CTA is not installed on the computer or is unreachable for other reasons, NAC-compliant AAA clients will attempt to perform posture validation on an audit server. The result returned by an audit server is a posture token. Posture-validation policies for external audit servers that may be associated with a rule are configured in Posture Validation External Posture Validation Audit Setup.

Posture Validation Rule Page

This page contains:

Field	Description
Rule Name	Displays the rule name for identification.
Add Rule	Click to add a posture-validation rule. The Posture Validation Rule configuration page appears.
Edit Rule	Highlight the Rule Name. The Posture Validation Rule configuration page for the specific profile appears for editing.
Action	
Select Internal Posture Validation Policies	See Chapter 14, "Posture Validation" for more information.
Select External Posture Validation Server	See Chapter 14, "Posture Validation" for more information.
Failure Action	Check to configure the Fail Open feature.
Failure Posture Token	Select the credential type (AV pair) that is returned to the supplicant. Select the Posture Token for the credential type.
System Posture Token Configuration	User this table to configure the SPT to return to the AAA client. There are six predefined, nonconfigurable SPTs. The SPT results are listed in order from best to worst.
System Posture Token	Enter a Posture Agent Message and URL Redirect for each posture token that you use.
PA Message	Enter a message that will appear for each posture agent. • **Healthy**–Host is compliant; no restrictions on network access. • **Checkup**–Host is within policy but an update is available. Used to proactively remediate a host to the Healthy state. • **Transition**–Host posturing is in process; give interim access pending full posture validation. Applicable during host boot when all services might not be running or audits are not yet available. • **Quarantine**–Host is out of compliance; restrict network access to a quarantined network for remediation. The host is not an active threat; but is vulnerable to a known attack or infection. • **Infected**–Host is an active threat to other endpoint devices; network access should be severely restricted or totally denied all network access. • **Unknown**–Host posture cannot be determined. Quarantine the host, and audit or remediate until a definitive posture can be determined.
URL Redirect-	Enter the URL redirect that will be sent to the AAA client for each posture token.

Deleting a Posture Validation Rule

To delete an internal posture-validation policy rule:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the Posture Validation for the selected profile.

Step 3 The Posture Validation Page appears.

Step 4 Click on **Rule Name**. The Posture Validation Rule Page appears.

Step 5 Click Delete.

A warning message appears.

Step 6 Click **OK**.

Audit Server Functionality

The audit server scans the host and returns the token to ACS.

The audit server may use asynchronous port scans, HTTP redirection, a proprietary client, and table lookups to provide posture-validation information.

ACS polls for the audit result, so the audit server must hold its results until the next poll.

System Posture Token Configuration

A system posture token is associated with the state of the computer and a posture token is associated with the state of a NAC-compliant application.

Actions are the result of applying a policy to the credentials received in a posture-validation request. ACS determines the posture token of each request by comparing the actions from all policies applied to the request. The worst posture token becomes the system posture token.

Mapping an Audit Server to a Profile

To add an external posture validation audit server to a profile:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose **Posture Validation** for the relevant profile.

Step 3 Click **Select Audit**.

Step 4 Select the relevant audit server.

Step 5 Click **Submit.**

Step 6 Click **Back** for the posture-validation policy.

Step 7 Select **Apply and Restart** for your changes to take effect.

Posture Validation for Agentless Hosts

Posture-validation rules define what the returned posture token for posture validation will be. The posture-validation table includes posture-validation rules and audit configuration settings.

Posture-validation rules contain:

- A required credential that defines the mandatory credential types that activate the rule.
- The local policies and external servers that will execute to calculate the posture token.
- PA (posture agent) Messages that will return to the client for each posture token.
- A URL redirect that will be sent to the AAA client for each posture token.

A posture-validation policy can have 0-*n* ordered posture rules.

The posture validation selected is the first that match of the mandatory credential types.

The posture token that will return is the worst assessment that returned from the selected local policies and external posture servers.

If the client is an agentless host, the selected Audit server will audit the client.

Configuring Fail Open

You can configure fail open for errors that can prevent the retrieval of posture token from an upstream NAC server. If fail open is not configured, the user request is rejected.

You can select whether to enable fail open for:

- Audit Server—for profiles that are associated with an audit server
- External Posture Validation Server—for profiles that are associated with an External Posture Validation Server

If you enable fail open, you will need to select the posture token to be granted when an error occurs in the initial authentication.

To configure fail open for an audit server:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose **Posture Validation** for the selected profile.

The Posture Validation Page appears.

Step 3 Choose **Select Audit**.

The Select External Posture Validation Audit for Profile Page appears.

Step 4 To enable fail open, check the **Do Not reject when Audit failed** check box.

Step 5 Select the posture token to be used in the event of a failure.

Step 6 Enter a value for session-timeout for the audit server.

Step 7 Click **Submit**.

To configure fail open for an external posture validation server:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose **Posture Validation** for the selected profile.

The Posture Validation Page appears.

Step 3 Select the **Rule Name.** To configure a rule, see Configuring Posture-Validation Policies, page 15-35.

Step 4 On the Posture Validation Rule for Profile page, check the check box in the Select column for the external posture validation server that you want to configure.

Step 5 Do one of the following:

- Check **Reject User** to deny access for fail open.
- In the Failure Posture Assessment field, select:
  - **Credential Type**—The namespace for the APT which replaces the APT that should have been returned from the failed server.
  - **Posture Token**—The posture token to be used in the event of a failure.

Step 6 Click **Submit**.

Select External Posture Validation Audit for Profile Page

This page contains:

Field	Description
Select	Click the radio button to select the external posture-validation audit server. Click **Do Not Use Audit Server** radio button if you do not want to use an audit server for posture validation.
Fail Open Configuration	Configure this option for any errors that might occur that prevent the retrieval of posture token from an upstream NAC server. If fail open is not configured, the user request is rejected.
Do not reject when Audit failed	Check this check box to enable fail open. The default is checked.
Use this token when unable to retrieve posture data	Select a token from the drop-down list.
Timeout	Set the timeout for the session granted.

Runtime Behavior

When fail open is configured, and an error occurs when communicating with an upstream posture-validation server, the policy results will be as if posture validation was successful. The SPT for the given policy will be a static, preconfigured value.

For an audit server, the configuration of fail open results in the SPT being set to the statically configured posture token. For External Posture Validation Servers, if more than one server is configured for a profile, each server that fails contributes an APT to the final SPT. The worst case token is used as the SPT, which symbolizes the overall posture of the NAC-client computer

Configuring Authorization Policies

Authorization policies comprise rules that are applied to a NAP. Authorization policies are used for authorizing an authenticated user. Authorization rules can be based on group membership, posture validation, or both. Authorization actions are built from the RADIUS Authorization Components and ACLs.

Credentials are used in identity and posture authorization. Each application's posture credentials are evaluated separately. Credentials are compared against the posture-validation policies.

When you configure authorization policies consider the result of:

- User authentication is assignment to a User Group.
- Posture validation is a System Posture Token.
- EAP-FAST authentication and posture validation in the same session results in assignment to a user group and a posture token.

Authorization policies are a conversion of an ACS user group and a posture token to a set of RADIUS attributes that will be sent to the device. You may deny access for a specific user group, or deny access based on a returned token.

Note When you deny access for a specific condition, you do not need to select RAC or downloadable ACLs.

Authorization Rules

Authorization rules allow for variation of device provisioning within the NAP based on group membership and posture token.

The set of possible mappings is theoretically quite high–for each NAP–for each group and for each posture. However, in practice most users will be caught by a default case; for example, normal healthy users.

Exceptions to the norm would be corner cases, such as groups that require specialized access rights (for example, administrators) or users with Infected or Quarantined postures.

Therefore, when you design the authorization rules, it is useful to define the normal condition first; then the set of exception cases that require more specific mappings.

In a non-NAC network, leave the System Posture Token as **Any**.

An authorization rule can be defined as:

If the user-group = selected-user-group or the posture-assessment = selected-posture-assessment, then provision the profile with the selected-RAC or the selected DACL.

You can also use authorization rules to explicitly deny (send an access-reject) as an action.

This section contains the following information on configuring authorization rules:

- Configuring an Authorization Rule, page 15-44
- Configuring a Default Authorization Rule, page 15-45
- Ordering the Authorization Rules, page 15-46
- Deleting an Authorization Rule, page 15-46
- Shared RACs, page 15-46
- RAC and Groups, page 15-47
- Merging Attributes, page 15-47
- Troubleshooting Profiles, page 15-47
- Migrating from Groups to RACs, page 15-47

Configuring an Authorization Rule

To configure an authorization rule:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the relevant profile **Authorization** policy.

Step 3 The Authorization Rules for Profile Page appears.

Step 4 Click **Add Rule**. The Authorization Rules for Profile Page appears.

Step 5 Select a **User Group** from the drop-down list.

Step 6 Select the **System Posture Token**

Step 7 Select Authentication Actions

You may select to deny access or one or both authorization actions to implement when the authorization rules match:

- **Deny Access**—Check this option to deny access for users that have matching conditions.
- **Shared RAC**—Select a Shared RAC from the drop-down list. See Shared RACs, page 15-46.
- **Downloadable ACL**—Select a downloadable ACL from the drop-down list. See Downloadable ACLs, page 15-15.

Step 8 Set RADIUS attribute overrides.

The following options are enabled by default. Uncheck them if you do not want to use RADIUS attributes per user record or per user's group:

- Include RADIUS attributes from user's group
- Include RADIUS attributes from user's record

Step 9 Click **Submit**.

Authorization Rules for Profile Page

This page contains:

Field	Description
Condition	
User Group	Select the ACS group to which the user was mapped. This field defines the group of users for this rule. If you are not basing authorization rules on authentication, select **Any**.
System Posture Token	Select the posture token that was returned as a result of posture validation. ACS checks the token status before proceeding to follow the configured actions. You can use posture tokens to validate user groups. If you are not using posture validation, select **Any**.
Action	
Deny Access	Enable this option to deny access for requests that do not match any configured policy.
Shared RAC	Select Shared RAC from the drop-down list. RAC are defined in Shared Profile Components > RADIUS Authorization Components option. For more information, see RADIUS Authorization Components, page 5-6. **Note** If you configure an external posture validation audit server to use session-timeout settings in the Authorization policy, you must select a shared RAC. See External Audit Server Configuration Options, page 14-16.
DACL	Select Interface Configuration > Advanced Options and then select User or Group Level Downloadable ACLs or both. Proceed to Shared Profile Components and then select Downloadable IP ACLs. For more information, see Downloadable IP ACLs, page 5-13.

Configuring a Default Authorization Rule

You can set a default authorization rule if a condition is not defined or no matched condition is found. You can deny or grant access based on Shared RACs and DACLs selections.

To configure a default authorization rule:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the relevant profile **Authorization** policy.

Step 3 The Authorization Rules for Profile Page appears.

Step 4 Click **Add Rule**. The Authorization Rules for Profile Page appears.

Step 5 Select Authentication Action for the line that contains the text **If a condition is not defined or there is no matched condition.**

Step 6 Select Authentication Actions.

You may select an authorization action to implement for the default rule:

- **Deny Access**–Check this option to deny access for users that have matching conditions.You do not have to select any shared RACs or DACLs for this option.
- **Shared RAC**–Select a Shared RAC from the drop-down list. For more information, see Shared RACs, page 15-46.
- **Downloadable ACL**–Select a downloadable ACL from the drop-down list. See Downloadable IP ACLs, page 5-13 for more information.

Step 7 Set RADIUS attribute overrides.

The following options are enabled by default. Uncheck them if you do not want to use RADIUS attributes per user record or per user's group:

- Include RADIUS attributes from user's group
- Include RADIUS attributes from user record

Step 8 Click **Submit**.

Ordering the Authorization Rules

The authorization policy first match is implemented to authorize a client request.

Note You must place your highest priority authorization policies at the top of the list. If you select Any Group for the User Group or Any Assessment for the posture token first match, the underlying policies will not be effective because authorization accepts the first match.

When you specify the order of conditions in a policy, determine the likelihood of each condition to be true and then order the policies so that the condition most likely to be true is first and the least likely to be true is last.

To order authorization rules:

Step 1 Click the radio button to select the authorization rule that you want to reorder.

Step 2 Click **Up** or **Down** to set the order.

Deleting an Authorization Rule

To delete an authorization rule:

Step 1 Click Internal Posture Validation Policies, External Posture Validation Servers to select an authorization policy.

Step 2 Click **Delete** to remove the selected rule.

By default, RADIUS attribute rules from user or group records are enabled.

Shared RACs

You can use NAPs to provision the same RADIUS attribute to have different values for different users, groups and NAPs. The one-user-one-group-one-profile is now more flexible by using profile based policies instead. For each NAP, you can configure what policies will authenticate and authorize based on RADIUS attribute values.

For a particular group (for example, Admins) who require distinct authorization profiles for the Corporate LAN, VPN, and WLAN NAPs, you can assign them a specific set of RADIUS attributes to allow them special access. If your user is in a group named contractors, they may get the same set of attributes with different values that may specify more stringent security measures.

RAC and Groups

ACS groups hold attributes that are related to the user group (for example admins, contractors, and so on) and do not cater to the same groups of users that require authorization for different network services (WLAN, VPN, and so on).

RACs hold attributes that can be specific to a single network profile by using authorization policies. You can map from various groups and postures to a set of RACs and ACLs.

You should use RACs when the customer requires profile-differentiated RADIUS authorization. For example, if the session-timeout must be several days for VPN and several hours for WLAN.

Merging Attributes

You can merge RADIUS attributes, downloadable ACLs, and other attributes that are created dynamically. RADIUS attributes can be at a user record level, group level and shared RAC level.

When group or user attributes are enabled, attribute merging is performed by a process of repeated overriding whatever is listed in priority order, highest first. The order is:

- User overrides
- Dynamic session (for example, posture token)
- Authentication protocol (for example, session timeout, wireless session keys)
- Downloadable ACL (assignment)
- Shared RACs
- Static group

The attributes in the assigned Shared RAC override those that are defined in a static ACS group. That attribute set is then overridden with attributes from downloadable ACL and so on. Be cautious when you use NAP authorization policies.

By default, RADIUS attribute rules from user or group records are enabled.

Troubleshooting Profiles

If the profile that is sent to the device is not what you expected, the authorization policy has probably been changed to disable group or user attributes. These attributes are being merged with the RAC that the policy assigns. Other possibilities are that ACS automatically adds certain attributes as part of the authentication protocol or an external audit server might sometimes dictate a specific Session-Timeout.

Ensure that attribute merging is not selected.

Note The Session-Timeout values for NAC deployments can have a significant impact on ACS performance. You should adjust it for the scale of your network and ACS transaction capacity.

Migrating from Groups to RACs

To set up a plan to migrate from groups to RACs:

Step 1 Define the appropriate network access policies and define rules.

Step 2 Create a matrix that shows the level of authorization for each user group and posture.

Step 3 Group all the similar cases and create RACs for them.

Step 4 Remove any previously defined attributes from the users groups if desired.

Step 5 You can use group attributes (if the authorization policy check box is selected) so that you can apply profile-independent attributes to all users of the group without having to duplicate each RAC for each profile.

When you merge between group, RAC, and user attributes, remember that attributes set at a group level are not guaranteed to make the final profile. Depending on your selections, RAC might override them.

You can create a base template authorization at group level and then supply the profile-specific attributes by using RACs. For example, setting a different Session-Timeout for VPN and WLAN.

Policy Replication and Backup

All NAP policies are entirely replicated when you select NAPs for replication. Profiles contain a collaboration of configuration settings. The profile replication components include:

- Network Access Profiles
- Posture-validation settings
- AAA clients and hosts
- External database configuration
- Global authentication configuration
- NDGs
- Dictionaries
- Shared-profile components (RAC, NAF, and downloadable ACLs)
- Additional logging attributes.

EAP-FAST uses a different mechanism for replication and, therefore, should also be checked.

Note Replication of profiles contradicts with replication of Network Configuration Device tables, therefore do not check both of these components at the same time. Replication in ACS only works between the same versions of ACS. Replication does not include external databases and all other global ACS configuration parameters.

To replicate policies:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 In the Database Replication Setup page select **Network Access Profiles**.

Step 3 Select whether this ACS is to receive or send the information.

CHAPTER 16

Unknown User Policy

This chapter addresses the Unknown User Policy feature, found in the External User Databases section of the ACS web interface.You can also configure the Unknown User Policy for Network Access Profiles (NAPs). In Cisco Secure Access Control Server for Windows, hereafter referred to as ACS, the internal database against which an unknown user authenticates, must be explicitly selected from the Credential Validation Databases in the NAP configuration settings for Authentication.

After you have configured at least one database in the External User Databases section of the ACS web interface, you can decide how to implement other ACS features that are related to authentication. These features are the Unknown User Policy and user group mapping.

For information about user group mapping, see Chapter 17, "User Group Mapping and Specification."

For information about databases supported by ACS and how to configure databases in the web interface, see Chapter 13, "User Databases."

This chapter contains the following topics:

- Known, Unknown, and Discovered Users, page 16-2
- Authentication and Unknown Users, page 16-3
  - About Unknown User Authentication, page 16-3
  - General Authentication of Unknown Users, page 16-3
  - Windows Authentication of Unknown Users, page 16-4
  - Performance of Unknown User Authentication, page 16-6
- Authorization of Unknown Users, page 16-6
- Unknown User Policy Options, page 16-7
- Database Search Order, page 16-7
- Configuring the Unknown User Policy, page 16-8
- Disabling Unknown User Authentication, page 16-9

Known, Unknown, and Discovered Users

The Unknown User Policy feature provides different means of handling authentication requests, depending upon the type of user requesting AAA services. There are three types of users. Their significance varies depending on whether the service requested is authentication:

- **Known Users**—Users explicitly added, manually or automatically, to the ACS internal database. These are users added by an administrator using the web interface, by the RDBMS Synchronization feature, by the Database Replication feature, or by the `CSUtil.exe` utility. For more information about `CSUtil.exe`, see Appendix D, "CSUtil Database Utility." ACS handles authentication requests for known users with authentication:

  ACS attempts to authenticate a known user with the single user database with which the user is associated with. If the user database is the ACS internal database and the user does not represent a Voice-over-IP (VoIP) user account, a password is required for the user. If the user database is an external user database or if the user represents a VoIP user account, ACS does not have to store a user password in the user database.

  ACS does not support failover authentication. If authentication fails with the database that the user is associated with, ACS uses no other means to authenticate the user and ACS informs the AAA client of the authentication failure.

- **Unknown Users**—Users who do not have a user account in the ACS internal database. This means that the user has not received authentication from ACS or that the user account was deleted. Your configuration of the Unknown User Policy specifies how ACS handles authentication requests for unknown users.

  For details about unknown user authentication, see General Authentication of Unknown Users, page 16-3.

- **Discovered Users**—Users whose accounts ACS created in the ACS internal database after successful authentication by using the Unknown User Policy. All discovered users were unknown users. When ACS creates a discovered user, the user account contains only the username, a Password Authentication list setting that reflects the database that provided authentication for the user, and a Group to which the user is assigned list setting of Mapped By External Authenticator, which enables group mapping. Using the ACS web interface or RDBMS Synchronization, you can further configure the user account as needed. For example, after a discovered user is created in ACS, you can assign user-specific network access restrictions to the discovered user.

  Note ACS does not import credentials (such as passwords, certificates) for a discovered user.

  The authentication process for discovered users is identical to the authentication process for known users who are authenticated with external user databases and whose ACS group membership is determined by group mapping.

Note We recommend removing a username from a database when the privileges that are associated with that username are no longer required. For more information about deleting a user account, see Deleting a User Account, page 7-38.

The unique identifiers for a user are the username and profile name. A user is no longer identified by its username only; but by combination of username and profile name. Discovered users that are dynamically created through use of different profiles have distinguished records in the database. So, settings for user **john** with profile name **routers** will not affect settings for user *john* and profile name *switches*.

For more information on NAPs, see Chapter 15, "Network Access Profiles."

Authentication and Unknown Users

This section provides information about using the Unknown User Policy with authentication. The information in this section is also relevant for NAP authentication policies, unless stated otherwise.

This section contains the following topics:

- About Unknown User Authentication, page 16-3
- General Authentication of Unknown Users, page 16-3
- Windows Authentication of Unknown Users, page 16-4
- Performance of Unknown User Authentication, page 16-6

About Unknown User Authentication

The Unknown User Policy is a form of authentication forwarding. In essence, this feature is an extra step in the authentication process. If a username does not exist in the ACS internal database, ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate. The external database must support the authentication protocol used in the authentication request.

The Unknown User Policy enables ACS to use a variety of external databases to attempt authentication of unknown users. This feature provides the foundation for a basic single sign-on capability through ACS. Because external user databases handle the incoming authentication requests, you do not have to maintain the credentials of users within ACS, such as passwords. This eliminates the necessity of entering every user multiple times and prevents data-entry errors inherent to manual procedures.

Note When you configure NAP, the internal database might not be selected in the web interface. You can select the internal database for authentication in the same way that you select external databases.

General Authentication of Unknown Users

If you have configured the Unknown User Policy in ACS, ACS attempts to authenticate unknown users:

1. ACS checks its internal user database. If the user exists in the ACS internal database (that is, it is a known or discovered user), ACS tries to authenticate the user with the authentication protocol of the request and the database that is specified in the user account. Authentication passes or fails.
2. If the user does not exist in the ACS internal database (that is, it is an unknown user), ACS tries each external user database that supports the authentication protocol of the request, in the order that the Selected Databases list specifies. If authentication with one of the external user databases passes, ACS automatically adds the user to the ACS internal database, with a pointer to use the external user database that succeeded on this authentication attempt. Users who are added by unknown user authentication are flagged as such within the ACS internal database and are called discovered users.

The next time the discovered user tries to authenticate, ACS authenticates the user against the database that was successful the first time. Discovered users are treated the same as known users.

3. If the unknown user fails authentication with all configured external databases, the user is not added to the ACS internal database and the authentication fails.

The previous scenario is handled differently if user accounts with identical usernames exist in separate Windows domains. For more information, see Windows Authentication of Unknown Users, page 16-4.

Note Because usernames in the ACS internal database must be unique, ACS supports a single instance of any given username across all databases that it is configured to use. For example, assume every external user database contains a user account with the username John. Each account is for a different user, but they each, coincidentally, have the same username. After the first John attempts to access the network and has authenticated through the unknown user process, ACS retains a discovered user account for that John and only that John. Now, ACS tries to authenticate subsequent attempts by any user named John using the same external user database that originally authenticated John. Assuming their passwords are different than the password for the John who authenticated first, the other Johns are unable to access the network.

Windows Authentication of Unknown Users

Because the same username can recur across the trusted Windows domains against which ACS authenticates users, ACS treats authentication with a Windows user database as a special case.

To perform authentication, ACS communicates with the Windows operating system of the computer that is running ACS. Windows uses its built-in facilities to forward the authentication requests to the appropriate domain controller.

This section contains the following topics:

- Domain-Qualified Unknown Windows Users, page 16-4
- Windows Authentication with Domain Qualification, page 16-5
- Multiple User Account Creation, page 16-5

Domain-Qualified Unknown Windows Users

When a domain name is supplied as part of a authentication request, ACS detects that a domain name was supplied and tries the authentication credentials against the specified domain. The dial-up networking clients that are provided with various Windows versions differ in the method by which users can specify their domains. For more information, see Windows Dial-Up Networking Clients, page 13-7.

Using a domain-qualified username allows ACS to differentiate a user from multiple instances of the same username in different domains. For unknown users who provide domain-qualified usernames and who are authenticated by a Windows user database, ACS creates their user accounts in the ACS internal database in the form *DOMAIN\username*. The combination of username and domain makes the user unique in the ACS database.

For more information about domain-qualified usernames and Windows authentication, see Usernames and Windows Authentication, page 13-8.

Windows Authentication with Domain Qualification

If the username is nondomain qualified or is in UPN format, the Windows operating system of the computer that is running ACS follows a more complex authentication order, which ACS cannot control. Though the order of resources used can differ, when searching for a non-domain qualified username or UPN username, Windows usually follows this order:

1. The local domain controller.
2. The domain controllers in any trusted domains, in an order determined by Windows.
3. If ACS runs on a member server, the local accounts database.

Windows attempts to authenticate the user with the first account that it finds whose username matches the one that ACS passes to Windows. Whether authentication fails or succeeds, Windows does not search for other accounts with the same username; therefore, Windows can fail to authenticate a user who supplies valid credentials because Windows may check the supplied credentials against the wrong account that coincidentally has an identical username.

You can circumvent this difficulty by using the Domain List in the ACS configuration for the Windows user database. If you have configured the Domain List with a list of trusted domains, ACS submits the username and password to each domain in the list, using a domain-qualified format, until ACS successfully authenticates the user, or has tried each domain in the Domain List and fails the authentication.

Note If your network has multiple occurrences of a username across domains (for example, every domain has a user called Administrator) or if users do not provide their domains as part of their authentication credentials, you must configure the Domain List for the Windows user database in the External User Databases section. If not, only the user whose account Windows happens to check first authenticates successfully. The Domain List is the only way that ACS controls the order in which Windows checks domains. The most reliable method of supporting multiple instances of a username across domains is to require users to supply their domain memberships as part of the authentication request. For more information about the effects of using the Domain List, see Nondomain-Qualified Usernames, page 13-9.

Multiple User Account Creation

Unknown user authentication can create more than one user account for the same user. For example, if a user provides a domain-qualified username and successfully authenticates, ACS creates an account in the format *FFF*. If the same user successfully authenticates without prefixing the domain name to the username, ACS creates an account in the format *username*. If the same user also authenticates with a UPN version of the username, such as *username@example.com*, ACS creates a third account.

If, to assign authorizations, you rely on groups rather than individual user settings, all accounts that authenticate by using the same Windows user account should receive the same privileges. Regardless of whether the user prefixes the domain name, group mapping will assign the user to the same ACS user group, because both ACS user accounts correspond to a single Windows user account.

Performance of Unknown User Authentication

Processing authentication requests for unknown users requires slightly more time than processing authentication requests for known users. This small delay may require additional timeout configuration on the AAA clients through which unknown users may attempt to access your network.

Added Authentication Latency

Adding external user databases against which to authenticate unknown users can significantly increase the time needed for each individual authentication. At best, the time needed for each authentication is the time taken by the external user database to authenticate, plus some time for ACS processing. In some circumstances (for example, when using a Windows user database), the extra latency introduced by an external user database can be as much as tens of seconds. If you have configured the Unknown User Policy to include multiple databases in unknown user authentication, the latency for which your AAA client timeout values must account is the sum of the time taken for each external user database to respond to an authentication request of an unknown user, plus the time taken for ACS processing.

You can reduce the effect of this added latency by setting the order of databases. If you are using an authentication protocol that is particularly time sensitive, such as PEAP, we recommend configuring unknown user authentication to attempt authentication first with the database most likely to contain unknown users who use the time-sensitive protocol. For more information, see Database Search Order, page 16-7.

Authentication Timeout Value on AAA clients

You must increase the AAA client timeout to accommodate the longer authentication time that is required for ACS to pass the authentication request to the external user databases that an unknown user authentication uses. If the AAA client timeout value is not set high enough to account for the delay that an unknown user authentication requires, the AAA client times out the request and every unknown user authentication fails.

In Cisco IOS, the default AAA client timeout value is five seconds. If you have ACS configured to search through several databases or your databases are slow to respond to authentication requests, consider increasing the timeout values on AAA clients. For more information about authentication timeout values in IOS, refer to your Cisco IOS documentation.

Authorization of Unknown Users

Although the Unknown User Policy allows authentication requests to be processed by databases that are configured in the External User Database section, ACS is responsible for all authorizations that are sent to AAA clients and end-user clients. Unknown user authentication works with the ACS user group mapping features to assign unknown users to user groups that you have already configured and, therefore, to assign authorization to all unknown users who pass authentication. For more information, see Chapter 17, “User Group Mapping and Specification,” and Chapter 14, “Posture Validation.”

Unknown User Policy Options

On the Configure Unknown User Policy page, you can specify what ACS does for unknown user authentication. The options for configuring the Unknown User Policy are:

- **Fail the attempt**—Disables unknown user authentication; therefore, ACS rejects authentication requests for users whom the ACS internal database does not contain. Selecting this option excludes the use of the Check the following external user databases option.
- **Check the following external user databases**—Enables unknown user authentication; therefore, ACS uses the databases in the Selected Databases list to provide unknown user authentication.

  Note For authentication requests, ACS applies the Unknown User Policy to unknown users only. ACS does not support fallback to unknown user authentication when known or discovered users fail authentication.

  Selecting this option excludes the use of the Fail the attempt option.
- **External Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that ACS does *not* use during unknown user authentication.
- **Selected Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that ACS *does* use during unknown user authentication. ACS attempts the requested service—authentication—by using the selected databases one at a time in the order that you specified. For more information about the significance of the order of selected databases, see Database Search Order, page 16-7.
- **Configure Enable Password Behavior**—Determines the initial TACACS+ Enable Password setting in the **Advanced TACACS+ Settings** section of newly created dynamic users. For more information, see Setting TACACS+ Enable Password Options for a User, page 7-23

  If **The Internal database** is selected, the TACACS+ Enable Password setting in the configuration of a new dynamic user will be set to Use Separate Password. Edit the TACACS+ Enable Password for the user to perform TACACS+ enable authentications.

  If **The database in which the user profile is held** is selected, the TACACS+ Enable Password setting in the configuration of a new dynamic user will be set to Use External Database Password, and the database by which the user was correctly authenticated will be selected in the selection box on the user record. This configuration affects the initial setting of the new dynamic user. Once ACS has cached the user, you can override the TACACS+ Enable Password setting, and use the Configure Enable Password Behavior.

For detailed steps for configuring the Unknown User Policy, see Configuring the Unknown User Policy, page 16-8.

Database Search Order

You can configure the order in which ACS checks the selected databases when ACS attempts unknown authentication. The Unknown User Policy supports unknown user authentication. It will:

1. Find the next user database in the Selected Databases list that supports the authentication protocol of the request. If the list contains no user databases that support the authentication protocol of the request, stop unknown user authentication and deny network access to the user.
2. Send the authentication request to the database in Step 1.

3. If the database responds with an `Authentication succeeded` message, create the discovered user account, perform group mapping, and grant the user access to the network.
4. If the database responds with an `Authentication failed` message or does not respond and other databases are listed below the current database, return to Step 1.
5. If no additional databases appear below the current database, deny network access to the user.

When you specify the order of databases in the Selected Databases list, we recommend placing as near to the top of the list as possible databases that:

- Process the most requests.
- Process requests that are associated with particularly time-sensitive AAA clients or authentication protocols.
- Require the most restrictive mandatory credential types (applies to policy only).

As a user authentication example, if wireless LAN users access your network with PEAP, arrange the databases in the Selected Databases list so that unknown user authentication takes less than the timeout value that is specified on the Cisco Aironet Access Point.

Configuring the Unknown User Policy

Use this procedure to configure your Unknown User Policy.

For NAP policies, see Adding a Profile, page 15-7.

Before You Begin

For information about the Configure the Unknown User Policy page, see Unknown User Policy Options, page 16-7.

To specify how ACS processes unknown users:

Step 1 In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.

Step 2 To deny unknown user authentication requests, select the **Fail the attempt** option.

Step 3 To allow unknown user authentication, enable the Unknown User Policy:

a. Select the **Check the following external user databases** option.

b. For each database that you want ACS to use for unknown user authentication, select the database in the External Databases list and click **-->** (right arrow button) to move it to the Selected Databases list. To remove a database from the Selected Databases list, select the database, and then click **<--** (left arrow button) to move it back to the External Databases list.

c. To assign the database search order, select a database from the Selected Databases list, and click **Up** or **Down** to move it into the position that you want.

Note For more information about the significance of database order, see Database Search Order, page 16-7.

Step 4 To configure the enable password behavior, select **The internal database** option for each authentication or select **The database in which the user profile is held** option to allow newly created dynamic users, using the TACACS+ protocol, to have their enable password settings initialized. Clicking **The database in which the user profile is held** option permits subsequent authentications to work with the external database that cached the user.

Step 5 Click **Submit**.

ACS saves and implements the Unknown User Policy configuration that you created. ACS processes unknown user authentication requests by using the databases in the order in the Selected Databases list.

Disabling Unknown User Authentication

You can configure ACS so that it does not provide authentication service to users who are not in the ACS internal database.

To turn off unknown user authentication:

Step 1 In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.

Step 2 Select the **Fail the attempt** option.

Step 3 Click **Submit**.

Unknown user authentication is halted. ACS does not allow unknown users to authenticate with external user databases.

User Group Mapping and Specification

This chapter provides information about group mapping and specification. The Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, uses these features to assign users who are authenticated by an external user database to a single ACS group.

This chapter contains the following topics:

- About User Group Mapping and Specification, page 17-1
- Group Mapping by External User Database, page 17-1
- Group Mapping by Group Set Membership, page 17-3
- RADIUS-Based Group Specification, page 17-8

About User Group Mapping and Specification

You can use the Database Group Mapping feature in the External User Databases section to associate unknown users with an ACS group for the purpose of assigning authorization profiles. For external user databases from which ACS can derive group information, you can associate the group memberships, which are defined for the users in the external user database, to specific ACS groups. For Windows user databases, group mapping is further specified by domain; because each domain maintains its own user database.

In addition to the Database Group Mapping feature, for some database types, ACS supports Remote Access Dial-In User Service (RADIUS)-based group specification.

Group Mapping by External User Database

You can map an external database to a ACS group. Unknown users who authenticate by using the specified database automatically belong to, and inherit the authorizations of, the group. For example, you could configure ACS so that all unknown users who authenticate with a certain token server database belong to a group called Telecommuters. You could then assign a group setup that is appropriate for users who are working away from home, such as `MaxSessions=1`. Or, you could configure restricted hours for other groups; but give unrestricted access to Telecommuters group members.

While you can configure ACS to map all unknown users in any external user database type to a single ACS group, the following external user database types are the external user database types whose users you can only map to a single ACS group:

- Open Database Connectivity (ODBC)
- Lightweight and Efficient Application Protocol (LEAP) Proxy RADIUS server
- Remote Access Dial-In User Service (RADIUS) token server
- Rivest, Shamir, and Adelman (RSA) SecurID token server

For a subset of the external user database types that were previously listed, group mapping by external database type is overridden on a user-by-user basis when the external user database specifies an ACS group with its authentication response. ACS supports specification of group membership for the following external user database types:

- LEAP Proxy RADIUS server.
- RADIUS token server.

For more information about specifying group membership for users who are authenticated with one of these database types, see RADIUS-Based Group Specification, page 17-8.

Additionally, users who are authenticated by an ODBC external user database can also be assigned to a specified ACS group. Group specification by ODBC database authentication overrides group mapping. For more information about specifying group membership for users who are authenticated with an ODBC database, see ODBC Database, page 13-34.

Creating an ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database

To set or change a token server, ODBC, or LEAP Proxy RADIUS Server database group mapping:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the name of the token server, LEAP Proxy RADIUS Server, or ODBC database configuration for which you want to configure a group mapping.

The Define Group Mapping table appears.

Step 4 From the Select a default group for *database* list, click the group to which users who were authenticated with this database should be assigned.

Tip The Select a default group for *database* list displays the number of users who are assigned to each group.

Step 5 Click **Submit**.

ACS assigns unknown and discovered users who are authenticated by the external database type that you selected in Step 3 to the ACS group that is selected in Step 4. For users who are authenticated by an ODBC, RADIUS token server, or LEAP Proxy RADIUS Server database, the mapping is only applied as a default if those databases did not specify an ACS group for the user.

Note For more information about group specification for RADIUS token servers, see RADIUS-Based Group Specification, page 17-8. For more information about group specification for ODBC databases, see ACS Authentication Process with an ODBC External User Database, page 13-35.

Group Mapping by Group Set Membership

You can create group mappings for some external user databases based on the combination of external user database groups to which users belong. The following database types are the external user database types for which you can create group mappings based on group set membership:

- Windows domains.

  Note Group mapping for Windows authentication supports only those users who belong to no more than 500 Windows groups.

- Generic Lightweight Directory Access Protocol (LDAP).

When you configure an ACS group mapping based on group set membership, you can add one or many external user database groups to the set. For ACS to map a user to the specified ACS group, the user must match *all* external user database groups in the set.

As an example, you could configure a group mapping for users who belong to the Engineering and Tokyo groups and a separate one for users who belong to Engineering and London. You could then configure separate group mappings for the combinations of Engineering-Tokyo and Engineering-London, and configure different access times for the ACS groups to which they map. You could also configure a group mapping that only included the Engineering group that would map other members of the Engineering group who were not members of Tokyo or London.

Group Mapping Order

ACS always maps users to a single ACS group; yet a user can belong to more than one group set mapping. For example, a user named *John* could be a member of the group combination Engineering and California, and at the same time be a member of the group combination Engineering and Managers. If ACS group set mappings exist for both these combinations, ACS has to determine to which group *John* should be assigned.

ACS prevents conflicting group set mappings by assigning a mapping order to the group set mappings. When a user who is authenticated by an external user database is assigned to an ACS group, ACS starts at the top of the list of group mappings for that database. ACS sequentially checks the user group memberships in the external user database against each group mapping in the list. When finding the first group set mapping that matches the external user database group memberships of the user, ACS assigns the user to the ACS group of that group mapping and terminates the mapping process.

Tip The order of group mappings is important because it affects the network access and services that are allowed to users. When defining mappings for users who belong to multiple groups, ensure that they are in the correct order; so that users are granted the correct group settings.

For example, a user named *Mary* is assigned to the three-group combination of Engineering, Marketing, and Managers. *Mary* should be granted the privileges of a manager rather than an engineer. Mapping A assigns to ACS Group 2 users who belong to all three groups of which *Mary* is a member. Mapping B assigns to ACS Group 1 users who belong to the Engineering and Marketing groups. If Mapping B is listed first, ACS authenticates *Mary* as a user of Group 1 and she is be assigned to Group 1, rather than Group 2 as managers should be.

No Access Group for Group Set Mappings

To prevent remote access for users who are assigned a group by a particular group set mapping, assign the group to the ACS No Access group. For example, you could assign all members of an external user database group *Contractors* to the No Access group so they could not dial in to the network remotely.

Default Group Mapping for Windows

For Windows user databases, ACS includes the ability to define a default group mapping. If no other group mapping matches an unknown user who is authenticated by a Windows user database, ACS assigns the user to a group based on the default group mapping.

Configuring the default group mapping for Windows user databases is the same as editing an existing group mapping, with one exception. When editing the default group mapping for Windows, instead of selecting a valid domain name on the Domain Configurations page, select **\DEFAULT**.

For more information about editing an existing group mapping, see Editing a Windows or Generic LDAP Group Set Mapping, page 17-6.

Windows Group Mapping Limitations

ACS has the following limits on group mapping for users who are authenticated by a Windows user database:

- ACS can only support group mapping for users who belong to 500 or fewer Windows groups.
- ACS can only perform group mapping by using the local and global groups to which a user belongs in the domain that authenticated the user. You cannot use group membership in domains that the authenticated domain trusts that is for ACS group mapping. This restriction is not removed by adding a remote group to a group that is local to the domain providing the authentication.

Creating an ACS Group Mapping for Windows or Generic LDAP Groups

Before You Begin

To map a Windows or generic LDAP group to an ACS group:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database name for which you want to configure a group mapping.

If you are mapping a Windows group set, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.

Step 4 If you are mapping a Windows group set for a new domain:

a. Click **New configuration**.

The Define New Domain Configuration page appears.

b. If the Windows domain for which you want to create a group set mapping configuration appears in the Detected domains list, select the name of the domain.

Tip To clear your domain selection, click **Clear Selection**.

c. If the Windows domain for which you want to create a group set mapping *does not appear* in the Detected domains list, type the name of a trusted Windows domain in the **Domain** box.

d. Click **Submit**.

The new Windows domain appears in the list of domains in the Domain Configurations page.

Step 5 If you are mapping a Windows group set, click the domain name for which you want to configure a group set mapping.

The Group Mappings for Domain: *domainname* table appears.

Step 6 Click **Add Mapping**.

The Create new group mapping for *database* page opens. The group list displays group names that are derived from the external user database.

Step 7 For each group to be added to the group set mapping, select the name of the applicable external user database group in the group list, and then click **Add to selected**.

Note A user must match *all* the groups in the Selected list so that ACS can use this group set mapping to map the user to an ACS group; however, a user can also belong to other groups (in addition to the groups listed) and still be mapped to an ACS group.

Tip To remove a group from the mapping, select the name of the group in the Selected list, and then click **Remove from selected**.

The Selected list shows all the groups to which a user must belong in order to be mapped to an ACS group.

Step 8 In the ACS group list, select the name of the ACS group to which you want to map users who belong to all the external user database groups in the Selected list.

Note You can also select **No Access**. For more information about the **No Access** group, see No Access Group for Group Set Mappings, page 17-4.

Step 9 Click **Submit**.

The group set you mapped to the ACS list appears at the bottom of the *database* groups column.

Note The asterisk (*) at the end of each set of groups indicates that users who are authenticated with the external user database can belong to other groups besides those in the set.

Editing a Windows or Generic LDAP Group Set Mapping

You can change the ACS group to which a group set mapping is mapped.

Note You cannot edit the external user database groups of an existing group set mapping. If you want to add or remove external user database groups from the group set mapping, delete the group set mapping and create one with the revised set of groups.

To edit a Windows or generic LDAP group mapping:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database name for which you want to edit a group set mapping.

If you are editing a Windows group set mapping, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.

Step 4 If you are editing a Windows group set mapping, click the domain name for which you want to edit a group set mapping.

The Group Mappings for Domain: *domainname* table appears.

Step 5 Click the group set mapping to be edited.

The Edit mapping for *database* page opens. The external user database group or groups that are included in the group set mapping appear above the ACS group list.

Step 6 From the ACS group list, select the name of the group to which to map the set of external database groups, and then click **Submit**.

Note You can also select **No Access**. For more information about the **No Access** group, see No Access Group for Group Set Mappings, page 17-4.

Step 7 Click **Submit**.

The Group Mappings for *database* page opens again and includes the changed group set mapping.

Deleting a Windows or Generic LDAP Group Set Mapping

You can delete individual group set mappings.

To delete a Windows or generic LDAP group mapping:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database configuration whose group set mapping you want to delete.

If you are deleting a Windows group set mapping, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.

Step 4 If you are deleting a Windows group set mapping, click the domain name whose group set mapping you want to delete.

The Group Mappings for Domain: *domainname* table appears.

Step 5 Click the group set mapping that you want to delete.

Step 6 Click **Delete**.

ACS displays a confirmation dialog box.

Step 7 Click **OK** in the confirmation dialog box.

ACS deletes the selected external user database group set mapping.

Deleting a Windows Domain Group Mapping Configuration

You can delete an entire group mapping configuration for a Windows domain. When you delete a Windows domain group mapping configuration, you delete all group set mappings in the configuration.

To delete a Windows group mapping:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the name of the Windows external user database.

Step 4 Click the domain name whose group set mapping you want to delete.

Step 5 Click **Delete Configuration**.

ACS displays a confirmation dialog box.

Step 6 Click **OK** in the confirmation dialog box.

ACS deletes the selected external user database group mapping configuration.

Changing Group Set Mapping Order

You can change the order in which ACS checks group set mappings for users who are authenticated by Windows and generic LDAP databases. To order group mappings, you must have already mapped them. For more information about creating group mappings, see Creating an ACS Group Mapping for Windows or Generic LDAP Groups, page 17-4.

To change the order of group mappings for a Windows or generic LDAP group mapping:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database name for which you want to configure group set mapping order.

If you are ordering Windows group set mappings, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.

Step 4 If you are configuring a Windows group mapping order, click the domain name for which you want to configure group set mapping order.

The Group Mappings for Domain: *domainname* table appears.

Step 5 Click **Order mappings**.

Note The Order mappings button appears only if more than one group set mapping exists for the current database and does not apply to default group mapping.

The Order mappings for *database* page appears. The group mappings for the current database appear in the Order list.

Step 6 Select the name of a group set mapping that you want to move, and then click **Up** or **Down** until it is in the position that you want.

Step 7 Repeat Step 7 until the group mappings are in the correct order.

Step 8 Click **Submit**.

The Group Mappings for *database* page displays the group set mappings in the order that you defined.

Step 9 Click **Submit**.

ACS saves the SPT-to-user-group mapping.

RADIUS-Based Group Specification

For some types of external user databases, ACS supports the assignment of users to specific ACS groups based on the RADIUS authentication response from the external user database. ACS provides this assignment in addition to the unknown user group mapping described in Group Mapping by External User Database, page 17-1. RADIUS-based group specification overrides group mapping. The database types that support RADIUS-based group specification are:

- LEAP Proxy RADIUS server
- RADIUS token server

ACS supports per-user group mapping for users who are authenticated with a LEAP Proxy RADIUS Server database. This group mapping support is provided in addition to the default group mapping described in Group Mapping by External User Database, page 17-1.

To enable per user group mapping, configure the external user database to return authentication responses that contain the Cisco IOS/PIX RADIUS attribute 1, [009\001] `cisco-av-pair` with the following value:

`ACS:CiscoSecure-Group-Id =` *N*

where *N* is the ACS group number (0 through 499) to which ACS should assign the user. For example, if the LEAP Proxy RADIUS Server authenticated a user and included the following value for the Cisco IOS/PIX RADIUS attribute 1, [009\001] `cisco-av-pair`:

```
ACS:CiscoSecure-Group-Id = 37
```

ACS assigns the user to group 37 and applies authorization that is associated with group 37.

Troubleshooting

This appendix provides information about certain basic problems and describes how to resolve them.

Scan the column on the left to identify the condition that you are trying to resolve, and then carefully go through each corresponding recovery action offered in the column on the right.

This chapter contains the following topics:

- Administration Issues, page A-2
- Browser Issues, page A-3
- Cisco NAC Issues, page A-3
- Database Issues, page A-6
- Dial-in Connection Issues, page A-8
- Proxy Issues, page A-11
- Installation and Upgrade Issues, page A-11
- MaxSessions Issues, page A-11
- Report Issues, page A-12
- Third-Party Server Issues, page A-14
- User Authentication Issues, page A-14
- TACACS+ and RADIUS Attribute Issues, page A-15

Administration Issues

Condition	Recovery Action
Remote administrator cannot bring up the ACS web interface in a browser or receives a warning that access is not permitted.	To recover from this condition: 1. Verify that you are using a supported browser. Refer to the *Release Notes for Cisco Secure Access Control Server for Windows* for a list of supported browsers. 2. Ping ACS to confirm connectivity. 3. Verify that the remote administrator is using a valid administrator name and password that have previously been added in Administration Control. 4. Verify that Java functionality is enabled in the browser. 5. Determine whether the remote administrator is trying to administer ACS through a firewall, through a device performing Network Address Translation, or from a browser configured to use an HTTP proxy server.
No remote administrators can log in.	The **Allow only listed IP addresses to connect** option is selected, but no start or stop IP addresses are listed. Choose **Administrator Control > Access Policy**, and specify the **Start IP Address** and **End IP Address**.
Unauthorized users can log in.	The **Reject listed IP addresses** option is selected, but no start or stop IP addresses are listed. Choose **Administrator Control > Access Policy**, and specify the **Start IP Address** and **Stop IP Address**.
The Restart Services function does not work.	This malfunction might occur if the system is not responding. To manually restart services: 1. From the Windows **Start** menu, choose **Settings > Control Panel > Administrative Tools > Services**. 2. Click **CSAdmin > Stop > Start**. If the services do not respond when manually restarted, reboot the server.
Administrator configured for event notification is not receiving e-mail.	Ensure that the SMTP server name is correct. If the name is correct, ensure that the computer running ACS can ping the SMTP server or can send e-mail via a third-party e-mail software package. Ensure that you have not used underscores (_)in the e-mail address.
Remote Administrator receives `Logon failed . . . protocol error` message, when browsing.	Restart the CSADMIN service. To restart the CSADMIN service: 1. From the Windows **Start** menu, choose **Control Panel > Services**. 2. Click **CSAdmin > Stop > Start**. If necessary, restart the server.
Remote administrator cannot bring up ACS from his or her browser, or receives a warning that access is not permitted.	If Network Address Translation is enabled on the PIX Firewall, administration through the firewall cannot work. To administer ACS through a firewall, you must configure an HTTP port range. Choose **Administrator Control > Access Policy**. You must configure the PIX Firewall to permit HTTP traffic over all ports in the range specified in ACS. For more information, see Access Policy, page 12-8.

Browser Issues

Condition	Recovery Action
The browser cannot bring up the ACS web interface.	Open Internet Explorer or Netscape Navigator. Choose **Help > About** to determine the version of the browser. See *Installation Guide for Cisco Secure ACS for Windows* for a list of browsers that ACS supports, and the release notes for known issues with a particular browser version.
The browser displays the Java message that your session connection is lost.	Check the **Session idle timeout** value for remote administrators. This value appears on the **Session Policy Setup** page of the **Administration Control** section. Increase the value as needed.
Administrator database appears corrupted.	The remote Netscape client is caching the password. If you specify an incorrect password, it is cached. When you attempt to re-authenticate with the correct password, the incorrect password is sent. Clear the cache before attempting to re-authenticate, or close the browser and open a new session.
Remote administrator intermittently can't browse the ACS web interface.	Ensure that the client browser does not have proxy server configured. ACS does not support HTTP proxy for remote administrative sessions. Disable proxy server settings.

Cisco NAC Issues

Condition	Recovery Action
The results of `show eou all` or `show eou ip` *address* include postures that do not match the actual result of posture validation or display "-------" instead of a posture.	If you see "-------", the AAA client is not receiving the posture-token attribute-value (AV) pair within a Cisco IOS/PIX RADIUS cisco-av-pair vendor-specific attribute (VSA). If the posture that appears does not correspond to the actual result of posture validation, the AAA client is receiving an incorrect value in the posture-token AV pair. Check group mappings for Network Admission Control (NAC) databases to verify that the correct user groups are associated with each system posture token (SPT). In the user groups that are configured for use with NAC, ensure that the Cisco IOS/PIX cisco-av-pair VSA is configured correctly. For example, in a group configured to authorize NAC clients receiving a Healthy SPT, be sure the **[009\001] cisco-av-pair** check box is checked and that the following string appears in the **[009\001] cisco-av-pair** text box: `posture-token=Healthy` ⚠ **Caution** The posture-token AV pair is the only way that ACS notifies the AAA client of the SPT that the posture validation returns. Because you manually configure the posture-token AV pair, errors in configuring posture-token can result in the incorrect SPT being sent to the AAA client; or, if the AV pair name is mistyped, the AAA client not receiving the SPT at all. **Note** AV pair names are case sensitive. For more information about the Cisco IOS/PIX cisco-av-pair VSA, see About the cisco-av-pair RADIUS Attribute, page C-5.

Condition	Recovery Action
Under EXEC Commands, Cisco IOS commands are not being denied when checked.	Examine the Cisco IOS configuration at the AAA client. If it is not already present, add the following Cisco IOS command to the AAA client configuration: `aaa authorization command <0-15> default group TACACS+` The correct syntax for the arguments in the text box is **permit** *argument* or **deny** *argument*.
EAP request has invalid signature. Error message appears in log.	If ACS receives traffic from any EAP-enabled device that has the wrong shared secret, this error message appears in the log. Three conditions that might cause this to occur are: • The wrong signature is being used. • A RADIUS packet was corrupted in transit. • ACS is being attacked. Check the EAP-enabled device and make changes if necessary.
Administrator has been locked out of the AAA client because of an incorrect configuration setup in the AAA client.	If you have a fallback method configured on your AAA client, disable connectivity to the AAA server and log in using local or line username and password. Try to connect directly to the AAA client at the console port. If that is not successful, consult your AAA client documentation or see the Password Recovery Procedures page on Cisco.com for information regarding your particular AAA client.
Unable to enter Enable Mode after doing `aaa authentication enable default tacacs+`. Getting error message: `Error in authentication on the router.`	Check the failed attempts log in the ACS. If the log reads `CS password invalid`, it may be that the user has no enable password set up. Set the TACACS+ Enable Password in the **Advanced TACACS+ Settings** section. If you do not see the Advanced TACACS+ Settings section among the user setup options, choose **Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features** and select that option to have the TACACS+ settings appear in the user settings. Then select **Max privilege for any AAA Client** (this will typically be 15) and enter the TACACS+ Enable Password that you want the user to have for enable.

Condition	Recovery Action
NAC NRE/Guest Access Limit of 100 Endpoints.	A feature in the EAPoUDP state table that prevents denial of service (DoS) attacks on the ACS server by throttling RADIUS requests. When the maximum limit of 100 unauthorized nonresponsive endpoints per NAD is reached, the following message appears on the router console: `*Jan 19 09:51:04.855: %AP-4-POSTURE_EXCEED_MAX_INIT: Exceeded maximum limit (100).` The router stops processing RADIUS requests for NAC. This mechanism will leave legitimate users—with or without CTA—with default network access (whatever the router's interface ACL allows). This message appears because 100 (or more) EAPoUDP sessions are in the INIT state. Normally, upon receiving a RADIUS Accept-Accept from the ACS, the session will transition out of this state. However, the EAPoUDP session will stay in this state during any of the following situations. The: • NAD has over 100 concurrently unauthorized endpoints. • Router receives an Access-Reject from ACS. • Router fails to receive a response from ACS. Based on this behavior, remember the following recommendations: • Properly configure ACS for NAC to minimize unintentional Access-Rejects. • When deploying NAC passively (monitor-only mode), configure ACS to accept all nonresponsive endpoints (NREs) by using a MAC or IP address wildcard with network access restrictions (NARs) in ACS. • You should never have more than 100 unauthorized endpoints behind a single NAC-enabled router or they will prevent access for CTA-enabled endpoints. • Set the default hold period to a low value. A new command will be added to the IOS to allow this limit to be increased or decreased as needed for a given deployment.

Database Issues

Condition	Recovery Action
RDBMS Synchronization is not operating properly.	Make sure that the correct server appears in the Partners list.
Database Replication not operating properly.	• Make sure you have set the server correctly as Send or Receive. • On the sending server, ensure that the receiving server is in the Replication list. • On the receiving server, ensure that the sending server is selected in the Accept Replication from list. Also, ensure that the sending server is not in the replication partner list. • Make sure that the replication schedule on the sending ACS is not conflicting with the replication schedule on the receiving ACS. • If the receiving server has dual network cards, on the sending server add a AAA server to the AAA Servers table in the Network Configuration section for every IP address of the receiving server. If the sending server has dual network cards, on the receiving server add a AAA server to the AAA Servers table in Network Configuration for every IP address of the receiving server.
The external user database is not available in the Group Mapping section.	The external database has not been configured in the External User Databases section; or, the username and password have been typed incorrectly. Click the applicable external database to configure. Make sure that the username and password are correct.
Windows external databases not operating properly.	Make sure that a two-way trust (for dial-in check) has been established between the ACS domain and the other domains. If ACS is installed on a Member Server and is authenticating to a Domain Controller, see the “Authentication Failures When ACS/NT 4.0 Is Authenticating to Active Directory” Field Notice at the following URL: http://www.cisco.com/en/US/ts/fn/200/fn20228.html

Condition	Recovery Action
Unknown users are not authenticated.	To remedy this situation: 1. Choose **External User Databases > Unknown User Policy**. 2. Select the **Check the following external user databases** option. 3. From the External Databases list, select the database(s) against which to authenticate unknown users. 4. Click **—>** (right arrow button) to add the database to the Selected Databases list. 5. Click **Up** or **Down** to move the selected database into the correct position in the authentication hierarchy. If you are using the ACS Unknown User feature, external databases can only authenticate by using PAP.
Same user appears in multiple groups or duplicate users exist in the ACS database. Unable to delete user from database.	Clean up the database by typing the following command from the command line: **csutil -q -d -n -l dump.txt** This command causes the database to be unloaded and reloaded to clear up the counters. **Tip** When you install ACS in the default location, `CSUtil.exe` is located in: `C:\Program Files\CiscoSecure ACS vX.X\Utils`. For more information on using the `CSUtil.exe` command, see Appendix D, "CSUtil Database Utility."

Dial-in Connection Issues

Condition	Recovery Action

A dial-in user cannot connect to the AAA client.
 	
No record of the attempt appears in the TACACS+ or RADIUS Accounting Report (in the Reports & Activity section, click **TACACS+ Accounting** or **RADIUS Accounting** or **Failed Attempts**).
	Examine the ACS Reports or AAA client Debug output to narrow the problem to a system error or a user error. Confirm that:
	• The dial-in user was able to establish a connection and ping the computer *before* ACS was installed. If the dial-in user could not, the problem is related to a AAA client/modem configuration, not ACS.
	• LAN connections for both the AAA client and the computer running ACS are physically connected.
	• IP address of the AAA client in the ACS configuration is correct.
	• IP address of ACS in AAA client configuration is correct.
	• TACACS+ or RADIUS key in both AAA client and ACS are identical (case sensitive).
	• The command **ppp authentication pap** is entered for each interface, if you are using a Windows user database.
	• The command **ppp authentication chap pap** is entered for each interface, if you are using the ACS database.
	• The AAA and TACACS+ or RADIUS commands are correct in the AAA client. The necessary commands reside in:
	`Program Files\CiscoSecure ACS vx.x\TacConfig.txt`
	`Program Files\CiscoSecure ACS vx.x\RadConfig.txt`
	• The ACS Services are running (CSAdmin, CSAuth, CSDBSync CSLog, CSRadius, CSTacacs) on the computer running ACS.

Condition	Recovery Action
A dial-in user cannot connect to the AAA client. The Windows user database is being used for authentication. A record of a failed attempt appears in the Failed Attempts Report (in the Reports & Activity section, click **Failed Attempts**).	Create a local user in the ACS internal database and test whether authentication is successful. If it is successful, the issue is that the user information is not correctly configured for authentication in Windows or ACS. From the Windows User Manager or Active Directory Users and Computers, confirm that the: • Username and password are configured in the Windows User Manager or Active Directory Users and Computers. • User can log in to the domain by authenticating through a workstation. • User Properties window does not have User Must Change Password at Login enabled. • User Properties window does not have Account Disabled selected. • User Properties for the dial-in window does not have Grant dial-in permission to user disabled, if ACS is using this option for authenticating. From within ACS confirm that: • If the username has already been entered into ACS, a Windows user database configuration is selected in the Password Authentication list on the User Setup page for the user. • If the username has already been entered into ACS, the ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Click **Submit + Restart** if a change has been made. • The user expiration information in the Windows user database has not caused failed authentication. For troubleshooting purposes, disable password expiry for the user in the Windows user database. Click **External User Databases**, click **List All Databases Configured**, and then ensure that the database configuration for Windows is listed. In the Configure Unknown User Policy table of the External User Databases section ensure that the Fail the attempt option is not selected. And ensure that the Selected Databases list reflects the necessary database. Verify that the Windows group that the user belongs to has not been mapped to No Access.
A dial-in user cannot connect to the AAA client. The ACS internal database is being used for authentication. A record of a failed attempt appears in the Failed Attempts Report (in the Reports & Activity section, click **Failed Attempts**).	From within ACS confirm that: • The username has been entered into ACS. • ACS internal database is selected from the Password Authentication list and a password has been entered in User Setup for the user. • The ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Click **Submit + Restart** if a change has been made. • Expiration information has not caused failed authentication. Set to **Expiration: Never** for troubleshooting.

Condition	Recovery Action
A dial-in user cannot connect to the AAA client; however, a Telnet connection can be authenticated across the LAN.	The problem is isolated to one of three areas: • Line or modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured. • The user is not assigned to a group that has the correct authorization rights. Authorization rights can be modified under Group Setup or User Setup. User settings override group settings. • The ACS or TACACS+ or RADIUS configuration is not correct in the AAA client. Additionally, you can verify ACS connectivity by attempting to Telnet to the access server from a workstation connected to the LAN. A successful authentication for Telnet confirms that ACS is working with the AAA client.
A dial-in user cannot connect to the AAA client, and a Telnet connection cannot be authenticated across the LAN.	Determine whether the ACS is receiving the request by viewing the ACS reports. Based on what does not appear in the reports and which database is being used, troubleshoot the problem based on: • Line or modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured. • The user does not exist in the Windows user database or the ACS internal database and might not have the correct password. Authentication parameters can be modified under User Setup. • The ACS or TACACS+ or RADIUS configuration is not correct in the AAA client.
Callback is not working.	Ensure that callback works on the AAA client when using local authentication. Then add AAA authentication.
User authentication fails when using PAP.	Outbound PAP is not enabled. If the Failed Attempts report shows that you are using outbound PAP, go to the Interface Configuration section and check the **Per-User Advanced TACACS+ Features** check box. Then, choose the TACACS+ Outbound Password section of the Advanced TACACS+ Settings table on the User Setup page and type and confirm the password in the boxes provided.

Proxy Issues

Condition	Recovery Action
Proxying requests to another server fail.	Ensure that the: • Direction on the remote server is set to Incoming/Outgoing or Incoming, and that the direction on the authentication forwarding server is set to Incoming/Outgoing or Outgoing. • Shared secret (key) matches the shared secret of one or both ACSes. • Character string and delimiter match the stripping information configured in the Proxy Distribution Table, and the position is set correctly to either Prefix or Suffix. If the previous conditions are met, one or more servers is probably down, or no fallback server is configured. Choose the Network Configuration section and configure a fallback server. Fallback servers are used only when: • The remote ACS is down. • One or more services (CSTacacs, CSRadius, or CSAuth) are down. • The secret key is misconfigured. • Inbound or Outbound messaging is misconfigured.

Installation and Upgrade Issues

Condition	Recovery Action

The following error message appears when you try to upgrade or uninstall ACS:
`The following file is invalid or the data is corrupted`
`"DelsL1.isu"`
	From the Windows Registry, delete the following Registry key:
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Uninstall\CiscoSecure`

All previous accounting logs are missing.	When reinstalling or upgrading the ACS software, these files are deleted; unless they have been moved to an alternative directory location.

MaxSessions Issues

Condition	Recovery Action
MaxSessions over VPDN is not working.	The use of MaxSessions over VPDN is not supported.

Condition	Recovery Action
User MaxSessions fluctuates or is unreliable.	Services were restarted, possibly because the connection between the ACS and the AAA client is unstable. Click to clear the **Single Connect TACACS+ AAA Client** check box.
User MaxSessions not taking affect.	Ensure that you have accounting configured on the AAA client, and you are receiving accounting start or stop records.

Report Issues

Condition	Recovery Action
The *logname*`active.csv` report is blank.	You changed protocol configurations recently. Whenever protocol configurations change, the existing *logname*`active.csv` report file is renamed to *logname*`yyyy-mm-dd.csv`, and a new, blank *logname*`active.csv` report is generated.
A report is blank.	Ensure that you have selected Log to *reportname* Report under System Configuration: Logging: Log Target: *reportname*. You must also set Network Configuration: *servername*: Access Server Type to ACS for Windows NT.
No Unknown User information is included in reports.	The Unknown User database was changed. Accounting reports will still contain unknown user information.
Two entries are logged for one user session.	Make sure that the remote logging function is not configured to send accounting packets to the same location as the Send Accounting Information fields in the Proxy Distribution Table.
After you have changed the date format, the Logged-In User list and the `CSAdmin` log still display old format dates.	To see the changes made, you must restart the `CSAdmin` services and log on again.
Effect of logging unavailability on authentication functionality.	When local or remote logging normal operation is halted, authentication functionality will stop after a very short time as all worker threads are busy with logging assignments. Fixing the logging functionality will restore authentication; thus, troubleshooting the logging service logs is necessary.

Condition	Recovery Action
The Logged in Users report works with some devices, but not with others	For the Logged in Users report to work (and this also applies to most other features involving sessions), packets should include at least the following fields: • **Authentication Request packet** – nas-ip-address – nas-port • **Accounting Start packet** – nas-ip-address – nas-port – session-id – framed-ip-address • **Accounting Stop packet** – nas-ip-address – nas-port – session-id – framed-ip-address Also, if a connection is so brief that there is little time between the start and stop packets (for example, HTTP through the PIX Firewall), the `Logged in Users` report may fail.

Third-Party Server Issues

Condition	Recovery Action
You cannot successfully implement the RSA token server.	To recover from this problem: 1. Log in to the computer running ACS. (Ensure that your login account has administrative privileges.) 2. Ensure that the RSA Client software is installed on the same computer as ACS. 3. Follow the setup instructions. Do not restart at the end of the installation. 4. Get the file named *sdconf.rec* from the `/data` directory of the RSA ACE server. 5. Place *sdconf.rec* in the *%SystemRoot%\system32* directory. 6. Ensure that you can ping the machine that is running the ACE server by hostname. (You might need to add the machine in the lmhosts file.) 7. Verify that support for RSA is enabled in External User Database: Database Configuration in the ACS. 8. Run Test Authentication from the Windows control panel for the ACE/Client application. 9. From ACS, install the token server.
Authentication request does not hit the external database.	Set logging to full. Choose **System Configuration > Service Control**. Check *auth.log* for confirmation that the authentication request is being forwarded to the third-party server. If it is not being forwarded, confirm that the external database. configuration is correct, as well as the unknown user policy settings.
On ACE/SDI server no incoming request is seen from ACS, although RSA/agent authentication works.	For dial-up users, ensure that you are using PAP and not MS-CHAP or CHAP. RSA/SDI does not support CHAP and ACS will not send the request to the RSA server; rather, it will log an error with external database failure.

User Authentication Issues

Condition	Recovery Action
After the administrator disables the Dialin Permission setting, Windows database users can still dial in and apply the Callback string configured under the Windows user database. (To locate the Dialin Permission check box, choose **External User Databases > Database Configuration > Windows Database > Configure**.)	Restart ACS services. For steps, see Stopping, Starting, or Restarting Services, page 8-2.
User did not inherit settings from new group.	Users moved to a new group inherit new group settings; but they keep their existing user settings. Manually change the settings in the User Setup section.

Condition	Recovery Action
Authentication fails.	Check the Failed Attempts report. The retry interval may be too short. (The default is 5 seconds.) Increase the retry interval (**tacacs-server timeout 20**) on the AAA client to 20 or greater.
The AAA client times out when authenticating against a Windows user database.	Increase the TACACS+/RADIUS timeout interval from the default, 5, to 20. Set the Cisco IOS command as: **tacacs-server timeout 20** **radius-server timeout 20**
Authentication fails; the error `Unknown NAS` appears in the Failed Attempts log.	Verify the following: • AAA client is configured under the Network Configuration section. • If you have RADIUS/TACACS source-interface command configured on the AAA client, ensure that the client on ACS is configured by using the IP address of the interface specified.
Authentication fails; the error `key mismatch` appears in the Failed Attempts log.	Verify that the TACACS+ or RADIUS keys, in AAA client and ACS, are identical (case sensitive). Re-enter the keys to confirm they are identical.
User can authenticate, but authorizations are not what is expected.	Different vendors use different AV pairs. AV pairs used in one vendor protocol may be ignored by another vendor protocol. Ensure that the user settings reflect the correct vendor protocol; for example, RADIUS (Cisco IOS/PIX).
LEAP authentication fails; the error `Radius extension DLL rejected user` appears in the Failed Attempts log.	Verify the correct authentication type has been set on the Access Point. Ensure that, at a minimum, the Network-EAP check box is selected. If you are using an external user database for authentication, verify that it is supported. For more information, see Authentication Protocol-Database Compatibility, page 1-7.

TACACS+ and RADIUS Attribute Issues

Condition	Recovery Action
TACACS+ and RADIUS attributes do not appear on the Group Setup page.	Ensure that you have at least one RADIUS or TACACS+ AAA client configured in the Network Configuration section and that, in the Interface Configuration section, you have enabled the attributes you need to configure. **Note** Some attributes are not customer-configurable in ACS; instead, their values are set by ACS.

TACACS+ Attribute-Value Pairs

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, supports Terminal Access Controller Access Control System (TACACS+) attribute-value (AV) pairs. You can enable different AV pairs for any supported attribute value.

Cisco IOS AV Pair Dictionary

To use the full range of the Cisco IOS AV-pair dictionary for TACACS+, the AAA client should use IOS version 11.3 or later. Cisco IOS 11.1 and 11.2 have only partial support for TACACS+ AV-pairs.

Note If you specify a given AV pair in ACS, you must also enable the corresponding AV pair in the Cisco IOS software that is running on the AAA client. Therefore, you must consider which AV pairs your Cisco IOS release supports. If ACS sends an AV pair to the AAA client that the Cisco IOS software does not support, that attribute is not implemented.

For more information on TACACS+ AV pairs, refer to Cisco IOS documentation for the release of Cisco IOS that is running on your AAA clients.

Note All TACACS+ values are strings. The concept of value *type* does not exist in TACACS+ as it does in Remote Access Dial-In User Service (RADIUS).

TACACS+ AV Pairs

Note Beginning with ACS 2.3, some TACACS+ attributes no longer appear on the Group Setup page; because IP pools and callback supersede:

addr
addr-pool
callback-dialstring

Additionally, these attributes cannot be set via database synchronization, and **ip:addr=n.n.n.n** is not allowed as a Cisco vendor-specific attribute (VSA).

ACS supports many TACACS+ AV pairs. For descriptions of these attributes, refer to Cisco IOS documentation for the release of Cisco IOS that is running on your AAA clients. TACACS+ AV pairs supported in ACS are:

- acl=
- autocmd=
- callback-line
- callback-rotary
- cmd-arg=
- cmd=
- dns-servers=
- gw-password
- idletime=
- inacl#*n*
- inacl=
- interface-config=
- ip-addresses
- link-compression=
- load-threshold=*n*
- max-links=*n*
- nas-password
- nocallback-verify
- noescape=
- nohangup=
- old-prompts
- outacl#*n*
- outacl=
- pool-def#*n*
- pool-timeout=
- ppp-vj-slot-compression
- priv-lvl=
- protocol=
- route
- route#*n*
- routing=
- rte-ftr-in#*n*
- rte-ftr-out#*n*
- sap#*n*

- sap-fltr-in#*n*
- sap-fltr-out#*n*
- service=
- source-ip=
- timeout=
- tunnel-id
- wins-servers=
- zonelist=

TACACS+ Accounting AV Pairs

ACS supports many TACACS+ accounting AV pairs. For descriptions of these attributes, see Cisco IOS documentation for the release of Cisco IOS that is running on your AAA clients. TACACS+ accounting AV pairs supported in ACS are:

- bytes_in
- bytes_out
- cmd
- data-rate
- disc-cause
- disc-cause-ext
- elapsed_time
- event
- mlp-links-max
- mlp-sess-id
- nas-rx-speed
- nas-tx-speed
- paks_in
- paks_out
- port
- pre-bytes-in
- pre-bytes-out
- pre-paks-in
- pre-paks-out
- pre-session-time
- priv_level
- protocol
- reason
- service

- start_time
- stop_time
- task_id
- timezone
- xmit-rate

RADIUS Attributes

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, supports many Remote Access Dial-In User Service (RADIUS) attributes. This appendix lists the standard attributes, vendor-proprietary attributes, and vendor-specific attributes that ACS supports.

This appendix contains the following topics:

- Before Using RADIUS Attributes, page C-1
- Cisco IOS Dictionary of RADIUS IETF, page C-2
- Cisco IOS/PIX 6.0 Dictionary of RADIUS VSAs, page C-4
- About the cisco-av-pair RADIUS Attribute, page C-5
- Cisco VPN 3000 Concentrator/ASA/PIX 7.x+ Dictionary of RADIUS VSAs, page C-6
- Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs, page C-10
- Cisco Building Broadband Service Manager Dictionary of RADIUS VSA, page C-10
- Cisco Airespace Dictionary of RADIUS VSA, page C-10
- IETF Dictionary of RADIUS IETF (AV Pairs), page C-11
- Microsoft MPPE Dictionary of RADIUS VSAs, page C-19
- Ascend Dictionary of RADIUS AV Pairs, page C-21
- Nortel Dictionary of RADIUS VSAs, page C-28
- Juniper Dictionary of RADIUS VSAs, page C-28

Before Using RADIUS Attributes

You can enable different attribute-value (AV) pairs for Internet Engineering Task Force (IETF) RADIUS and any supported vendor. For outbound attributes, you can configure the attributes that are sent and their content by using the ACS web interface. The RADIUS attributes that are sent to authentication, authorization, and accounting (AAA) clients in access-accept messages are user specific.

To configure a specific attribute to be sent for a user, you must ensure that:

1. In the Network Configuration section, you must configure the AAA client entry corresponding to the access device that grants network access to the user to use a variety of RADIUS that supports the attribute that you want sent to the AAA client. For more information about the RADIUS attribute sets that RADIUS varieties support, see Protocol Configuration Options for RADIUS, page 3-9.

2. In the Interface Configuration section, you must enable the attribute so that it appears on user or user group profile pages. You can enable attributes on the page corresponding to the RADIUS variety that supports the attribute. For example, IETF RADIUS Session-Timeout attribute (27) appears on the RADIUS (IETF) page.

Note By default, per-user RADIUS attributes are not enabled (they do not appear in the Interface Configuration page). Before you can enable attributes on a per-user basis, you must enable the **Per-user TACACS+/RADIUS Attributes** option on the Advanced Options page in the Interface Configuration section. After enabling per-user attributes, a user column will appear as disabled in the Interface Configuration page for that attribute.

3. In the profile that you use to control authorizations for the user— in the user or group edit pages or Shared RADIUS Authorization Component page—you must enable the attribute. Enabling this attribute causes ACS to send the attribute to the AAA client in the access-accept message. In the options that are associated with the attribute, you can determine the value of the attribute that is sent to the AAA client.

Note Settings in a user profile override settings in a group profile. For example, if you configure Session-Timeout in the user profile and also in the group to which the user is assigned, ACS sends the AAA client the Session-Timeout value that is specified in the user profile. If Network Access Profiles (NAPs) are being used, it is possible that attributes from Shared RADIUS Authorization Components may be included in the access accept response. For a discussion about the interaction among group, user, and Shared Radius Authorization Components (SRAC) attributes, see Merging Attributes, page 15-47.

Cisco IOS Dictionary of RADIUS IETF

ACS supports Cisco RADIUS IETF (IOS RADIUS AV pairs). Before selecting AV pairs for ACS, you must confirm that your AAA client is a compatible release of Cisco IOS or compatible AAA client software. For more information, see *Installation Guide for Cisco Secure ACS for Windows* for information about network and port requirements.

Note If you specify a given AV pair on ACS, the corresponding AV pair must be implemented in the Cisco IOS software that is running on the network device. Always consider which AV pairs your Cisco IOS release supports. If ACS sends an AV pair that the Cisco IOS software does not support, the attribute is not implemented.

Note Because IP pools and callback supersede them, the following RADIUS attributes do not appear on the Group Setup page:

Number	Name
8	Framed-IP-Address
19	Callback-Number
218	Ascend-Assign-IP-Pool

None of these attributes can be set via Relational Database Management System (RDBMS) Synchronization.

Table C-1 lists the supported Cisco IOS RADIUS AV pairs.

Table C-1 Cisco IOS Software RADIUS AV Pairs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
1	User-Name	String	Inbound	No
2	User-Password	String	Outbound	No
3	CHAP-Password	String	Outbound	No
4	NAS-IP Address	Ipaddr	Inbound	No
5	NAS-Port	Integer	Inbound	No
6	Service-Type	Integer	Both	No
7	Framed-Protocol	Integer	Both	No
9	Framed-IP-Netmask	Ipaddr (maximum length 15 characters)	Outbound	No
10	Framed-Routing	Integer	Outbound	No
11	Filter-Id	String	Outbound	Yes
12	Framed-MTU	Integer (maximum length 10 characters)	Outbound	No
13	Framed-Compression	Integer	Outbound	Yes
14	Login-IP-Host	Ipaddr (maximum length 15 characters)	Both	Yes
15	Login-Service	Integer	Both	No
16	Login-TCP-Port	Integer (maximum length 10 characters)	Outbound	No
18	Reply-Message	String	Outbound	Yes
21	Expiration	Date	—	—
22	Framed-Route	String	Outbound	Yes
24	State	String (maximum length 253 characters)	Outbound	No
25	Class	String	Outbound	Yes
26	Vendor specific	String	Outbound	Yes
27	Session-Timeout	Integer (maximum length 10 characters)	Outbound	No
28	Idle-Timeout	Integer (maximum length 10 characters)	Outbound	No
30	Called-Station-ID	String	Inbound	No

Table C-1 Cisco IOS Software RADIUS AV Pairs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
31	Calling-Station-ID	String	Inbound	No
33	Login-LAT-Service	String (maximum length 253 characters)	Inbound	No
40	Acct-Status-Type	Integer	Inbound	No
41	Acct-Delay-Time	Integer	Inbound	No
42	Acct-Input-Octets	Integer	Inbound	No
43	Acct-Output-Octets	Integer	Inbound	No
44	Acct-Session-ID	String	Inbound	No
45	Acct-Authentic	Integer	Inbound	No
46	Acct-Session-Time	Integer	Inbound	No
47	Acct-Input-Packets	Integer	Inbound	No
48	Acct-Output-Packets	Integer	Inbound	No
49	Acct-Terminate-Cause	Integer	Inbound	No
61	NAS-Port-Type	Integer	Inbound	No
62	NAS-Port-Limit	Integer (maximum length 10 characters)	Both	No

Cisco IOS/PIX 6.0 Dictionary of RADIUS VSAs

ACS supports Cisco IOS/PIX 6.0 vendor-specific attributes (VSAs). The vendor ID for this Cisco RADIUS Implementation is 9.

Table C-2 lists the supported Cisco IOS/PIX 6.0 RADIUS VSAs.

Note For a discussion of the Cisco IOS/PIX 6.0 RADIUS `cisco-av-pair` attribute, see About the cisco-av-pair RADIUS Attribute, page C-5.

Note For details about the Cisco IOS H.323 VSAs, refer to Cisco IOS Voice-over-IP (VoIP) documentation.

Note For details about the Cisco IOS Node Route Processor-Service Selection Gateway VSAs (VSAs 250, 251, and 252), refer to Cisco IOS documentation.

Table C-2 Cisco IOS/PIX 6.0 RADIUS VSAs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
1	cisco-av-pair	String	Both	Yes
2	cisco-nas-port	String	Inbound	No
23	cisco-h323-remote-address	String	Inbound	No
24	cisco-h323-conf-id	String	Inbound	No

Table C-2 Cisco IOS/PIX 6.0 RADIUS VSAs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
25	cisco-h323-setup-time	String	Inbound	No
26	cisco-h323-call-origin	String	Inbound	No
27	cisco-h323-call-type	String	Inbound	No
28	cisco-h323-connect-time	String	Inbound	No
29	cisco-h323-disconnect-time	String	Inbound	No
30	cisco-h323-disconnect-cause	String	Inbound	No
31	cisco-h323-voice-quality	String	Inbound	No
33	cisco-h323-gw-id	String	Inbound	No
35	cisco-h323-incoming-conn-id	String	Inbound	No
101	cisco-h323-credit-amount	String (maximum length 247 characters)	Outbound	No
102	cisco-h323-credit-time	String (maximum length 247 characters)	Outbound	No
103	cisco-h323-return-code	String (maximum length 247 characters)	Outbound	No
104	cisco-h323-prompt-id	String (maximum length 247 characters)	Outbound	No
105	cisco-h323-day-and-time	String (maximum length 247 characters)	Outbound	No
106	cisco-h323-redirect-number	String (maximum length 247 characters)	Outbound	No
107	cisco-h323-preferred-lang	String (maximum length 247 characters)	Outbound	No
108	cisco-h323-redirect-ip-addr	String (maximum length 247 characters)	Outbound	No
109	cisco-h323-billing-model	String (maximum length 247 characters)	Outbound	No
110	cisco-h323-currency	String (maximum length 247 characters)	Outbound	No
250	cisco-ssg-account-info	String (maximum length 247 characters)	Outbound	No
251	cisco-ssg-service-info	String (maximum length 247 characters)	Both	No
253	cisco-ssg-control-info	String (maximum length 247 characters)	Both	No

About the cisco-av-pair RADIUS Attribute

The first attribute in the Cisco IOS/PIX 6.0 RADIUS implementation, `cisco-av-pair`, supports the inclusion of many AV pairs by using the following format:

attribute sep value

where *attribute* and *value* are an AV pair supported by the releases of IOS implemented on your AAA clients, and *sep* is **=** for mandatory attributes and asterisk (*) for optional attributes. You can then use the full set of Terminal Access Controller Access Control System (TACACS+) authorization features for RADIUS.

Note The attribute name in an AV pair is case sensitive. Typically, attribute names are all in lowercase letters.

The following is an example of two AV pairs included in a single Cisco IOS/PIX 6.0 RADIUS `cisco-av-pair` attribute:

```
ip:addr-pool=first
shell:priv-lvl=15
```

The first example activates the Cisco multiple named IP address pools feature during IP authorization (during PPP IPCP address assignment). The second example immediately grants access to a user of a device-hosted administrative session to **EXEC** commands.

In IOS, support for Network Admission Control (NAC) includes the use of the following AV pairs:

- **url-redirect**—Enables the AAA client to intercept an HTTP request and redirect it to a new URL. This pair is especially useful if the result of posture validation indicates that the NAC-client computer requires an update or patch that you have made available on a remediation web server. For example, a user can be redirected to a remediation web server to download and apply a new virus DAT file or an operating system patch. For example:

  ```
  url-redirect=http://10.1.1.1
  ```

- **posture-token**—Enables ACS to send a text version of a system posture token (SPT) derived by posture validation. The SPT is always sent in numeric format and using the posture-token AV pair renders the result of a posture validation request more easily read on the AAA client. For example:

  ```
  posture-token=Healthy
  ```

Caution The posture-token AV pair is the only way that ACS notifies the AAA client of the SPT that posture validation returns. Because you manually configure the posture-token AV pair, errors in configuring the posture-token can cause the incorrect system posture token to be sent to the AAA client or; if the AV pair name is mistyped, the AAA client will not receive the system posture token at all.

  For a list of valid SPTs, see Posture Tokens, page 14-3.

- **status-query-timeout**—Overrides the status-query default value of the AAA client with the value that you specify, in seconds. For example:

  ```
  status-query-timeout=150
  ```

For more information about AV pairs that IOS supports, refer to the documentation for the releases of IOS implemented on your AAA clients.

Cisco VPN 3000 Concentrator/ASA/PIX 7.x+ Dictionary of RADIUS VSAs

ACS supports Cisco VPN 3000/ASA/PIX 7.x+ RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 3076.

Note Some of the RADIUS VSAs supported by Cisco virtual private network (VPN) 3000 Concentrators, Adaptive Security Appliance (ASA), and Project Information Exchange (PIX) 7.x+ appliances are interdependent. Before you implement them, we recommend that you refer to your respective device documentation.

For example, to control Microsoft Point-to-Point Encryption (MPPE) settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

Table C-3 lists the supported Cisco VPN 3000 Concentrator RADIUS VSAs.

Table C-3 Cisco VPN 3000 Concentrator /ASA/PIX 7.x+ RADIUS VSAs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
1	CVPN3000-Access-Hours	String (maximum length 247 characters)	Outbound	No
2	CVPN3000-Simultaneous-Logins	Integer (maximum length 10 characters)	Outbound	No
5	CVPN3000-Primary-DNS	Ipaddr (maximum length 15 characters)	Outbound	No
6	CVPN3000-Secondary-DNS	Ipaddr (maximum length 15 characters)	Outbound	No
7	CVPN3000-Primary-WINS	Ipaddr (maximum length 15 characters)	Outbound	No
8	CVPN3000-Secondary-WINS	Ipaddr (maximum length 15 characters)	Outbound	No
9	CVPN3000-SEP-Card-Assignment	Integer	Outbound	No
11	CVPN3000-Tunneling-Protocols	Integer	Outbound	No
12	CVPN3000-IPSec-Sec-Association	String (maximum length 247 characters)	Outbound	No
13	CVPN3000-IPSec-Authentication	Integer	Outbound	No
15	CVPN3000-IPSec-Banner1	String (maximum length 247 characters)	Outbound	No
16	CVPN3000-IPSec-Allow-Passwd-Store	Integer	Outbound	No
17	CVPN3000-Use-Client-Address	Integer	Outbound	No
20	CVPN3000-PPTP-Encryption	Integer	Outbound	No
21	CVPN3000-L2TP-Encryption	Integer	Outbound	No
27	CVPN3000-IPSec-Split-Tunnel-List	String (maximum length 247 characters)	Outbound	No
28	CVPN3000-IPSec-Default-Domain	String (maximum length 247 characters)	Outbound	No
29	CVPN3000-IPSec-Split-DNS-Names	String (maximum length 247 characters)	Outbound	No
30	CVPN3000-IPSec-Tunnel-Type	Integer	Outbound	No
31	CVPN3000-IPSec-Mode-Config	Integer	Outbound	No
33	CVPN3000-IPSec-User-Group-Lock	Integer	Outbound	No
34	CVPN3000-IPSec-Over-UDP	Integer	Outbound	No
35	CVPN3000-IPSec-Over-UDP-Port	Integer (maximum length 10 characters)	Outbound	No
36	CVPN3000-IPSec-Banner2	String (maximum length 247 characters)	Outbound	No
37	CVPN3000-PPTP-MPPC-Compression	Integer	Outbound	No
38	CVPN3000-L2TP-MPPC-Compression	Integer	Outbound	No
39	CVPN3000-IPSec-IP-Compression	Integer	Outbound	No
40	CVPN3000-IPSec-IKE-Peer-ID-Check	Integer	Outbound	No
41	CVPN3000-IKE-Keep-Alives	Integer	Outbound	No

Table C-3 Cisco VPN 3000 Concentrator /ASA/PIX 7.x+ RADIUS VSAs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
42	CVPN3000-IPSec-Auth-On-Rekey	Integer	Outbound	No
45	CVPN3000-Required-Client-Firewall-Vendor-Code	Integer (maximum length 10 characters)	Outbound	No
46	CVPN3000-Required-Client-Firewall-Product-Code	Integer (maximum length 10 characters)	Outbound	No
47	CVPN3000-Required-Client-Firewall-Description	String (maximum length 247 characters)	Outbound	No
48	CVPN3000-Require-HW-Client-Auth	Integer	Outbound	No
49	CVPN3000-Require-Individual-User-Auth	Integer	Outbound	No
50	CVPN3000-Authenticated-User-Idle-Timeout	Integer (maximum length 10 characters)	Outbound	No
51	CVPN3000-Cisco-IP-Phone-Bypass	Integer	Outbound	No
52	CVPN3000-User-Auth-Server-Name	String (maximum length 247 characters)	Outbound	No
53	CVPN3000-User-Auth-Server-Port	Integer (maximum length 10 characters)	Outbound	No
54	CVPN3000-User-Auth-Server-Secret	String (maximum length 247 characters)	Outbound	No
55	CVPN3000-IPSec-Split-Tunneling-Policy	Integer	Outbound	No
56	CVPN3000-IPSec-Required-Client-Firewall-Capability	Integer	Outbound	No
57	CVPN3000-IPSec-Client-Firewall-Filter-Name	String (maximum length 247 characters)	Outbound	No
58	CVPN3000-IPSec-Client-Firewall-Filter-Optional	Integer	Outbound	No
59	CVPN3000-IPSec-Backup-Servers	Integer	Outbound	No
60	CVPN3000-IPSec-Backup-Server-List	String (maximum length 247 characters)	Outbound	No
62	CVPN3000-MS-Client-Intercept-DHCP-Configure-Message	Integer	Outbound	No
63	CVPN3000-MS-Client-Subnet-Mask	Ipaddr (maximum length 15 characters)	Outbound	No
64	CVPN3000-Allow-Network-Extension-Mode	Integer	Outbound	No
65	Authorization-Type	Integer	Outbound	No
66	Authorization-Required	Integer	Outbound	No
67	Authorization-DN-Field	String	Outbound	No
68	IKE-Keepalive-Confidence-Interval	Integer	Outbound	No
69	WebVPN-Content-Filter-Parameters	Integer	Outbound	No
75	Cisco-LEAP-Bypass	Integer	Outbound	No
77	Client-Type-Version-Limiting	String	Outbound	No
79	WebVPN-Port-Forwarding-Name	String	Outbound	No

Table C-3 Cisco VPN 3000 Concentrator /ASA/PIX 7.x+ RADIUS VSAs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
80	IE-Proxy-Server	String	Outbound	No
81	IE-Proxy-Server-Policy	Integer	Outbound	No
82	IE-Proxy-Exception-List	String	Outbound	No
83	IE-Proxy-Bypass-Local	Integer	Outbound	No
84	IKE-Keepalive-Retry-Interval	Integer	Outbound	No
85	Tunnel-Group-Lock	String	Outbound	No
86	Access-List-Inbound	String	Outbound	No
87	Access-List-Outbound	String	Outbound	No
88	Perfect-Forward-Secrecy-Enable	Integer	Outbound	No
89	NAC-Enable	Integer	Outbound	No
90	NAC-Status-Query-Timer	Integer	Outbound	No
91	NAC-Revalidation-Timer	Integer	Outbound	No
92	NAC-Default-ACL	Integer	Outbound	No
93	WebVPN-URL-Entry-Enable	Integer	Outbound	No
94	WebVPN-File-Access-Enable	Integer	Outbound	No
95	WebVPN-File-Server-Entry-Enable	Integer	Outbound	No
96	WebVPN-File-Server-Browsing-Enable	Integer	Outbound	No
97	WebVPN-Port-Forwarding-Enable	Integer	Outbound	No
98	WebVPN-Outlook-Exchange-Proxy-Enable	Integer	Outbound	No
98	WebVPN-Port-Forwarding-HTTP-Proxy	Integer	Outbound	No
99	WebVPN-Outlook-Exchange-Proxy-Enable	Integer	Outbound	No
100	WebVPN-Auto-Applet-Download-Enable	Integer	Outbound	No
101	WebVPN-Citrix-MetaFrame-Enable	Integer	Outbound	No
102	WebVPN-Apply-ACL	Integer	Outbound	No
103	WebVPN-SSL-VPN-Client-Enable	Integer	Outbound	No
104	WebVPN-SSL-VPN-Client-Required	Integer	Outbound	No
105	WebVPN-SSL-VPN-Client-Keep-Installation	Integer	Outbound	No
135	CVPN3000-Strip-Realm	Integer	Outbound	No

Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs

ACS supports the Cisco VPN 5000 RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 255. Table C-4 lists the supported Cisco VPN 5000 Concentrator RADIUS VSAs.

Table C-4 Cisco VPN 5000 Concentrator RADIUS VSAs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
001	CVPN5000-Tunnel-Throughput	Integer	Inbound	No
002	CVPN5000-Client-Assigned-IP	String	Inbound	No
003	CVPN5000-Client-Real-IP	String	Inbound	No
004	CVPN5000-VPN-GroupInfo	String (maximum length 247 characters)	Outbound	No
005	CVPN5000-VPN-Password	String (maximum length 247 characters)	Outbound	No
006	CVPN5000-Echo	Integer	Inbound	No
007	CVPN5000-Client-Assigned-IPX	Integer	Inbound	No

Cisco Building Broadband Service Manager Dictionary of RADIUS VSA

ACS supports a Cisco Building Broadband Service Manager (BBSM) RADIUS VSA. The vendor ID for this Cisco RADIUS Implementation is 5263.

Table C-5 lists the supported Cisco BBSM RADIUS VSA.

Table C-5 Cisco BBSM RADIUS VSA

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
001	CBBSM-Bandwidth	Integer	Both	No

Cisco Airespace Dictionary of RADIUS VSA

Table C-6 lists the supported RADIUS (Cisco Airespace) attributes. In addition to these attributes, Cisco Airespace devices support some IETF attributes for 802.1x identity networking:

- Tunnel-Type (64)
- Tunnel-Medium-Type (65)
- Tunnel-Private-Group-Id (81)

ACS cannot offer partial support of IETF; hence, adding an Cisco Airespace device (into the Network Configuration) will automatically enable all IETF attributes.

Table C-6 Cisco Airespace RADIUS Attributes

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
1	Aire-WLAN-Id	Name of the user being authenticated.	Integer	Outbound	No
2	Aire-QoS-Level	Enumerations: 0: Bronze 1: Silver 2: Gold 3: Platinum 4: Uranium	Integer	Outbound	No
3	Aire-DSCP	—	Integer	Outbound	No
4	Aire-802.1P-Tag	—	Integer	Outbound	No
5	Aire-Interface-Name	—	String	Outbound	No
6	Aire-ACL-Name	—	String	Outbound	No

IETF Dictionary of RADIUS IETF (AV Pairs)

Table C-7 lists the supported RADIUS (IETF) attributes. If the attribute has a security server-specific format, the format is specified.

Table C-7 RADIUS (IETF) Attributes

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
1	User-Name	Name of the user being authenticated.	String	Inbound	No
2	User-Password	User password or input following an access challenge. Passwords longer than 16 characters are encrypted by using IETF Draft #2 or later specifications.	String	Outbound	No
3	CHAP-Password	PPP (Point-to-Point Protocol) Challenge Handshake Authentication Protocol (CHAP) response to an Access-Challenge.	String	Outbound	No
4	NAS-IP Address	IP address of the AAA client that is requesting authentication.	Ipaddr	Inbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
5	NAS-Port	Physical port number of the AAA client that is authenticating the user. The AAA client port value (32 bits) comprises one or two 16-bit values, depending on the setting of the RADIUS server extended **portnames** command. Each 16-bit number is a 5-digit decimal integer interpreted as: • Asynchronous terminal lines, async network interfaces, and virtual async interfaces, the value is `00`*ttt*, where *ttt* is the line number or async interface unit number. • Ordinary synchronous network interfaces, the value is `10xxx`. • Channels on a primary-rate ISDN (Integrated Services Digital Network) interface, the value is `2ppcc`. • Channels on a basic rate ISDN interface, the value is `3bb0c`. • Other types of interfaces, the value is `6nnss`.	Integer	Inbound	No
6	Service-Type	Type of service requested or type of service to be provided: • In a request: – **Framed**—For a known Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP) connection. – **Administrative User**—For **enable** command. • In a response: – **Login**—Make a connection. – **Framed**—Start SLIP or PPP. – **Administrative User**—Start an EXEC or **enable ok**. – **Exec User**—Start an EXEC session.	Integer	Both	No
7	Framed-Protocol	Framing to be used for framed access.	Integer	Both	No
8	Framed-IP-Address	Address to be configured for the user.	—	—	—
9	Framed-IP-Netmask	IP netmask to be configured for the user when the user is a router to a network. This AV causes a static route to be added for Framed-IP-Address with the mask specified.	Ipaddr (maximum length 15 characters)	Outbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
10	Framed-Routing	Routing method for the user when the user is a router to a network. Only None and Send and Listen values are supported for this attribute.	Integer	Outbound	No
11	Filter-Id	Name of the filter list for the user, formatted: *%d*, *%d.in*, or *%d.out*. This attribute is associated with the most recent service-type command. For **login** and **EXEC**, use *%d* or *%d.out* as the line access list value from 0 to 199. For Framed service, use *%d* or *%d.out* as interface output access list and *%d.in* for input access list. The numbers are self-encoding to the protocol to which they refer.	String	Outbound	Yes
12	Framed-MTU	Indicates the maximum transmission unit (MTU) that you can configure for the user when the MTU is not negotiated by PPP or some other means.	Integer (maximum length 10 characters)	Outbound	No
13	Framed-Compression	Compression protocol used for the link. This attribute results in **/compress** being added to the PPP or SLIP autocommand generated during EXEC authorization. Not currently implemented for non-EXEC authorization.	Integer	Outbound	Yes
14	Login-IP-Host	Host to which the user will connect when the `Login-Service` attribute is included.	Ipaddr (maximum length 15 characters)	Both	Yes
15	Login-Service	Service that you should use to connect the user to the login host. Service is indicated by a numeric value: 0: Telnet 1: Rlogin 2: TCP-Clear 3: PortMaster 4: LAT	Integer	Both	No
16	Login-TCP-Port	Transmission Control Protocol (TCP) port with which to connect the user when the Login-Service attribute is also present.	Integer (maximum length 10 characters)	Outbound	No
18	Reply-Message	Text that the user will see.	String	Outbound	Yes
19	Callback-Number	—	String	Outbound	No
20	Callback-Id	—	String	Outbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
22	Framed-Route	Routing information to configure for the user on this AAA client. The RADIUS RFC (Request for Comments) format (net/bits [router [metric]]) and the old style dotted mask (net mask [router [metric]]) are supported. If the router field is omitted or zero (0), the peer IP address is used. Metrics are ignored.	String	Outbound	Yes
23	Framed-IPX-Network	—	Integer	Outbound	No
24	State	Allows State information to be maintained between the AAA client and the RADIUS server. This attribute is applicable only to CHAP challenges.	String (maximum length 253 characters)	Outbound	No
25	Class	Arbitrary value that the AAA client includes in all accounting packets for this user if supplied by the RADIUS server.	String	Both	Yes
26	Vendor-Specific	Carries subattributes known as vendor-specific attributes (VSAs), a feature of RADIUS that allows vendors to support their own extended attributes. Subattributes are identified by IANA-assigned vendor numbers in combination with the vendor-assigned subattribute number. For example, the vendor number for Cisco IOS/PIX 6.0 RADIUS is 9. The `cisco-av-pair` VSA is attribute 1 in the set of VSAs related to vendor number 9.	String	Outbound	Yes
27	Session-Timeout	Maximum number of seconds of service to provide to the user before the session terminates. This AV becomes the per-user absolute timeout. This attribute is not valid for PPP sessions.	Integer (maximum length 10 characters)	Outbound	No
28	Idle-Timeout	Maximum number of consecutive seconds of idle connection time that the user is allowed before the session terminates. This AV becomes the per-user session-timeout. This attribute is not valid for PPP sessions.	Integer (maximum length 10 characters)	Outbound	No
29	Termination-Action	Indicates what action the NAS should take when the specified service is completed. It is only used in Access-Accept packets. If the Value is set to RADIUS-Request (1), upon termination of the specified service, the NAS may send a new Access-Request to the RADIUS server, including the State attribute if any.	Integer	Both	No
30	Called-Station-Id	Allows the AAA client to send the telephone number or other information identifying the AAA client as part of the access-request packet by using automatic number identification or similar technology. Different devices provide different identifiers.	String	Inbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
31	Calling-Station-Id	Allows the AAA client to send the telephone number or other information identifying the end-user client as part of the access-request packet by using Dialed Number Identification Server (DNIS) or similar technology. For example, Cisco Aironet Access Points usually send the MAC address of the end-user client.	String	Inbound	No
32	NAS-Identifier	—	String	Inbound	No
33	Proxy-State	Included in proxied RADIUS requests per RADIUS standards. The operation of ACS does not depend on the contents of this attribute.	String (maximum length 253 characters)	Inbound	No
34	Login-LAT-Service	System with which the local area transport (LAT) protocol connects the user. This attribute is only available in the EXEC mode.	String (maximum length 253 characters)	Inbound	No
35	Login-LAT-Node	—	String	Inbound	No
36	Login-LAT-Group	—	String	Inbound	No
37	Framed-AppleTalk-Link	—	Integer	Outbound	No
38	Framed-AppleTalk-Network	—	Integer	Outbound	Yes
39	Framed-AppleTalk-Zone	—	String	Out	No
40	Acct-Status-Type	Specifies whether this accounting-request marks the beginning of the user service (start) or the end (stop).	Integer	Inbound	No
41	Acct-Delay-Time	Number of seconds the client has been trying to send a particular record.	Integer	Inbound	No
42	Acct-Input-Octets	Number of octets received from the port while this service is being provided.	Integer	Inbound	No
43	Acct-Output-Octets	Number of octets sent to the port while this service is being delivered.	Integer	Inbound	No
44	Acct-Session-Id	Unique accounting identifier that makes it easy to match start and stop records in a log file. The `Acct-Session-Id` restarts at 1 each time the router is power cycled or the software is reloaded. Contact Cisco support if this interval is unsuitable.	String	Inbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
44	Acct-Authentic	Way in which the user was authenticated—by RADIUS, the AAA client itself, or another remote authentication protocol. This attribute is set to **radius** for users who are authenticated by RADIUS; to **remote** for TACACS+ and Kerberos; or to **local** for local, enable, line, and if-needed methods. For all other methods, the attribute is omitted.	Integer	Inbound	No
46	Acct-Session-Time	Number of seconds the user has been receiving service.	Integer	Inbound	No
47	Acct-Input-Packets	Number of packets received from the port while this service is being provided to a framed user.	Integer	Inbound	No
48	Acct-Output-Packets	Number of packets sent to the port while this service is being delivered to a framed user.	Integer	Inbound	No
49	Acct-Terminate-Cause	Reports details on why the connection was terminated. Termination causes are indicated by a numeric value: 1: User request 2: Lost carrier 3: Lost service 4: Idle timeout 5: Session-timeout 6: Admin reset 7: Admin reboot 8: Port error 9: AAA client error 10: AAA client request 11: AAA client reboot 12: Port unneeded 13: Port pre-empted 14: Port suspended 15: Service unavailable 16: Callback 17: User error 18: Host request	Integer	Inbound	No
50	Acct-Multi-Session-Id	—	String	Inbound	No
51	Acct-Link-Count	—	Integer	Inbound	No
52	Acct-Input-Gigawords	—	Integer	Inbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
53	Acct-Output-Gigawords	—	Integer	Inbound	No
55	Event-Timestamp	—	Date	Inbound	No
60	CHAP-Challenge	—	String	Inbound	No
61	NAS-Port-Type	Indicates the type of physical port the AAA client is using to authenticate the user. Physical ports are indicated by a numeric value: 0: Asynchronous 1: Synchronous 2: ISDN-Synchronous 3: ISDN-Asynchronous (V.120) 4: ISDN- Asynchronous (V.110) 5: Virtual	Integer	Inbound	No
62	Port-Limit	Sets the maximum number of ports to be provided to the user by the network-access server.	Integer (maximum length 10 characters)	Both	No
63	Login-LAT-Port	—	String	Both	No
64	Tunnel-Type	—	Tagged integer	Both	Yes
65	Tunnel-Medium-Type	—	Tagged integer	Both	Yes
66	Tunnel-Client-Endpoint	—	Tagged string	Both	Yes
67	Tunnel-Server-Endpoint	—	Tagged string	Both	Yes
68	Acct-Tunnel-Connection	—	String	Inbound	No
69	Tunnel-Password	—	Tagged string	Both	Yes
70	ARAP-Password	—	String	Inbound	No
71	ARAP-Features	—	String	Outbound	No
72	ARAP-Zone-Access	—	Integer	Outbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
73	ARAP-Security	—	Integer	Inbound	No
74	ARAP-Security-Data	—	String	Inbound	No
75	Password-Retry	—	Integer	Internal use only	No
76	Prompt	—	Integer	Internal use only	No
77	Connect-Info	—	String	Inbound	No
78	Configuration-Token	—	String	Internal use only	No
79	EAP-Message	—	String	Internal use only	No
80	Message-Authenticator	—	String	Outbound	No
81	Tunnel-Private-Group-ID	—	Tagged string	Both	Yes
82	Tunnel-Assignment-ID	—	Tagged string	Both	Yes
83	Tunnel-Preference	—	Tagged integer	Both	No
85	Acct-Interim-Interval	—	Integer	Outbound	No
87	NAS-Port-Id	—	String	Inbound	No
88	Framed-Pool	—	String	Internal use only	No
90	Tunnel-Client-Auth-ID	—	Tagged string	Both	Yes
91	Tunnel-Server-Auth-ID	—	Tagged string	Both	Yes
135	Primary-DNS-Server	—	Ipaddr	Both	No
136	Secondary-DNS-Server	—	Ipaddr	Both	No
187	Multilink-ID	—	Integer	Inbound	No
188	Num-In-Multilink	—	Integer	Inbound	No
190	Pre-Input-Octets	—	Integer	Inbound	No

Table C-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
191	Pre-Output-Octets	—	Integer	Inbound	No
192	Pre-Input-Packets	—	Integer	Inbound	No
193	Pre-Output-Packets	—	Integer	Inbound	No
194	Maximum-Time	—	Integer	Both	No
195	Disconnect-Cause	—	Integer	Inbound	No
197	Data-Rate	—	Integer	Inbound	No
198	PreSession-Time	—	Integer	Inbound	No
208	PW-Lifetime	—	Integer	Outbound	No
209	IP-Direct	—	Ipaddr	Outbound	No
210	PPP-VJ-Slot-Comp	—	Integer	Outbound	No
218	Assign-IP-pool	—	Integer	Outbound	No
228	Route-IP	—	Integer	Outbound	No
233	Link-Compression	—	Integer	Outbound	No
234	Target-Utils	—	Integer	Outbound	No
235	Maximum-Channels	—	Integer	Outbound	No
242	Data-Filter	—	Ascend filter	Outbound	Yes
243	Call-Filter	—	Ascend filter	Outbound	Yes
244	Idle-Limit	—	Integer	Outbound	No

Microsoft MPPE Dictionary of RADIUS VSAs

ACS supports the Microsoft RADIUS VSAs used for MPPE. The vendor ID for this Microsoft RADIUS Implementation is 311. MPPE is an encryption technology developed by Microsoft to encrypt PPP links. These PPP connections can be via a dial-up line, or over a VPN tunnel such as PPTP. MPPE is supported by several RADIUS network device vendors that ACS supports. The following ACS RADIUS protocols support the Microsoft RADIUS VSAs:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+

- Ascend
- Cisco Airespace

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

Table C-8 lists the supported MPPE RADIUS VSAs.

Table C-8 Microsoft MPPE RADIUS VSAs

Number	Attribute	Type of Value	Description	Inbound/ Outbound	Multiple
1	MS-CHAP-Response	String	—	Inbound	No
2	MS-CHAP-Error	String	—	Outbound	No
3	MS-CHAP-CPW-1	String	—	Inbound	No
4	MS-CHAP-CPW-2	String	—	Inbound	No
5	MS-CHAP-LM-Enc-PW	String	—	Inbound	No
6	MS-CHAP-NT-Enc-PW	String	—	Inbound	No
7	MS-MPPE-Encryption-Policy	Integer	The MS-MPPE-Encryption-Policy attribute signifies whether the use of encryption is allowed or required. If the Policy field is equal to 1 (Encryption-Allowed), you can use any or none of the encryption types specified in the MS-MPPE-Encryption-Types attribute. If the Policy field is equal to 2 (Encryption-Required), you can use any of the encryption types specified in the MS-MPPE-Encryption-Types attribute; but at least one must be used.	Outbound	No
8	MS-MPPE-Encryption-Types	Integer	The MS-MPPE-Encryption-Types attribute signifies the types of encryption available for use with MPPE. It is a four-octet integer that is interpreted as a string of bits.	Outbound	No
10	MS-CHAP-Domain	String	—	Inbound	No
11	MS-CHAP-Challenge	String	—	Inbound	No

Table C-8 Microsoft MPPE RADIUS VSAs (continued)

Number	Attribute	Type of Value	Description	Inbound/ Outbound	Multiple
12	MS-CHAP-MPPE-Keys	String	The MS-CHAP-MPPE-Keys attribute contains two session keys for use by the MPPE. This attribute is only included in Access-Accept packets. **Note** ACS auto generates the MS-CHAP-MPPE-Keys attribute value; there is no value to set in the web interface.	Outbound	No
16	MS-MPPE-Send-Key	String (maximum length 240 characters)	The MS-MPPE-Send-Key attribute contains a session key for use by MPPE. This key is for encrypting packets sent from the AAA client to the remote host. This attribute is only included in Access-Accept packets.	Outbound	No
17	MS-MPPE-Recv-Key	String (maximum length 240 characters)	The MS-MPPE-Recv-Key attribute contains a session key for use by MPPE. This key is for encrypting packets that the AAA client from the remote host receives. This attribute is only included in Access-Accept packets.	Outbound	No
18	MS-RAS-Version	String	—	Inbound	No
25	MS-CHAP-NT-Enc-PW	String	—	Inbound	No
26	MS-CHAP2-Response	String	—	Outbound	No
27	MS-CHAP2-CPW	String	—	Inbound	No

Ascend Dictionary of RADIUS AV Pairs

ACS supports the Ascend RADIUS AV pairs. Table C-9 contains Ascend RADIUS dictionary translations for parsing requests and generating responses. All transactions comprise AV pairs. The value of each attribute is specified as:

- **String**—0-253 octets.
- **Abinary**—0-254 octets.
- **Ipaddr**—4 octets in network byte order.
- **Integer**—32-bit value in big endian order (high byte first).
- **Call filter**—Defines a call filter for the profile.

Note RADIUS filters are retrieved only when a call is placed by using a RADIUS outgoing profile or answered by using a RADIUS incoming profile. Filter entries are applied in the order in which they are entered. If you change a filter in an Ascend RADIUS profile, the changes do not take effect until a call uses that profile.

- **Date**—32-bit value in big-endian order. For example, seconds since 00:00:00 universal time (UT), January 1, 1970.

- **Enum**—Enumerated values are stored in the user file with dictionary value translations for easy administration.

Table C-9 Ascend RADIUS Attributes

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
Dictionary of Ascend Attributes				
1	User-Name	String	Inbound	No
2	User-Password	String	Outbound	No
3	CHAP-Password	String	Outbound	No
4	NAS-IP-Address	Ipaddr	Inbound	No
5	NAS-Port	Integer	Inbound	No
6	Service-Type	Integer	Both	No
7	Framed-Protocol	Integer	Both	No
8	Framed-IP-Address	Ipaddr	Both	No
9	Framed-IP-Netmask	Ipaddr	Outbound	No
10	Framed-Routing	Integer	Outbound	No
11	Framed-Filter	String	Outbound	Yes
12	Framed-MTU	Integer	Outbound	No
13	Framed-Compression	Integer	Outbound	Yes
14	Login-IP-Host	Ipaddr	Both	Yes
15	Login-Service	Integer	Both	No
16	Login-TCP-Port	Integer	Outbound	No
17	Change-Password	String	—	—
18	Reply-Message	String	Outbound	Yes
19	Callback-ID	String	Outbound	No
20	Callback-Name	String	Outbound	No
22	Framed-Route	String	Outbound	Yes
23	Framed-IPX-Network	Integer	Outbound	No
24	State	String	Outbound	No
25	Class	String	Outbound	Yes
26	Vendor-Specific	String	Outbound	Yes
30	Call-Station-ID	String	Inbound	No
31	Calling-Station-ID	String	Inbound	No
40	Acct-Status-Type	Integer	Inbound	No
41	Acct-Delay-Time	Integer	Inbound	No
42	Acct-Input-Octets	Integer	Inbound	No
43	Acct-Output-Octets	Integer	Inbound	No
44	Acct-Session-Id	Integer	Inbound	No

Table C-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
45	Acct-Authentic	Integer	Inbound	No
46	Acct-Session-Time	Integer	Inbound	No
47	Acct-Input-Packets	Integer	Inbound	No
48	Acct-Output-Packets	Integer	Inbound	No
64	Tunnel-Type	String	Both	Yes
65	Tunnel-Medium-Type	String	Both	Yes
66	Tunnel-Client-Endpoint	String (maximum length 250 characters)	Both	Yes
67	Tunnel-Server-Endpoint	String (maximum length 250 characters)	Both	Yes
68	Acct-Tunnel-Connection	Integer (maximum length 253 characters)	Inbound	No
104	Ascend-Private-Route	String (maximum length 253 characters)	Both	No
105	Ascend-Numbering-Plan-ID	Integer (maximum length 10 characters)	Both	No
106	Ascend-FR-Link-Status-Dlci	Integer (maximum length 10 characters)	Both	No
107	Ascend-Calling-Subaddress	String (maximum length 253 characters)	Both	No
108	Ascend-Callback-Delay	String (maximum length 10 characters)	Both	No
109	Ascend-Endpoint-Disc	String (maximum length 253 characters)	Both	No
110	Ascend-Remote-FW	String (maximum length 253 characters)	Both	No
111	Ascend-Multicast-GLeave-Delay	Integer (maximum length 10 characters)	Both	No
112	Ascend-CBCP-Enable	String	Both	No
113	Ascend-CBCP-Mode	String	Both	No
114	Ascend-CBCP-Delay	String (maximum length 10 characters)	Both	No
115	Ascend-CBCP-Trunk-Group	String (maximum length 10 characters)	Both	No
116	Ascend-AppleTalk-Route	String (maximum length 253 characters)	Both	No
117	Ascend-AppleTalk-Peer-Mode	String (maximum length 10 characters)	Both	No
118	Ascend-Route-AppleTalk	String (maximum length 10 characters)	Both	No
119	Ascend-FCP-Parameter	String (maximum length 253 characters)	Both	No
120	Ascend-Modem-PortNo	Integer (maximum length 10 characters)	Inbound	No
121	Ascend-Modem-SlotNo	Integer (maximum length 10 characters)	Inbound	No
122	Ascend-Modem-ShelfNo	Integer (maximum length 10 characters)	Inbound	No
123	Ascend-Call-Attempt-Limit	Integer (maximum length 10 characters)	Both	No
124	Ascend-Call-Block_Duration	Integer (maximum length 10 characters)	Both	No
125	Ascend-Maximum-Call-Duration	Integer (maximum length 10 characters)	Both	No
126	Ascend-Router-Preference	String (maximum length 10 characters)	Both	No
127	Ascend-Tunneling-Protocol	String (maximum length 10 characters)	Both	No
128	Ascend-Shared-Profile-Enable	Integer	Both	No
129	Ascend-Primary-Home-Agent	String (maximum length 253 characters)	Both	No

Table C-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
130	Ascend-Secondary-Home-Agent	String (maximum length 253 characters)	Both	No
131	Ascend-Dialout-Allowed	Integer	Both	No
133	Ascend-BACP-Enable	Integer	Both	No
134	Ascend-DHCP-Maximum-Leases	Integer (maximum length 10 characters)	Both	No
135	Ascend-Client-Primary-DNS	Address (maximum length 15 characters)	Both	No
136	Ascend-Client-Secondary-DNS	Address (maximum length 15 characters)	Both	No
137	Ascend-Client-Assign-DNS	Enum	Both	No
138	Ascend-User-Acct-Type	Enum	Both	No
139	Ascend-User-Acct-Host	Address (maximum length 15 characters)	Both	No
140	Ascend-User-Acct-Port	Integer (maximum length 10 characters)	Both	No
141	Ascend-User-Acct-Key	String (maximum length 253 characters)	Both	No
142	Ascend-User-Acct-Base	Enum (maximum length 10 characters)	Both	No
143	Ascend-User-Acct-Time	Integer (maximum length 10 characters)	Both	No
Support IP Address Allocation from Global Pools				
144	Ascend-Assign-IP-Client	Ipaddr (maximum length 15 characters)	Outbound	No
145	Ascend-Assign-IP-Server	Ipaddr (maximum length 15 characters)	Outbound	No
146	Ascend-Assign-IP-Global-Pool	String (maximum length 253 characters)	Outbound	No
DHCP Server Functions				
147	Ascend-DHCP-Reply	Integer	Outbound	No
148	Ascend-DHCP-Pool-Number	Integer (maximum length 10 characters)	Outbound	No
Connection Profile/Telco Option				
149	Ascend-Expect-Callback	Integer	Outbound	No
Event Type for an Ascend-Event Packet				
150	Ascend-Event-Type	Integer (maximum length 10 characters)	Inbound	No
RADIUS Server Session Key				
151	Ascend-Session-Svr-Key	String (maximum length 253 characters)	Outbound	No
Multicast Rate Limit Per Client				
152	Ascend-Multicast-Rate-Limit	Integer (maximum length 10 characters)	Outbound	No
Connection Profile Fields to Support Interface-Based Routing				
153	Ascend-IF-Netmask	Ipaddr (maximum length 15 characters)	Outbound	No
154	Ascend-Remote-Addr	Ipaddr (maximum length 15 characters)	Outbound	No
Multicast Support				
155	Ascend-Multicast-Client	Integer (maximum length 10 characters)	Outbound	No
Frame Datalink Profiles				
156	Ascend-FR-Circuit-Name	String (maximum length 253 characters)	Outbound	No

Table C-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
157	Ascend-FR-LinkUp	Integer (maximum length 10 characters)	Outbound	No
158	Ascend-FR-Nailed-Group	Integer (maximum length 10 characters)	Outbound	No
159	Ascend-FR-Type	Integer (maximum length 10 characters)	Outbound	No
160	Ascend-FR-Link-Mgt	Integer (maximum length 10 characters)	Outbound	No
161	Ascend-FR-N391	Integer (maximum length 10 characters)	Outbound	No
162	Ascend-FR-DCE-N392	Integer (maximum length 10 characters)	Outbound	No
163	Ascend-FR-DTE-N392	Integer (maximum length 10 characters)	Outbound	No
164	Ascend-FR-DCE-N393	Integer (maximum length 10 characters)	Outbound	No
165	Ascend-FR-DTE-N393	Integer (maximum length 10 characters)	Outbound	No
166	Ascend-FR-T391	Integer (maximum length 10 characters)	Outbound	No
167	Ascend-FR-T392	Integer (maximum length 10 characters)	Outbound	No
168	Ascend-Bridge-Address	String (maximum length 253 characters)	Outbound	No
169	Ascend-TS-Idle-Limit	Integer (maximum length 10 characters)	Outbound	No
170	Ascend-TS-Idle-Mode	Integer (maximum length 10 characters)	Outbound	No
171	Ascend-DBA-Monitor	Integer (maximum length 10 characters)	Outbound	No
172	Ascend-Base-Channel-Count	Integer (maximum length 10 characters)	Outbound	No
173	Ascend-Minimum-Channels	Integer (maximum length 10 characters)	Outbound	No
IPX Static Routes				
174	Ascend-IPX-Route	String (maximum length 253 characters)	Inbound	No
175	Ascend-FT1-Caller	Integer (maximum length 10 characters)	Inbound	No
176	Ascend-Backup	String (maximum length 253 characters)	Inbound	No
177	Ascend-Call-Type	Integer	Inbound	No
178	Ascend-Group	String (maximum length 253 characters)	Inbound	No
179	Ascend-FR-DLCI	Integer (maximum length 10 characters)	Inbound	No
180	Ascend-FR-Profile-Name	String (maximum length 253 characters)	Inbound	No
181	Ascend-Ara-PW	String (maximum length 253 characters)	Inbound	No
182	Ascend-IPX-Node-Addr	String (maximum length 253 characters)	Both	No
183	Ascend-Home-Agent-IP-Addr	Ipaddr (maximum length 15 characters)	Outbound	No
184	Ascend-Home-Agent-Password	String (maximum length 253 characters)	Outbound	No
185	Ascend-Home-Network-Name	String (maximum length 253 characters)	Outbound	No
186	Ascend-Home-Agent-UDP-Port	Integer (maximum length 10 characters)	Outbound	No
187	Ascend-Multilink-ID	Integer	Inbound	No
188	Ascend-Num-In-Multilink	Integer	Inbound	No
189	Ascend-First-Dest	Ipaddr	Inbound	No
190	Ascend-Pre-Input-Octets	Integer	Inbound	No

Table C-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
191	Ascend-Pre-Output-Octets	Integer	Inbound	No
192	Ascend-Pre-Input-Packets	Integer	Inbound	No
193	Ascend-Pre-Output-Packets	Integer	Inbound	No
194	Ascend-Maximum-Time	Integer (maximum length 10 characters)	Both	No
195	Ascend-Disconnect-Cause	Integer	Inbound	No
196	Ascend-Connect-Progress	Integer	Inbound	No
197	Ascend-Data-Rate	Integer	Inbound	No
198	Ascend-PreSession-Time	Integer	Inbound	No
199	Ascend-Token-Idle	Integer (maximum length 10 characters)	Outbound	No
200	Ascend-Token-Immediate	Integer	Outbound	No
201	Ascend-Require-Auth	Integer (maximum length 10 characters)	Outbound	No
202	Ascend-Number-Sessions	String (maximum length 253 characters)	Outbound	No
203	Ascend-Authen-Alias	String (maximum length 253 characters)	Outbound	No
204	Ascend-Token-Expiry	Integer (maximum length 10 characters)	Outbound	No
205	Ascend-Menu-Selector	String (maximum length 253 characters)	Outbound	No
206	Ascend-Menu-Item	String	Outbound	Yes
RADIUS Password Expiration Options				
207	Ascend-PW-Warntime	Integer (maximum length 10 characters)	Outbound	No
208	Ascend-PW-Lifetime	Integer (maximum length 10 characters)	Outbound	No
209	Ascend-IP-Direct	Ipaddr (maximum length 15 characters)	Outbound	No
210	Ascend-PPP-VJ-Slot-Comp	Integer (maximum length 10 characters)	Outbound	No
211	Ascend-PPP-VJ-1172	Integer (maximum length 10 characters)	Outbound	No
212	Ascend-PPP-Async-Map	Integer (maximum length 10 characters)	Outbound	No
213	Ascend-Third-Prompt	String (maximum length 253 characters)	Outbound	No
214	Ascend-Send-Secret	String (maximum length 253 characters)	Outbound	No
215	Ascend-Receive-Secret	String (maximum length 253 characters)	Outbound	No
216	Ascend-IPX-Peer-Mode	Integer	Outbound	No
217	Ascend-IP-Pool-Definition	String (maximum length 253 characters)	Outbound	No
218	Ascend-Assign-IP-Pool	Integer	Outbound	No
219	Ascend-FR-Direct	Integer	Outbound	No
220	Ascend-FR-Direct-Profile	String (maximum length 253 characters)	Outbound	No
221	Ascend-FR-Direct-DLCI	Integer (maximum length 10 characters)	Outbound	No
222	Ascend-Handle-IPX	Integer	Outbound	No
223	Ascend-Netware-Timeout	Integer (maximum length 10 characters)	Outbound	No
224	Ascend-IPX-Alias	String (maximum length 253 characters)	Outbound	No

Table C-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
225	Ascend-Metric	Integer (maximum length 10 characters)	Outbound	No
226	Ascend-PRI-Number-Type	Integer	Outbound	No
227	Ascend-Dial-Number	String (maximum length 253 characters)	Outbound	No
Connection Profile/PPP Options				
228	Ascend-Route-IP	Integer	Outbound	No
229	Ascend-Route-IPX	Integer	Outbound	No
230	Ascend-Bridge	Integer	Outbound	No
231	Ascend-Send-Auth	Integer	Outbound	No
232	Ascend-Send-Passwd	String (maximum length 253 characters)	Outbound	No
233	Ascend-Link-Compression	Integer	Outbound	No
234	Ascend-Target-Util	Integer (maximum length 10 characters)	Outbound	No
235	Ascend-Max-Channels	Integer (maximum length 10 characters)	Outbound	No
236	Ascend-Inc-Channel-Count	Integer (maximum length 10 characters)	Outbound	No
237	Ascend-Dec-Channel-Count	Integer (maximum length 10 characters)	Outbound	No
238	Ascend-Seconds-Of-History	Integer (maximum length 10 characters)	Outbound	No
239	Ascend-History-Weigh-Type	Integer	Outbound	No
240	Ascend-Add-Seconds	Integer (maximum length 10 characters)	Outbound	No
241	Ascend-Remove-Seconds	Integer (maximum length 10 characters)	Outbound	No
Connection Profile/Session Options				
242	Ascend-Data-Filter	Call filter	Outbound	Yes
243	Ascend-Call-Filter	Call filter	Outbound	Yes
244	Ascend-Idle-Limit	Integer (maximum length 10 characters)	Outbound	No
245	Ascend-Preempt-Limit	Integer (maximum length 10 characters)	Outbound	No
Connection Profile/Telco Options				
246	Ascend-Callback	Integer	Outbound	No
247	Ascend-Data-Svc	Integer	Outbound	No
248	Ascend-Force-56	Integer	Outbound	No
249	Ascend-Billing-Number	String (maximum length 253 characters)	Outbound	No
250	Ascend-Call-By-Call	Integer (maximum length 10 characters)	Outbound	No
251	Ascend-Transit-Number	String (maximum length 253 characters)	Outbound	No
Terminal Server Attributes				
252	Ascend-Host-Info	String (maximum length 253 characters)	Outbound	No
PPP Local Address Attribute				
253	Ascend-PPP-Address	Ipaddr (maximum length 15 characters)	Outbound	No

Table C-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
MPP Percent Idle Attribute				
254	Ascend-MPP-Idle-Percent	Integer (maximum length 10 characters)	Outbound	No
255	Ascend-Xmit-Rate	Integer (maximum length 10 characters)	Outbound	No

Nortel Dictionary of RADIUS VSAs

Table C-10 lists the Nortel RADIUS VSAs supported by ACS. The Nortel vendor ID number is 1584.

Table C-10 Nortel RADIUS VSAs

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
035	Bay-Local-IP-Address	Ipaddr (maximum length 15 characters)	Outbound	No
054	Bay-Primary-DNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
055	Bay-Secondary-DNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
056	Bay-Primary-NBNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
057	Bay-Secondary-NBNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
100	Bay-User-Level	Integer	Outbound	No
101	Bay-Audit-Level	Integer	Outbound	No

Juniper Dictionary of RADIUS VSAs

Table C-11 lists the Juniper RADIUS VSAs supported by ACS. The Juniper vendor ID number is 2636.

Table C-11 Juniper RADIUS VSAs

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
001	Juniper-Local-User-Name	String (maximum length 247 characters)	Outbound	No
002	Juniper-Allow-Commands	String (maximum length 247 characters)	Outbound	No
003	Juniper-Deny-Commands	String (maximum length 247 characters)	Outbound	No

CSUtil Database Utility

This appendix details the command-line utility, `CSUtil.exe`, for Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS. Among its several functions, your can use `CSUtil.exe` to add, change, and delete users from a colon-delimited text file. You can also use the utility to add and delete AAA client configurations.

Note You can accomplish similar tasks by using the ACS System Backup, ACS System Restore, Database Replication, and RDBMS Synchronization features. For more information on these features, see Chapter 9, "System Configuration: Advanced."

This chapter contains the following topics:

- Location of CSUtil.exe and Related Files, page D-2
- CSUtil Command Syntax, page D-2
- Backing Up ACS with CSUtil.exe, page D-3
- Restoring ACS with CSUtil.exe, page D-4
- Creating an ACS Internal Database, page D-5
- Creating an ACS Internal Database Dump File, page D-6
- Loading the ACS Internal Database from a Dump File, page D-7
- Compacting the ACS Internal Database, page D-8
- User and AAA Client Import Option, page D-9
- Exporting User List to a Text File, page D-15
- Exporting Group Information to a Text File, page D-16
- Decoding Error Numbers, page D-17
- User-Defined RADIUS Vendors and VSA Sets, page D-18
- PAC File Generation, page D-25
- Posture-Validation Attributes, page D-28

Location of CSUtil.exe and Related Files

When you install ACS in the default location, `CSUtil.exe` is located in:

`C:\Program Files\CiscoSecure ACS v`*x.x*`\bin`

where *x.x* is the version of your ACS software. The `CSUtil.exe` tool is located in the *\bin* subdirectory of your ACS installation directory. Files generated by or accessed by `CSUtil.exe` are also located in the *\bin* directory. If you add other files, such as vendor definitions for the ACS dictionary, be sure to put them in the *\bin* directory.

CSUtil Command Syntax

The syntax for the **CSUtil** command is:

csutil [**-q**] [**-b** *backup_filename*] [**-d** [**-p** *secret_key*] *dump_filename*] [**-e** *number*]
[**-g** *group_number*] [**-i** *file*] [**-p** *secret_key*] [**-l** *filename* [**-passwd** *secret_key*]] [**-n**]
[**-r** all|users|config *backup_file*] [**-u**] [**-listUDV**] [**-addUDV** *slot filename.ini*]
[**-delUDV** *slot*] [**-dumpUDV** *database_dump_filename*]
[**-t**] [-filepath *full_filepath*] [-passwd *password*] [*-machine*]
(-a | -g *group_number* | -u *user_name* | -f *user_list_filepath*)
[-addAVP *filepath*] [-delAVP *vendor_id application_id attribute_id*] [-dumpAVP *filename*]
[-delPropHPP *attribute_ID property_ID*] [-delEntHPP *attribute_ID entity_name*]

Table D-1 shows the options that you can use with the **CSUtil** command.

Table D-1 CSUtil Options

Syntax	Use to ...
-q	Use Quiet mode. Does not prompt, use before other options.
-**b** *backup_filename*	Create a system backup.
-**d** [**-p** *secret_key*] *dump_filename*	Dump users and groups database to *dump.txt* or a named file. You should provide a key to encrypt user passwords and other sensitive information in the dump file.
-e *number*	Decode error number to ASCII message.
-g *group_number*	Dump group information only to *group.txt*.
-i *file*	Import users or NASs from *import.txt* or named file.
-p *secret_key*	Reset password-aging counters during users' and groups' database dump (**-d**).
-l *filename* [**-passwd** *secret_key*]	Empty the user table, initialize profiles, and load users and groups database from *dump.txt* or named file. If you used an encrypt key when dumping the information, you must provide a key to decrypt user passwords and other sensitive information in the dump file.
-n	Empty the user table and shared profile components table, initialize user, group, and network access profiles, and create a new database.
-r all|users|config *backup_file*	Restore a system backup.
-u	List users by group to *users.txt*.

Table D-1 CSUtil Options (continued)

Syntax	Use to ...
-listUDV	List currently installed user defined vendors (UDVs).
-addUDV*slot filename.ini*	Install user defined vendor or vendor specfic attribute (VSA) data from the *.ini* file.
-delUDV *slot*	Remove a vendor or VSA.
-dumpUDV *database_dump_file*	Dump currently installed vendors to the System UDVs folder.
-t -filepath *full_filepath* **-passwd** *password -machine* (-a | -g *group_number* | -u *user_name* | -f *user_list_filepath*)	Generate protected access credentials (PAC) files for use with Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) clients. You can generate a user PAC or a machine PAC.
-addAVP *filename*	Add attributes from <*filename*>.
-delAVP *vendor_id application_id attribute_id*	Remove an AVP attribute
-dumpAVP ***filename***	Dump AVP attributes into <*filename*>
-delPropHPP *attribute_ID property_ID*	Remove specific property from an extended attribute under Cisco:Host.
-delEntHPP *attribute_ID entity_name*	Remove specific entity from an extended attribute under Cisco:Host.

Caution Most **CSUtil** options require that you stop the **CSAuth** service. While the **CSAuth** service is stopped, ACS does not authenticate users. To determine if an option requires that you stop **CSAuth**, refer to the detailed topics about the option.

You can combine many of the options in a single use of `CSUtil.exe`. If you are new to using `CSUtil.exe`, we recommend performing only one option at a time, with the exception of those options, such as **-p**, that must be used in conjunction with other options.

Experienced `CSUtil.exe` users might find it useful to combine `CSUtil.exe` options, such as in the following example, which would first import AAA client configurations and then generate a dump of all ACS internal data:

CSUtil.exe -i newnases.txt -d

Backing Up ACS with CSUtil.exe

You can use the **-b** option to create a system backup of all ACS internal data. The resulting backup file has the same data as the backup files that are produced by the ACS Backup feature found in the web interface. For more information about the ACS Backup feature, see ACS Backup, page 8-7.

Note During the backup, all services are automatically stopped and restarted. No users are authenticated while the backup is occurring.

To back up ACS with `CSUtil.exe`:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 Type:

CSUtil.exe -b *filename*

where *filename* is the name of the backup file. Press **Enter**.

`CSUtil.exe` displays a confirmation prompt.

Step 3 To confirm that you want to perform a backup and to halt all ACS services during the backup, type **Y** and press **Enter**.

`CSUtil.exe` generates a complete backup of all ACS internal data, including user accounts and system configuration. This process may take a few minutes.

Note `CSUtil.exe` displays the error message `Backup Failed` when it attempts to back up components of ACS that are empty, such as when no administrator accounts exist. These messages apply only to components that are empty, not to the overall success or failure of the backup.

Restoring ACS with CSUtil.exe

You can use the **-r** option to restore all ACS internal data. The backup file from which you restore ACS can be one generated by the `CSUtil.exe` **-b** option or by the ACS Backup feature in the web interface.

ACS backup files contain:

- User and group data.
- System configuration.

You can restore user and group data, or system configuration, or both. For more information about the ACS Backup feature, see ACS Backup, page 8-7.

Note During the restoration, all services are automatically stopped and restarted. No users are authenticated while the restoration is occurring.

To restore ACS with `CSUtil.exe`:

Step 1 On the computer running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 Perform one of the following:

- To restore all data (user and group data, and system configuration), type:

  CSUtil.exe -r all *filename*

  where *filename* is the name of the backup file.

  Press **Enter**.

- To restore only user and group data, type:

  CSUtil.exe -r users *filename*

  where *filename* is the name of the backup file.

Press **Enter**.

- To restore only the system configuration, type:

  CSUtil.exe -r config *filename*

  where *filename* is the name of the backup file.

  Press **Enter**.

`CSUtil.exe` displays a confirmation prompt.

Step 3 To confirm that you want to perform a restoration and to halt all ACS services during the restoration, type **Y** and press **Enter**.

`CSUtil.exe` restores the specified portions of your ACS data. This process may take a few minutes.

Note If the backup file is missing a database component, `CSUtil.exe` displays an error message. Such an error message applies only to the restoration of the missing component. The absence of a database component in a backup is usually intentional and indicates that the component was empty in ACS at the time the backup was created.

Creating an ACS Internal Database

You can use the **-n** option to create an ACS internal database. The **-n** option empties the user table and shared profile components table, initializes user, group, and network access profiles, and creates a new database.

Note Using the **-n** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

Caution Using the **-n** option erases all user information in the ACS internal database. Unless you have a current backup or dump of your ACS internal database, all user accounts are lost when you use this option.

To create an ACS internal database:

Step 1 If you have not performed a backup or dump of the ACS internal database, do so now before proceeding. For more information about backing up the database, see Backing Up ACS with CSUtil.exe, page D-3.

Step 2 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 3 If the **CSAuth** service is running, type:

net stop csauth

Press **Enter**.

The **CSAuth** service stops.

Step 4 Type:

CSUtil.exe -n

Press **Enter**.

`CSUtil.exe` displays a confirmation prompt.

Step 5 To confirm that you want to initialize the ACS internal database, type **Y** and press **Enter**.

The ACS internal database is initialized. This process may take a few minutes.

Step 6 To resume user authentication, type:

net start csauth

Press **Enter**.

Creating an ACS Internal Database Dump File

You can use the **-d** option to dump all contents of the ACS internal database into a password-protected text file. You can provide a name for the file; otherwise, it is called *dump.txt*. The dump file provides a thorough and compressible backup of all ACS internal data.

Using the **-l** option, you can reload the ACS internal data from a dump file created by the **-d** option. For more information about the **-l** option, see Loading the ACS Internal Database from a Dump File, page D-7.

Note Using the **-d** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To dump all ACS internal data into a text file:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 If the **CSAuth** service is running, type:

net stop csauth

Press **Enter**.

The **CSAuth** service stops.

Step 3 To dump to the default *dump.txt* file, type:

CSUtil.exe -d -p *secret_key*

Press **Enter**.

`CSUtil.exe` displays a confirmation prompt.

Step 4 To dump to a named file, type:

CSUtil.exe -d -p *secret_key dump_filename*

Press **Enter**.

`CSUtil.exe` displays a confirmation prompt.

Note If you do not enter a password, you will be prompted to enter one before the confirmation prompt appears.

Step 5 To confirm that you want to dump all ACS internal data into a text file, type **Y** and press **Enter**.

`CSUtil.exe` creates the dump text file. This process may take a few minutes.

Step 6 To resume user authentication, type:

net start csauth

Press **Enter**.

Loading the ACS Internal Database from a Dump File

You can use the **-l** option to overwrite all ACS internal data from a dump text file. This option replaces the existing all ACS internal data with the data in the dump text file. In effect, the **-l** option initializes all ACS internal data before loading it from the dump text file. Dump text files are created by using the **-d** option. You must use the same password used to encrypt the dump files.

You can use the **-p** option in conjunction with the `-1` option to reset password-aging counters.

Note Using the **-l** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To load all ACS internal data from a text file:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 If the **CSAuth** service is running, type:

net stop csauth

Press **Enter**.

The **CSAuth** service stops.

Step 3 To load from the default *dump.txt* file, type:

CSUtil.exe -l -passwd *secret_key*

where *secret_key* is the same password that was used to encrypt the dump text file. Press **Enter**.

Step 4 To load from a named dump file and reset password-aging counters, type:

CSUtil.exe -l *filename* -passwd *secret_key* -p

where *filename* is the name of the dump file that you want `CSUtil.exe` to use to load ACS internal data. *secret_key* is the same password that was used to encrypt the `dump.txt` file.

Press **Enter**.

`CSUtil.exe` displays a confirmation prompt for overwriting all ACS internal data with the data in the dump text file.

Note Overwriting the database does not preserve any data; instead, after the overwrite, the database contains only what is specified in the dump text file.

Step 5 To confirm that you want to replace all ACS internal data, type **Y** and press **Enter**.

`CSUtil.exe` initializes all ACS internal data, and then loads ACS with the information in the dump file specified. This process may take a few minutes.

Step 6 To resume user authentication, type:

net start csauth

Press **Enter**.

Compacting the ACS Internal Database

Like many relational databases, the ACS internal database handles the deletion of records by marking deleted records as deleted; but not removing the records from the database. Over time, your ACS internal database may be substantially larger than is required by the number of users that it contains. To reduce the ACS internal database size, you can compact it periodically.

You can compact the ACS internal database by using the following `CSUtil.exe` options:

- **-d**—Export all ACS internal data to a text file, named *dump.txt*.
- **-n**—Create an ACS internal database and index.
- **-l**—Load all ACS internal data from the *dump.txt* file.

Additionally, if you want to automate this process, consider using the **-q** option to suppress the confirmation prompts that otherwise appear before `CSUtil.exe` performs the **-n** and **-l** options.

Note Compacting the ACS internal database requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To compact the ACS internal database:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 If the **CSAuth** service is running, type:

net stop csauth

Press **Enter**.

The **CSAuth** service stops.

Step 3 Type:

CSUtil.exe -d -n -l

Press **Enter**.

Tip If you include the **-q** option in the command, **CSUtil** does not prompt you for confirmation of initializing or loading the database.

If you do not use the **-q** option, `CSUtil.exe` displays a confirmation prompt for initializing the database and then for loading the database. For more information about the effects of the **-n** option, see Creating an ACS Internal Database, page D-5. For more information about the effects of the **-l** option, see Loading the ACS Internal Database from a Dump File, page D-7.

Step 4 For each confirmation prompt that appears, type **Y** and press **Enter**.

`CSUtil.exe` dumps all ACS internal data to `dump.txt`, initializes the ACS internal database, and reloads all ACS internal data from `dump.txt`. This process may take a few minutes.

Step 5 To resume user authentication, type:

net start csauth

Press **Enter**.

User and AAA Client Import Option

You can use the **-i** option to update ACS with data from a colon-delimited text file. You can also update AAA client definitions.

For user accounts, you can add users, change user information such as passwords, or delete users. For AAA client definitions, you can add or delete AAA clients.

This section contains the following topics:

- Importing User and AAA Client Information, page D-9
- User and AAA Client Import File Format, page D-10
  - About User and AAA Client Import File Format, page D-11
  - ONLINE or OFFLINE Statement, page D-11
  - ADD Statements, page D-12
  - UPDATE Statements, page D-13
  - DELETE Statements, page D-13
  - ADD_NAS Statements, page D-14
  - DEL_NAS Statements, page D-15
  - Import File Example, page D-15

Importing User and AAA Client Information

To import user or AAA client information:

Step 1 If you have not performed a backup or dump of ACS, do so now before proceeding. For more information about backing up the database, see Backing Up ACS with CSUtil.exe, page D-3.

Step 2 Create an import text file. For more information about what an import text file can or must contain, see User and AAA Client Import File Format, page D-10.

Step 3 Copy or move the import text file to the same directory as `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 4 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`.

Step 5 Type:

CSUtil.exe -i *filename*

where *filename* is the name of the import text file you want `CSUtil.exe` to use to update ACS. Press **Enter**.

`CSUtil.exe` displays a confirmation prompt for updating the database.

Step 6 To confirm that you want to update ACS with the information from the import text file specified, type **Y** and press **Enter**.

ACS is updated with the information in the import text file specified. This process may take a few minutes.

If the import text file contained AAA client configuration data, `CSUtil.exe` warns you that you must restart CSTacacs and CSRadius for these changes to take effect.

Step 7 To restart CSRadius:

a. Type:

net stop csradius

Press **Enter**. The CSRadius service stops.

b. To start CSRadius, type:

net start csradius

Press **Enter**.

Step 8 To restart CSTacacs:

a. Type:

net stop cstacacs

Press **Enter**. The CSTacacs service stops.

b. To start CSTacacs, type:

net start cstacacs

Press **Enter**.

User and AAA Client Import File Format

This section contains the following topics:

- About User and AAA Client Import File Format, page D-11
- ONLINE or OFFLINE Statement, page D-11
- ADD Statements, page D-12
- UPDATE Statements, page D-13

- DELETE Statements, page D-13
- ADD_NAS Statements, page D-14
- DEL_NAS Statements, page D-15
- Import File Example, page D-15

About User and AAA Client Import File Format

The import file can contain six different line types, as discussed in following topics. The first line of the import file must be one of the tokens defined in Table D-2.

Each line of a `CSUtil.exe` import file is a series of colon-separated tokens. Some of the tokens are followed by values. Values, like tokens, are colon-delimited. For tokens that require values, `CSUtil.exe` expects the value of the token to be in the colon-delimited field immediately following the token.

Note There are no password character limitations in the ACS user interface, or when using the `CSUtil.exe` to import passwords.

ONLINE or OFFLINE Statement

`CSUtil.exe` requires an **ONLINE** or **OFFLINE** token in an import text file. The file must begin with a line that contains only an **ONLINE** or **OFFLINE** token. The **ONLINE** and **OFFLINE** tokens are described in Table D-2.

Table D-2 ONLINE/OFFLINE Statement Tokens

Token	Required	Value Required	Description
ONLINE	**ONLINE** or **OFFLINE** must be present	—	The **CSAuth** service remains active while `CSUtil.exe` imports the text file. `CSUtil.exe` performance is slower when run in this mode, but ACS continues to authenticate users during the import.
OFFLINE	**ONLINE** or **OFFLINE** must be present	—	The **CSAuth** service is stopped while `CSUtil.exe` imports the text file. Although `CSUtil.exe` performance is fastest in this mode, no users are authenticated during the import. If you need to import a large amount of user information quickly, consider using the **OFFLINE** token. While performing an import in the **OFFLINE** mode stops authentication during the import, the import is much faster. For example, importing 100,000 users in the **OFFLINE** mode takes less than one minute.

ADD Statements

ADD statements are optional. Only the **ADD** token and its value are required to add a user to ACS. Table D-3 lists the valid tokens for **ADD** statements.

Note `CSUtil.exe` provides no means to specify a particular instance of an external user database type. If an external user database authenticates a user and ACS has multiple instances of the specified database type, `CSUtil.exe` assigns the user to the first instance of that database type. For example, if ACS has two LDAP external user databases configured, `CSUtil.exe` creates the user record and assigns the user to the LDAP database that was added to ACS first.

Table D-3 ADD Statement Tokens

Token	Required	Value Required	Description
ADD	Yes	username	Add user information to ACS. If the username already exists, no information is changed.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. If you do not use the **PROFILE** token or fail to provide a group number, the user is added to the default group.
CHAP	No	CHAP password	Require a Challenge Authentication Handshake Protocol (CHAP) password for authentication.
CSDB	No	password	Authenticate the username with the ACS internal database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the ACS internal database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows external user database.
EXT_NDS	No	—	Authenticate the username with a Novell Network Directory Services (NDS) external user database.
EXT_SDI	No	—	Authenticate the username with an Rivest, Shamir, and Adelman (RSA) external user database.
EXT_ODBC	No	—	Authenticate the username with an Open Database Connectivity (ODBC) external user database.
EXT_LDAP	No	—	Authenticate the username with a generic Lightweight Directory Access Protocol (LDAP) external user database.
EXT_LEAP	No	—	Authenticate the username with a Lightweight and Efficient Application Protocol (LEAP) proxy Remote Access Dial-In User Service (RADIUS) server external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following **ADD** statement would create an account with the username *John*, assign it to Group 3, and specify that *John* should be authenticated by the ACS internal database with the password **closedmondays**:

ADD:John:PROFILE:3:CSDB:closedmondays

UPDATE Statements

UPDATE statements are optional. They make changes to existing user accounts. Only the UPDATE token and its value are required by `CSUtil.exe`, but if no other tokens are included, no changes are made to the user account. You can use the UPDATE statement to update the group that a user is assigned to or to update which database ACS uses to authenticate the user.

Table D-4 lists the valid tokens for UPDATE statements.

Table D-4 UPDATE Statement Tokens

Token	Required	Value Required	Description
UPDATE	Yes	username	Update user information to ACS.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. **Note** If you do not specify a database token, such as CSDB or **EXT_NT**, updating a group assignment may erase a user's password.
CHAP	No	CHAP password	Require a CHAP password for authentication.
CSDB	No	password	Authenticate the username with the ACS internal database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the ACS internal database by using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows external user database.
EXT_NDS	No	—	Authenticate the username with a Novell NDS external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following UPDATE statement causes `CSUtil.exe` to update the account with username *John*, assign it to Group 50, specify that *John* should be authenticated by a UNIX-encrypted password, with a separate CHAP password **goodoldchap**:

```
UPDATE:John:PROFILE:50:CSDB_UNIX:3Al3qf9:CHAP:goodoldchap
```

DELETE Statements

DELETE statements are optional. The DELETE token and its value are required to delete a user account from ACS. The DELETE token, detailed in Table D-5, is the only token in a DELETE statement.

Table D-5 UPDATE Statement Tokens

Token	Required	Value Required	Description
DELETE	Yes	username	The name of the user account to delete.

For example, the following DELETE statement causes `CSUtil.exe` to permanently remove the account with username *John* from the ACS internal database:

DELETE:John

ADD_NAS Statements

ADD_NAS statements are optional. The **ADD_NAS**, **IP**, **KEY**, and **VENDOR** tokens and their values are required to add a AAA client definition to ACS.

Table D-6 lists the valid tokens for ADD_NAS statements.

Table D-6 ADD_NAS Statement Tokens

Token	Required	Value Required	Description
ADD_NAS	Yes	AAA client name	The name of the AAA client to add.
IP	Yes	IP address	The IP address of the AAA client being added. Use a pipe (|) between IP addresses to import devices with multiple IPs.
KEY	Yes	Shared secret	The shared secret for the AAA client.
VENDOR	Yes	See description	The authentication protocol that the AAA client uses. For RADIUS, this includes the VSA. **Note** The following values are valid. Quotation marks ("") are required, due to the spaces in the protocol names. • "TACACS+ (Cisco IOS)" • "RADIUS (Cisco Aironet)" • "RADIUS (Cisco Airespace)" • "RADIUS (Cisco BBSM)" • "RADIUS (Cisco IOS/PIX 6.x)" • "RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)" • "RADIUS (Cisco VPN 5000)" • "RADIUS (IETF)" • "RADIUS (Ascend)" • "RADIUS (Juniper)" • "RADIUS (Nortel)" • "RADIUS (iPass)"
NDG	No	NDG name	The name of the Network Device Group to which to add the AAA client.
SINGLE_CON	No	Y or N	For AAA clients using TACACS+ only, the value set for this TOKEN specifies whether the Single Connect TACACS+ AAA Client option is enabled. For more information, see Adding AAA Clients, page 4-11.
KEEPALIVE	No	Y or N	For AAA clients that are using TACACS+ only, the value set for this token specifies whether the Log Update or Watchdog Packets from this Access Server option is enabled. For more information, see Adding AAA Clients, page 4-11.

For example, the following **ADD_NAS** statement causes `CSUtil.exe` to add the AAA client with the name **SVR2-T+**, using TACACS+ with the single connection and keep alive packet options enabled:

ADD_NAS:SVR2-T+:IP:*IP address*:KEY:*shared secret*:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East Coast":SINGLE_CON:Y:KEEPALIVE:Y

DEL_NAS Statements

DEL_NAS statements are optional. The **DEL_NAS** token, detailed in Table D-7, is the only token in a **DEL_NAS** statement. **DEL_NAS** statements delete AAA client definitions from ACS.

Table D-7 DEL_NAS Statement Tokens

Token	Required	Value Required	Description
DEL_NAS	Yes	AAA client name	The name of the AAA client to delete.

For example, the following **DEL_NAS** statement causes `CSUtil.exe` to delete a AAA client with the name **SVR2-T+**:

DEL_NAS:SVR2-T+

Import File Example

An example of the import text file is:

```
OFFLINE
ADD:user01:CSDB:userpassword:PROFILE:1
ADD:user02:EXT_NT:PROFILE:2
ADD:chapuser:CSDB:hello:CHAP:chappw:PROFILE:3
ADD:mary:EXT_NT:CHAP:achappassword
ADD:joe:EXT_SDI
ADD:vanessa:CSDB:vanessaspassword
ADD:juan:CSDB_UNIX:unixpassword
UPDATE:foobar:PROFILE:10
DELETE:paul
ADD_NAS:SVR2-T+:IP:209.165.202.136:KEY:A87i1032bzg:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East
Coast"
DEL_NAS:SVR16-RAD
```

Exporting User List to a Text File

You can use the **-u** option to export a list of all users in the ACS internal database to a text file named *users.txt*. The *users.txt* file organizes users by group. Within each group, users are listed in the order that their user accounts were created in the ACS internal database. For example, if accounts were created for *Pat*, *Dana*, and *Lloyd*, in that order, *users.txt* lists them in that order as well; rather than alphabetically.

Note Using the **-u** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To export user information from the ACS internal database into a text file:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 If the **CSAuth** service is running, type:

net stop csauth

Press **Enter**.

The **CSAuth** service stops.

Step 3 Type:

CSUtil.exe -u

Press **Enter**.

`CSUtil.exe` exports information for all users in the ACS internal database to a file named *users.txt*.

Step 4 To resume user authentication, type:

net start csauth

Press **Enter**.

Exporting Group Information to a Text File

You can use the **-g** option to export group configuration data, including device command sets, from the ACS internal database to a text file named **groups.txt**. The **groups.txt** file is useful primarily for debugging purposes while working with the TAC.

Note Using the **-g** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To export group information from the ACS internal database to a text file:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 If the **CSAuth** service is running, type:

net stop csauth

Press **Enter**.

The **CSAuth** service stops.

Step 3 Type:

CSUtil.exe -g

Press **Enter**.

`CSUtil.exe` exports information for all groups in the ACS internal database to a file named `groups.txt`.

Step 4 To resume user authentication, type:

net start csauth

Press **Enter**.

Decoding Error Numbers

You can use the **-e** option to decode error numbers in ACS service logs. These error codes are internal to ACS. For example, the CSRadius log could contain a message similar to:

```
CSRadius/Logs/RDS.log:RDS 05/22/2001 10:09:02 E 2152 4756 Error -1087 authenticating geddy
- no NAS response sent
```

In this example, the error code number that you could use `CSUtil.exe` to decode is `-1087`:

```
C:\Program Files\CiscoSecure ACS vx.x\Utils: CSUtil.exe -e -1087
CSUtil v3.0(1.14), Copyright 1997-2001, Cisco Systems Inc
Code -1087 : External database reported error during authentication
```

Note The **-e** option applies to ACS internal error codes only; not to Windows error codes that are sometimes captured in ACS logs, such as when Windows authentication fails.

For more information about ACS service logs, see Service Logs, page 11-23.

To decode an error number from an ACS service log:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 Type:

CSUtil.exe -e -*number*

where *number* is the error number in the ACS service log.

Press **Enter**.

Note The hyphen (-) before *number* is required.

`CSUtil.exe` displays the text message that is equivalent to the error number specified.

User-Defined RADIUS Vendors and VSA Sets

This section provides information and procedures about user-defined RADIUS vendors and VSAs.

This section contains the following topics:

- About User-Defined RADIUS Vendors and VSA Sets, page D-18
- Adding a Custom RADIUS Vendor and VSA Set, page D-18
- Deleting a Custom RADIUS Vendor and VSA Set, page D-19
- Listing Custom RADIUS Vendors, page D-20
- Exporting Custom RADIUS Vendor and VSA Sets, page D-21
- RADIUS Vendor/VSA Import File, page D-21

About User-Defined RADIUS Vendors and VSA Sets

In addition to supporting a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), ACS supports RADIUS vendors and VSAs that you define. We recommend that you use RDBMS Synchronization to add and configure custom RADIUS vendors; however, you can use `CSUtil.exe` to accomplish the same custom RADIUS vendor and VSA configurations that you can accomplish by using RDBMS Synchronization. Custom RADIUS vendor and VSA configurations that you create by using RDBMS Synchronization or `CSUtil.exe` can be modified by the other feature. Choosing one feature for configuring custom RADIUS vendors and VSAs does not preclude using the other feature. For more information about RDMBS Synchronization, see RDBMS Synchronization, page 9-17.

Vendors that you add must be Internet Engineering Task Force (IETF)-compliant; therefore, all VSAs that you add must be subattributes of IETF RADIUS attribute number 26. You can define up to ten custom RADIUS vendors, numbered zero (0) through 9. `CSUtil.exe` allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and the vendor name.

Note If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary ACSs, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see ACS Internal Database Replication, page 9-1.

Adding a Custom RADIUS Vendor and VSA Set

You can use the **-addUDV** option to add up to ten custom RADIUS vendors and VSA sets to ACS. Each RADIUS vendor and VSA set is added to one of ten possible user-defined RADIUS vendor slots.

Note While `CSUtil.exe` adds a custom RADIUS vendor and VSA set to ACS, all ACS services are automatically stopped and restarted. No users are authenticated during this process.

Before You Begin

- Define a custom RADIUS vendor and VSA set in a RADIUS vendor/VSA import file. For more information, see RADIUS Vendor/VSA Import File, page D-21.

- Determine the RADIUS vendor slot to which you want to add the new RADIUS vendor and VSAs. For more information, see Listing Custom RADIUS Vendors, page D-20.

To add a custom RADIUS VSA to ACS:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 Type:

CSUtil.exe -addUDV *slot-number*
filename

where *slot-number* is an unused ACS RADIUS vendor slot and *filename* is the name of a RADIUS vendor/VSA import file. The *filename* can include a relative or absolute path to the RADIUS vendor/VSA import file. Press **Enter**.

For example, to add the RADIUS vendor defined in `d:\acs\myvsa.ini` to slot 5, use the command:

CSUtil.exe -addUDV 5 d:\acs\myvsa.ini

`CSUtil.exe` displays a confirmation prompt.

Step 3 To confirm that you want to add the RADIUS vendor and halt all ACS services during the process, type **Y** and press **Enter**.

`CSUtil.exe` halts ACS services, parses the vendor/VSA input file, and adds the new RADIUS vendor and VSAs to ACS. This process may take a few minutes. After it is complete, `CSUtil.exe` restarts ACS services.

Note We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the *\Utils* directory, where `CSUtil.exe` is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

Deleting a Custom RADIUS Vendor and VSA Set

You can use the **-delUDV** option to delete a custom RADIUS vendor from ACS.

Note While `CSUtil.exe` deletes a custom RADIUS vendor from ACS, all ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

Before You Begin

Verify that, in the Network Configuration section of the ACS web interface, no AAA client uses the RADIUS vendor. For more information about configuring AAA clients, see AAA Client Configuration, page 4-7.

Verify that your RADIUS accounting log does not contain attributes from the RADIUS vendor that you want to delete. For more information about configuring your RADIUS accounting log, see Accounting Logs, page 11-4.

To delete a custom RADIUS vendor and VSA set from ACS:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 Type:

CSUtil.exe -delUDV ***slot-number***

where *slot-number* is the slot containing the RADIUS vendor that you want to delete.

Press **Enter**.

Note For more information about determining what RADIUS vendor a particular slot contains, see Listing Custom RADIUS Vendors, page D-20.

`CSUtil.exe` displays a confirmation prompt.

Step 3 To confirm that you want to halt all ACS services while deleting the custom RADIUS vendor and VSAs, type **Y** and press **Enter**.

`CSUtil.exe` displays a second confirmation prompt.

Step 4 To confirm that you want to delete the RADIUS vendor, type **Y** and press **Enter**.

`CSUtil.exe` halts ACS services, deletes the specified RADIUS vendor from ACS. This process may take a few minutes. After it is complete, `CSUtil.exe` restarts ACS services.

Listing Custom RADIUS Vendors

You can use the **-listUDV** option to determine what custom RADIUS vendors are defined in ACS. You also use this option to determine which of the ten possible custom RADIUS vendor slots are in use and which RADIUS vendor occupies each used slot.

To list all custom RADIUS vendors that are defined in ACS:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 Type:

CSUtil.exe -listUDV

Press **Enter**.

`CSUtil.exe` lists each user-defined RADIUS vendor slot in slot number order. `CSUtil.exe` lists slots that do not contain a custom RADIUS vendor as **Unassigned**. An unassigned slot is empty. You can add a custom RADIUS vendor to any slot listed as **Unassigned**.

Exporting Custom RADIUS Vendor and VSA Sets

You can export all custom RADIUS vendor and VSA sets to files. Each vendor and VSA set is saved to a separate file. The files that this option creates are in the same format as RADIUS vendor/VSA import files. This option is particularly useful if you need to modify a custom RADIUS vendor and VSA set, and you have misplaced the original file that was used to import the set.

Note Exporting a custom RADIUS vendor and VSA set does not remove the vendor and VSA set from ACS.

ACS places all exported vendor/VSA files in a subdirectory of the directory containing `CSUtil.exe`. The subdirectory is named `System UDVs`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Each exported vendor/VSA file is named *UDV_n.ini*, where *n* is the slot number that the current custom RADIUS vendor currently occupies and VSA set. For example, if vendor Widget occupies slot 4, the exported file that `CSUtil.exe` creates is *UDV_4.ini*.

To export custom RADIUS vendor and VSA sets to files:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see Location of CSUtil.exe and Related Files, page D-2.

Step 2 Type:

CSUtil.exe -dumpUDV

Press **Enter**.

For each custom RADIUS vendor and VSA set that is currently configured in ACS, `CSUtil.exe` writes a file in the *\System UDVs* subdirectory.

RADIUS Vendor/VSA Import File

To import a custom RADIUS vendor and VSA set into ACS, you must define the RADIUS vendor and VSA set in an import file. This section details the format and content of RADIUS VSA import files.

We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the *\Utils* directory, where `CSUtil.exe` is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

This section contains the following topics:

- About the RADIUS Vendor/VSA Import File, page D-22
- Vendor and VSA Set Definition, page D-22
- Attribute Definition, page D-23
- Enumeration Definition, page D-24
- Example RADIUS Vendor/VSA Import File, page D-24

About the RADIUS Vendor/VSA Import File

RADIUS Vendor/VSA import files use a Windows .ini file format. Each RADIUS vendor/VSA import file comprises three types of sections, detailed in Table D-8. Each section comprises a section header, and a set of keys and values. The order of the sections in the RADIUS vendor/VSA import file is irrelevant.

Table D-8 RADIUS VSA Import File Section Types

Section	Required	Number	Description
Vendor and VSA set definition	Yes	1	Defines the RADIUS vendor and VSA set. For more information, see Vendor and VSA Set Definition, page D-22.
Attribute definition	Yes	1 to 255	Defines a single attribute of the VSA set. For more information, see Attribute Definition, page D-23.
Enumeration	No	0 to 255	Defines enumerations for attributes with integer data types. For more information, see Enumeration Definition, page D-24.

Vendor and VSA Set Definition

Each RADIUS vendor/VSA import file must have one vendor and VSA set section. The section header must be `[User Defined Vendor]`. Table D-9 lists valid keys for the vendor and VSA set section.

Table D-9 Vendor and VSA Set Keys

Keys	Required	Value Required	Description
Name	Yes	Vendor name	The name of the RADIUS vendor.
IETF Code	Yes	An integer	The IETF-assigned vendor number for this vendor.
VSA *n* (where *n* is the VSA number)	Yes—you can define 1 to 255 VSAs	Attribute name	The name of a VSA. For each VSA named here, the file must contain a corresponding attribute definition section. **Note** Attribute names must be unique within the RADIUS vendor/VSA import file, and within the set of all RADIUS attributes in ACS. To facilitate unique names, we recommend that you prefix the vendor name to each attribute name, such as `widget-encryption` for an encryption-related attribute for the vendor Widget. This naming convention also makes accounting logs easier to understand.

For example, the following vendor and VSA set section defines the vendor `Widget`, whose IETF-assigned vendor number is 9999. Vendor Widget has 4 VSAs (thus requiring 4 attribute definition sections):

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
```

Attribute Definition

Each RADIUS vendor/VSA import file must have one attribute definition section for each attribute that is defined in the vendor and VSA set section. The section header of each attribute definition section must match the attribute name that is defined for that attribute in the vendor and VSA set section. Table D-9 lists the valid keys for an attribute-definition section.

Table D-10 Attribute Definition Keys

Keys	Required	Value Required	Description
Type	Yes	See description	The data type of the attribute. It must be one of: • STRING • INTEGER • IPADDR If the attribute is an integer, the **Enums** key is valid.

Profile	Yes	See description	The attribute profile defines if the attribute is used for authorization or accounting, or both. The **Profile** key definition must contain at least one of these values:
			• **IN**—The attribute is used for accounting. After you add the attribute to ACS, you can configure your RADIUS accounting log to record the new attribute. For more information about RADIUS accounting logs, see Accounting Logs, page 11-4.
			• **OUT**—The attribute is used for authorization.
			In addition, you can use the value `MULTI` to allow several instances of the attribute per RADIUS message.
			Combinations are valid. For example:
			`Profile=MULTI OUT`
			or
			`Profile=IN OUT`

Enums	No (only valid when the TYPE value is INTEGER)	Enumera-tions section name	The name of the enumeration section. **Note** Several attributes can reference the same enumeration section. For more information, see Enumeration Definition, page D-24.

For example, the following attribute definition section defines the widget-encryption VSA, which is an integer used for authorization, and for which enumerations exist in the Encryption-Types enumeration section:

```
[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types
```

Enumeration Definition

You can use enumeration definitions to associate a text-based name for each valid numeric value of an integer-type attribute. In the Group Setup and User Setup sections of the ACS web interface, the text values that you define appear in lists that are associated with the attributes that use the enumerations. Enumeration definition sections are required only if an attribute definition section references them. Only attributes that are integer-type can reference an enumeration definition section.

The section header of each enumeration definition must match the value of an Enums key that references it. More than one **Enums** key can reference an enumeration definition section; thus, allowing for reuse of common enumeration definitions. An enumeration definition section can have up to 1000 keys.

Table D-11 lists the valid keys for an enumeration definition section.

Table D-11 Enumerations Definition Keys

Keys	Required	Value Required	Description
n (See description.)	Yes	String	For each valid integer value of the corresponding attribute, an enumerations section must have one key. Each key defines a string value that is associated with an integer value. ACS uses these string values in the web interface. For example, if 0 through 4 are valid integer values for a given attribute, its enumeration definition would contain: `0=`*value0* `1=`*value1* `2=`*value2* `3=`*value3* `4=`*value4*

For example, the following enumerations definition section defines the Encryption-Types enumeration, which associates the string value 56-bit with the integer 0 and the string value 128-bit with the integer 1:

```
[Encryption-Types]
0=56-bit
1=128-bit
```

Example RADIUS Vendor/VSA Import File

The following example RADIUS vendor/VSA import file defines the vendor Widget, whose IETF number is 9999. The vendor Widget has 5 VSAs. Of those attributes, 4 are for authorization and one is for accounting. Only one attribute can have multiple instances in a single RADIUS message. Two attributes have enumerations for their valid integer values and they share the same enumeration definition section.

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
VSA 5=widget-remote-address

[widget-encryption]
```

```
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-admin-interface]
Type=IPADDR
Profile=OUT

[widget-group]
Type=STRING
Profile=MULTI OUT

[widget-admin-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-remote-address]
Type=STRING
Profile=IN

[Encryption-Types]
0=56-bit
1=128-bit
2=256-bit
```

PAC File Generation

You can use the **-t** option to generate PAC files for use with EAP-FAST clients. You can generate PACs for users or for machines. For more information about PACs and EAP-FAST, see EAP-FAST Authentication, page 10-8.

This section contains the following topics:

- PAC File Options and Examples, page D-25
- Generating PAC Files, page D-27

PAC File Options and Examples

When you use the **-t** option to generate PAC files with `CSUtil.exe`, you have the following additional options.

- **-filepath** *full_filepath*—Specifies the location of the generated files.
- **-machine**—Use this option to generate PACs for machines instead of users.
- **User specification options**—You must choose one of the four options for specifying the users for whom you want PAC files; otherwise, `CSUtil.exe` displays an error message because no users are specified. User specification options are:
  - **-a**—`CSUtil.exe` generates a PAC file for each user in the ACS internal database. For example, if you have 3278 users in the ACS internal database and ran **CSUtil.exe -t -a**, `CSUtil.exe` would generate 3278 PAC files, one for each user.

Note Using the **-a** option restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.

– **-g** *N*—`CSUtil.exe` generates a PAC file for each user in the user group specified by the variable (*N*). ACS has 500 groups, numbered from zero (0) to 499. For example, if group 7 has 43 users and you ran **CSUtil.exe -t -g 7**, `CSUtil.exe` would generate 43 PAC files, one for each user who is a member of group 7.

Note Using the **-g** option restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.

– **-u** *username*—`CSUtil.exe` generates a PAC file for the user specified by the variable (*username*). For example, if you ran **CSUtil.exe -t -u seaniemop, CSUtil.exe** would generate a single PAC file, named *seaniemop.pac*.

Tip You can also specify a domain-qualified username by using the format *DOMAIN\username*. For example, if you specify `ENGINEERING\augustin`, ACS generates a PAC file named *ENGINEERING_augustin.pac*.

– **-f** *list*—`CSUtil.exe` generates a PAC file for each username in the file that is specified, where *list* represents the full path and filename of the list of usernames.

Lists of usernames should contain one username per line, with no additional spaces or other characters.

For example, if *list.txt* in *d:\temp\pacs* contains the following usernames:

```
seaniemop
jwiedman
echamberlain
```

and you ran **CSUtil.exe -t -f d:\temp\pacs\list.txt**, `CSUtil.exe` generates three PAC files:

```
seaniemop.pac
jwiedman.pac
echamberlain.pac.
```

Tip You can also specify domain-qualified usernames by using the format *DOMAIN\username*. For example, if you specify `ENGINEERING\augustin`, ACS generates a PAC file named *ENGINEERING_augustin.pac*.

- **-passwd** *password*—`CSUtil.exe` uses the password specified, rather than the default password, to protect the PAC files that it generates. The password that you specify is required when the PACs it protects are loaded into an EAP-FAST end-user client.

  Note We recommend that you use a password that you devise, rather than the default password.

  PAC passwords can contain any characters and are case-sensitive. They must contain between four and 128 characters. While `CSUtil.exe` does not enforce strong password rules, we recommend that you use a strong password.

Your PAC password should:

- Be very long.
- Contain uppercase and lowercase letters.
- Contain numbers in addition to letters.
- Contain no common words or names.

Generating PAC Files

Note If you use the **-a** or **-g** option during PAC file generation, `CSUtil.exe` restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.

For more information about PACs, see About PACs, page 10-11.

To generate PAC files:

Step 1 Use the discussion in PAC File Options and Examples, page D-25, to determine the following:

- Which users for whom you want to generate PAC files. If you want to use a list of users, create it now.
- What password to use to protect the PAC files that you generate. If necessary, create a password. Your PAC password should:
  - Be very long.
  - Contain uppercase and lowercase letters.
  - Contain numbers in addition to letters.
  - Contain no common words or names.
- The full path to the directory in which you want the PAC files. If necessary, create the directory.

Step 2 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`.

Step 3 To create a PAC file for a user, type:

CSUtil.exe -t *additional arguments*

where *additional arguments* represents at least one option for specifying the users for whom to generate PAC files. You can also use the options to specify filepath and password.

Press **Enter**.

To create a PAC file for a machine, type:

CSUtil.exe -t -machine *additional arguments*

where *additional arguments* represents at least one option for specifying the users for whom to generate PAC files. You can also use the options to specify filepath and password.

Press **Enter**.

CSUtil.exe generates the PAC files for each user that is specified. The PAC files are named with the username plus a *.pac* file extension. For example, a PAC file for the username *seaniemop* would be *seaniemop.pac* and a PAC file for the domain-qualified username **ENGINEERING\augustin** would be *ENGINEERING_augustin.pac*.

If you specified a filepath, the PAC files are saved to the location that you specified. You can distribute the PAC files to the applicable end-user clients.

Posture-Validation Attributes

You can use CSUtil.exe to export, add, and delete posture-validation attributes, which are essential to Network Admission Control (NAC). For more information about NAC, see Chapter 14, "Posture Validation."

This section contains the following topics:

- Posture-Validation Attribute Definition File, page D-28
- Exporting Posture-Validation Attribute Definitions, page D-31
- Importing Posture-Validation Attribute Definitions, page D-31
- Deleting a Posture-Validation Attribute Definition, page D-33
- Default Posture-Validation Attribute Definition File, page D-35

Posture-Validation Attribute Definition File

A posture-validation attribute definition file is a text file that contains one or more posture-validation attribute definitions. Each definition comprises a definition header and several of the following described values. For an example of the contents of a posture-validation attribute definition file, see Default Posture-Validation Attribute Definition File, page D-35.

With the exception of the attribute definition header, each attribute definition value must be formatted:

name=value

where *name* is the value name and *value* is a string or integer, as specified in the following list.

Tip Use a semicolon (;) to identify lines that are comments.

Example D-1 shows an example of a posture-validation attribute definition, including a comment after the attribute definition:

Example D-1 Example Attribute Definition

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
```

```
attribute-profile=out
attribute-type=unsigned integer

; attribute 1 is reserved for the APT
```

A posture-validation attribute is uniquely defined by the combination of its vendor ID, application ID, and attribute ID. The following list provides details of these values and of each line that is required in an attribute definition:

- **[attr#*n*]**—Attribute definition header, where *n* is a unique, sequential integer, beginning with zero (0). `CSUtil.exe` uses the definition header to distinguish the beginning of a new attribute definition. Each attribute definition *must* begin with a line containing the definition header. The first attribute definition in the file *must* have the header `[attr#0]`, the second attribute definition in a file must have the header `[attr#1]`, and so on. A break in the numbering causes `CSUtil.exe` to ignore attribute definitions at the break and beyond. For example, if a file with 10 attribute definitions the fifth attribute is defined as `[attr#5]` instead of `[attr#4]`, `CSUtil.exe` ignores the attribute that is defined as `[attr#5]` and remaining five the attributes following it.

Tip The value of *n* is irrelevant to any of the ID values in the attribute definition file. For example, the 28th definition in a file must have the header `[attr#27]`, but this does not limit or otherwise define valid values for `vendor-id`, `application-id`, or `attribute-id`. Neither does it limit or define the number of posture-validation attributes that ACS supports.

- **vendor-id**—An unsigned integer, the vendor number is of the vendor associated with the posture-validation attribute. The vendor number should be the number that is assigned to the vendor in the IANA Assigned Numbers RFC. For example, `vendor-id 9` corresponds to Cisco Systems, Inc.

  Vendor IDs have one or more applications that are associated with them, identified by the `application-id` value.

- **vendor-name**—A string, the `vendor-name` appears in the ACS web interface and logs for the associated posture-validation attribute. For example, any attribute definition with a `vendor-name` of `9` could have the vendor name **Cisco**.

  Note The vendor name cannot differ for each attribute that shares the same `vendor-id`. For example, you cannot add an attribute with a `vendor-id` of `9` if the `vendor-name` is not **Cisco**.

- **application-id**—An unsigned integer, the `application-id` uniquely identifies the vendor application associated with the posture-validation attribute. For example, if the `vendor-id` is `9` and the `application-id` is `1`, the posture-validation attribute is associated with the Cisco application with an `application-id` of `1`, which is the Cisco Trust Agent (CTA), also known as a posture agent (PA).

- **application-name**—A string, the `application-name` appears in the ACS web interface and logs for the associated posture-validation attribute. For example, if the `vendor-id` is `9` and the `application-id` is `1`, the `application-name` would be `PA`, an abbreviation of posture agent, which is another term for CTA.

  Note The `application-name` cannot differ for each attribute that shares the same `vendor-id` and `application-id` pair. For example, you cannot add an attribute with a `vendor-id` of `9` and `application-id` of `1` if the `application-name` is not `PA`.

- **attribute-id**—An unsigned integer in the range of 1 to 65535, the `attribute-id` uniquely identifies the posture-validation attribute for the `vendor-id` and `attribute-id` specified.

  Note For each application, attributes 1 and 2 are reserved. If you add attributes that imply a new application, `CSUtil.exe` automatically creates attribute 1 as `Application-Posture-Token` and attribute 2 as `System-Posture-Token`.

- **attribute-name**—A string, the `attribute-name` appears in the ACS web interface and logs for the associated posture-validation attribute. For example, if the `vendor-id` is 9, the `application-id` is `1`, and the `attribute-id` is `1`, the `attribute-name` is `Application-Posture-Token`.
- **attribute-profile**—A string, the attribute profile specifies whether ACS can send the attribute in a posture-validation response, can receive the attribute in a posture-validation request, or can both send and receive the attribute during posture validation. Valid values for `attribute-profile` are:
  - **in**—ACS accepts the attribute in posture-validation requests and can log the attribute, and you can use it in internal policy rule definitions. Attributes with an `in attribute-profile` are also known as inbound attributes.
  - **out**—ACS can send the attribute in posture-validation responses but you cannot use it in internal policy rule definitions. Attributes with an `out attribute-profile` are also known as outbound attributes. The only outbound attributes that you can configure ACS to log are the attributes for Application Posture Tokens and System Posture Tokens; however, these are system-defined attributes that you cannot modify.
  - **in out**—ACS accepts the attribute in posture-validation requests and can send the attribute in posture-validation responses. Attributes with an `in out attribute-profile` are also known as inbound and outbound attributes.
- **attribute-type**—A string, the `attribute-type` specifies the kind of data that is valid in the associated attribute. For attributes whose `attribute-profile` is `in` or `in out`, the `attribute-type` determines the types of operators that are available for defining internal policy rules that use the attribute. An example of an inbound attribute is the `ServicePacks` attribute sent by CTA. An example of an outbound attribute is the `System-Posture-Token` attribute sent to CTA.

  Valid values of `attribute-type` are:
  - `boolean`
  - `string`
  - `integer`
  - `unsigned integer`
  - `ipaddr`
  - `date`
  - `version`
  - `octet-array`

  For more information about attribute data types, see Posture Validation Attribute Data Types, page 14-8.

Exporting Posture-Validation Attribute Definitions

The **-dumpAVP** option exports the current posture-validation attributes to an attribute definition file. For an explanation of the contents of a posture-validation attribute definition file, see Posture-Validation Attribute Definition File, page D-28. For an example of an attribute-definition file, see Default Posture-Validation Attribute Definition File, page D-35.

To export posture-validation attributes:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`.

Step 2 Type:

CSUtil.exe -dumpavp *filename*

where *filename* is the name of the file in which you want `CSUtil.exe` to write all attribute definitions.

Press **Enter**.

Tip When you specify *filename*, you can prefix the filename with a relative or absolute path, too. For example, **CSUtil.exe -dumpavp c:\temp\allavp.txt** writes the file *allavp.txt* in *c:\temp*.

Step 3 If you are prompted to confirm overwriting a file with the same path and name that you specified in Step 2, do one of the following:

- To overwrite the file, type **Y** and press **Enter**.

Tip To force `CSUtil.exe` to overwrite an existing file, use the **-q** option: **CSUtil.exe -q -dumpavp *filename***.

- To preserve the file, type **N**, press **Enter**, and return to Step 2.

`CSUtil.exe` writes all posture-validation attribute definitions in the file specified. To view the contents of the file, use the text editor of your choice.

Importing Posture-Validation Attribute Definitions

The **-addAVP** option imports posture-validation attribute definitions into ACS from an attribute definition file. For an explanation of the contents of a posture-validation attribute definition file, see Posture-Validation Attribute Definition File, page D-28. For an example of an attribute definition file, see Default Posture-Validation Attribute Definition File, page D-35.

Before You Begin

Because completing this procedure requires restarting the **CSAuth** service, which temporarily suspends authentication services, consider performing this procedure when demand for ACS services is low.

Use the steps in Exporting Posture-Validation Attribute Definitions, page D-31, to create a backup of posture-validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of current posture-validation attributes.

To import posture-validation attributes:

Step 1 Use the discussion in Posture-Validation Attribute Definition File, page D-28, to create a properly formatted attribute definition file. Place the file in the directory containing `CSUtil.exe` or a directory that is accessible from the computer that is running ACS.

Step 2 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`.

Step 3 Type:

CSUtil.exe -addavp *filename*

where *filename* is the name of the file in which you want `CSUtil.exe` to write all attribute definitions.

Press **Enter**.

Tip When you specify *filename*, you can prefix the filename with a relative or absolute path, too. For example, **CSUtil.exe -addavp c:\temp\addavp.txt** writes the file *addavp.txt* in *c:\temp*.

`CSUtil.exe` adds or modifies the attributes that are specified in the file. An example of a successful addition of nine posture-validation attributes is:

```
C:.../Utils 21: csutil -addavp myavp.txt
CSUtil v3.3(1.6), Copyright 1997-2001, Cisco Systems Inc
Attribute 9876:1:11 (Calliope) added to dictionary
Attribute 9876:1:3 (Clio) added to dictionary
Attribute 9876:1:4 (Erato) added to dictionary
Attribute 9876:1:5 (Euterpe) added to dictionary
Attribute 9876:1:6 (Melpomene) added to dictionary
Attribute 9876:1:7 (Polyhymnia) added to dictionary
Attribute 9876:1:8 (Terpsichore) added to dictionary
Attribute 9876:1:9 (Thalia) added to dictionary
Attribute 9876:1:10 (Urania) added to dictionary

AVPs from 'myavp.txt' were successfully added
```

Step 4 If you are ready for the imported attribute definitions to take effect, restart the **CSAuth** and **CSAdmin** services.

Caution While **CSAuth** is stopped, no users are authenticated.

To restart the **CSAuth**, **CSLog**, and **CSAdmin** services, enter the following commands at the command prompt, allowing the computer time to perform each command:

```
net stop csauth
net start csauth
net stop cslog
net start cslog
net stop csadmin
net start csadmin
```

ACS begins using the imported posture-validation attributes. Attributes that have an attribute type of `in` or `in out` are available in the web interface when you define internal policy rules.

Importing External Audit Posture-Validation Servers

To create an audit vendor file to import into the ACS dictionary:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change to the *\bin* directory (the directory containing `CSUtil.exe`).

Step 2 Type:

CSUtil.exe -addavp *filename*

where *filename* is the name of the file that contains the audit server vendor data. If the file is not located in the *\bin* directory, you must add the full path name.

The format of the file should be:

```
[attr#0]
    vendor-id=<the vendor identifier number>
    vendor-name=<the name of the vendor>
    application-id=6
    application-name=Audit
```

Step 3 Press **Enter**.

Step 4 Restart the ACS Services. Choose Windows **Programs> Administrative Tools > Services**.

Deleting a Posture-Validation Attribute Definition

The **-delAVP** option deletes a single posture-validation attribute from ACS.

Before You Begin

Because completing this procedure requires restarting the **CSAuth** service, which temporarily suspends authentication services, consider performing this procedure when demand for ACS services is low.

Use the steps in Exporting Posture-Validation Attribute Definitions, page D-31, to create a backup of posture-validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of the posture-validation attribute you want to delete.

To delete posture-validation attributes:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`.

Step 2 Type:

CSUtil.exe -delavp *vendor-ID*
application-ID
attribute-ID

For more information about vendor, application, and attribute IDs, see Posture-Validation Attribute Definition File, page D-28.

`CSUtil.exe` prompts you to confirm the attribute deletion.

Step 3 Examine the confirmation prompt and then:

- If you are certain that you want to delete the attribute identified by the confirmation prompt, type **Y** and press **Enter**.

Tip You can use the **-q** option to suppress the confirmation prompt.

- If you do not want to delete the attribute that the confirmation prompt identifies, type **N**, press **Enter**, and return to Step 2.

`CSUtil.exe` deletes the posture-validation attribute that you specified from its internal database. In the following example, `CSUtil.exe` deleted an attribute with a vendor ID of 9876, an application ID of 1, and an attribute ID of 1.

```
CSUtil v3.3, Copyright 1997-2004, Cisco Systems Inc
Are you sure you want to delete vendor 9876; application 1; attribute 1? (y/n)
y

Vendor 9876; application 1; attribute 1 was successfully deleted
```

Step 4 For the attribute deletion to take effect, restart the **CSAuth** and **CSAdmin** services.

Caution While **CSAuth** is stopped, no users are authenticated.

To restart the **CSAuth**, **CSLog**, and **CSAdmin** services, enter the following commands at the command prompt, allowing the computer time to perform each command:

```
net stop csauth
net start csauth
net stop cslog
net start cslog
net stop csadmin
net start csadmin
```

Deleted posture-validation attributes are no longer are available in ACS.

Deleting an Extended Posture-Validation Attribute Definition

To delete the extended posture-validation Property attribute contained in the Cisco:Host application:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`.

Step 2 Type:

CSUtil.exe -delPropHPP <attribute ID> <property ID>

This command removes the specific **PROPERTY** from an Extended attribute under **Cisco:Host**.

For more information about vendor, application, and attribute IDs, see Posture-Validation Attribute Definition File, page D-28.

To delete extended posture-validation **ENTITY** attributes in the **Cisco:Host** application:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing `CSUtil.exe`.

Step 2 Type:

CSUtil.exe -delEntHPP <attribute ID> <entity name>

This command removes the specific **ENTITY** from an Extended attribute under **Cisco:Host**.

For more information about vendor, application, and attribute IDs, see Posture-Validation Attribute Definition File, page D-28.

Note Extended attributes are supported only as descendants of the **Cisco:Host** application.

Default Posture-Validation Attribute Definition File

Example D-2 provides the definitions for the posture-validation attributes that we provide with ACS. This example is contained in the file *acs4.0_avp.txt*, in the *\Utils* folder. If you need to reset the default attributes to their original definitions, use the syntax in Example D-2 to create a posture-validation attribute definition file. For more information about the format of an attribute definition file, see Posture-Validation Attribute Definition File, page D-28.

Example D-2 Default Posture-Validation Attribute Definitions

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#1]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00002
attribute-name=System-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#2]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00003
attribute-name=PA-Name
attribute-profile=in out
attribute-type=string
```

```
[attr#3]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00004
attribute-name=PA-Version
attribute-profile=in out
attribute-type=version

[attr#4]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00005
attribute-name=OS-Type
attribute-profile=in out
attribute-type=string

[attr#5]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00006
attribute-name=OS-Version
attribute-profile=in out
attribute-type=version

[attr#6]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00007
attribute-name=PA-User-Notification
attribute-profile=out
attribute-type=string

[attr#7]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00008
attribute-name=OS-Release
attribute-profile=in out
attribute-type=string

[attr#8]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00009
attribute-name=Kernel-Version
attribute-profile=in out
attribute-type=version

[attr#9]
vendor-id=9
vendor-name=Cisco
```

```
application-id=1
application-name=PA
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=string

[attr#10]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00011
attribute-name=Machine-Posture-State
attribute-profile=in out
attribute-type=unsigned integer

[attr#11]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00001
attribute-name=Application-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#12]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00002
attribute-name=System-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#13]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00006
attribute-name=ServicePacks
attribute-profile=in
attribute-type=string

[attr#14]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00007
attribute-name=HotFixes
attribute-profile=in
attribute-type=string

[attr#15]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00008
attribute-name=HostFQDN
```

```
attribute-profile=in
attribute-type=string

[attr#16]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00100
attribute-name=Package
attribute-profile=in
attribute-type=string

[attr#17 (extended)]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00100
attribute-name=Package
entities-list=acrobat;cpio;cups;curl;cvs;cyrus-sasl;emacs;enscript;ethereal;evolution;gaim
;gd;gdk-pixbuf;glibc;gnome-vfs2;gnupg;gtk2;httpd;ia32el;imagemagick;imap;imlib;iproute;ips
ec-tools;kdegraphics;kdelibs;kdenetwork;kdepim;kernel;krb5;less;lftp;lha;libpng;libtiff;li
bxml;libxml2;mailman;mod_python;mozilla;mutt;mysql;mysql-server;nasm;net-snmp;netpbm;nfs-u
tils;openmotif;openoffice.org;openssh;openssl;perl;perl-dbi;php;postgresql;pwlib;python;qt
;realplayer;redhat-config-nfs;rh-postgresql;rsh;rsync;ruby;samba;sharutils;slocate;sox;spa
massassin;squid;squirrelmail;sysstat;tcpdump;telnet;tetex;utempter;vim;xchat;xemacs;xfree8
6;xloadimage;xpdf;zip;
property-id=4
property-name=Version
attribute-profile=in
attribute-type=version

[attr#18 (extended)]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00100
attribute-name=Package
entities-list=acrobat;cpio;cups;curl;cvs;cyrus-sasl;emacs;enscript;ethereal;evolution;gaim
;gd;gdk-pixbuf;glibc;gnome-vfs2;gnupg;gtk2;httpd;ia32el;imagemagick;imap;imlib;iproute;ips
ec-tools;kdegraphics;kdelibs;kdenetwork;kdepim;kernel;krb5;less;lftp;lha;libpng;libtiff;li
bxml;libxml2;mailman;mod_python;mozilla;mutt;mysql;mysql-server;nasm;net-snmp;netpbm;nfs-u
tils;openmotif;openoffice.org;openssh;openssl;perl;perl-dbi;php;postgresql;pwlib;python;qt
;realplayer;redhat-config-nfs;rh-postgresql;rsh;rsync;ruby;samba;sharutils;slocate;sox;spa
massassin;squid;squirrelmail;sysstat;tcpdump;telnet;tetex;utempter;vim;xchat;xemacs;xfree8
6;xloadimage;xpdf;zip;
property-id=5
property-name=Version-String
attribute-profile=in
attribute-type=string

[attr#19]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00001
attribute-name=Application-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#20]
```

```
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00002
attribute-name=System-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#21]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00005
attribute-name=CSAVersion
attribute-profile=in
attribute-type=version

[attr#22]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00009
attribute-name=CSAOperationalState
attribute-profile=in
attribute-type=unsigned integer

[attr#23]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32768
attribute-name=CSAMCName
attribute-profile=in
attribute-type=string

[attr#24]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32769
attribute-name=CSAStates
attribute-profile=in
attribute-type=string

[attr#25]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32770
attribute-name=DaysSinceLastSuccessfulPoll
attribute-profile=in
attribute-type=unsigned integer
```

VPDN Processing

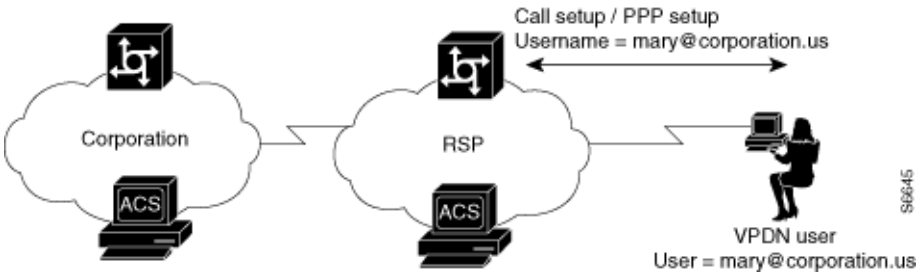
Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, supports authentication forwarding of virtual private dial-up network (VPDN) requests. There are two basic types of roaming users: Internet and intranet; VPDN addresses the requirements of roaming intranet users. This chapter provides information about the VPDN process and how it affects the operation of ACS.

VPDN Process

This section describes the steps for processing VPDN requests in a standard environment.

1. A VPDN user dials in to the network access server (NAS) of the regional service provider (RSP). The standard call/point-to-point protocol (PPP) setup is done. A username and password are sent to the NAS in the format *username@domain* (for example, *mary@corporation.us*). See Figure E-1.

Figure E-1 VPDN User Dials In



2. If VPDN is enabled, the NAS assumes that the user is a VPDN user. The NAS strips off the *username@* (*mary@*) portion of the username and authorizes (not authenticates) the domain portion (*coporation.us*) with the ACS. See Figure E-2.

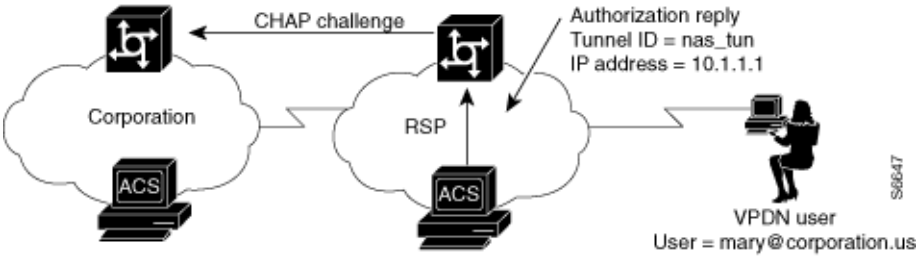
Figure E-2 NAS Attempts to Authorize Domain

3. If the domain authorization fails, the NAS assumes that the user is not a VPDN user. The NAS then authenticates (not authorizes) the user as if the user is a standard non-VPDN dial user. See Figure E-3.

Figure E-3 Authorization of Domain Fails

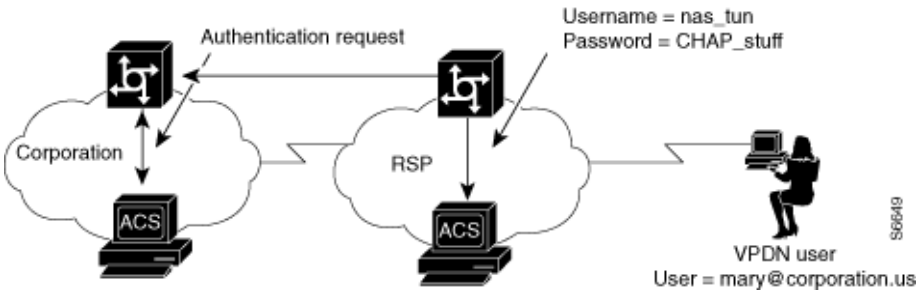
If the ACS authorizes the domain, it returns the Tunnel ID and the IP address of the home gateway (HG); these are used to create the tunnel. See Figure E-4.

Figure E-4 ACS Authorizes Domain



4. The HG uses its ACS to authenticate the tunnel, where the username is the name of the tunnel (**nas_tun**). See Figure E-5.

Figure E-5 HG Authenticates Tunnel with ACS

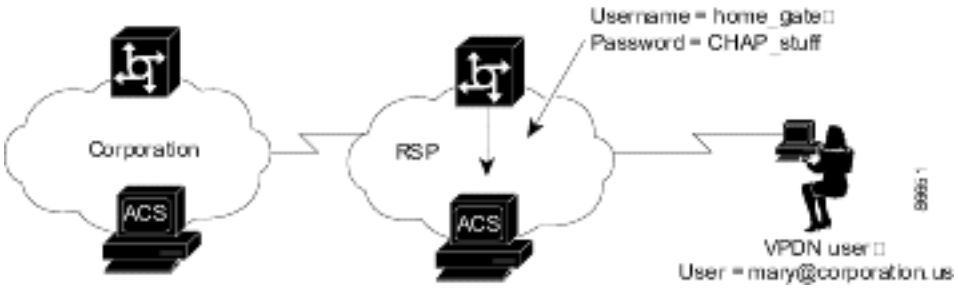


5. The HG now authenticates the tunnel with the NAS, where the username is the name of the HG. This name is chosen based on the name of the tunnel, so the HG might have different names depending on the tunnel being set up. See Figure E-6.

Figure E-6 HG Authenticates Tunnel with the NAS

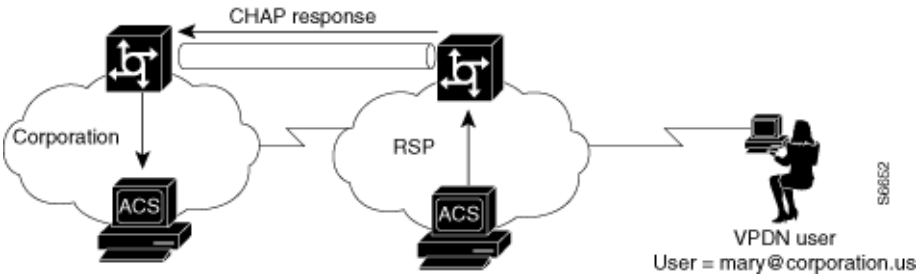
6. The NAS now uses its ACS to authenticate the tunnel from the HG. See Figure E-7.

Figure E-7 NAS Authenticates Tunnel with ACS



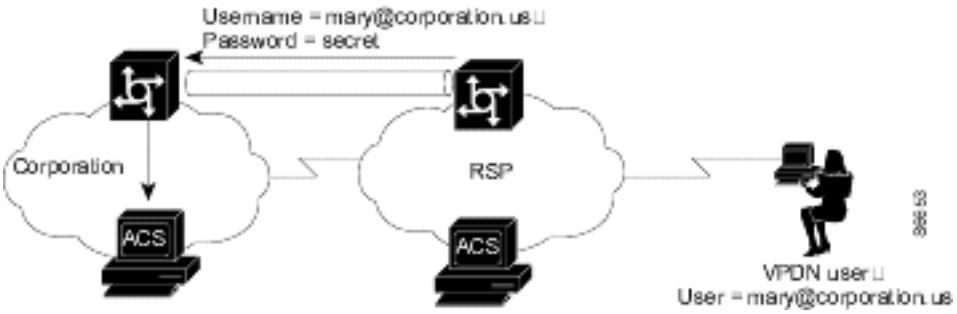
7. After authenticating, the tunnel is established. Now the actual user (*mary@corporation.us*) must be authenticated. See Figure E-8.

Figure E-8 VPDN Tunnel is Established



8. The HG now authenticates the user as if the user dialed directly in to the HG. The HG might now challenge the user for a password. The ACS at RSP can be configured to strip off the at symbol (@) and domain before it passes the authentication to the HG. (The user is passed as *mary@corporation.us*.) The HG uses it ACS to authenticate the user. See Figure E-9.

Figure E-9 HG Uses ACS to Authenticate User



9. If another user (*sue@corporation.us*) dials in to the NAS while the tunnel is up, the NAS does not repeat the entire authorization and authentication process. Instead, it passes the user through the existing tunnel to the HG. See Figure E-10.

Figure E-10 Another User Dials In While Tunnel is Up

RDBMS Synchronization Import Definitions

RDBMS synchronization import definitions are a listing of the action codes allowable in an accountActions table. The RDBMS Synchronization feature of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, uses a table named accountActions as input for automated or manual updates of the ACS internal database. For more information about the RDBMS Synchronization feature and accountActions, see RDBMS Synchronization, page 9-17.

This chapter contains the following topics:

- accountActions Specification, page F-1
- Supported Versions for ODBC Datasources, page F-3
- Action Codes, page F-3
- ACS Attributes and Action Codes, page F-22
- An Example of accountActions, page F-25

accountActions Specification

Whether you create accountActions by hand in a text editor or through automation using a third-party system that writes to accountActions, you must adhere to the accountActions specification and must only use the action codes detailed in Action Codes, page F-3. Otherwise, RDBMS Synchronization may import incorrect information into the ACS internal database or may fail to occur at all.

accountActions Format

Each row in accountActions has 14 fields (or columns). Table F-1 lists the fields that compose accountActions. Table F-1 also reflects the order in which the fields appear in accountActions.

The one-letter or two-letter abbreviations given in the Mnemonic column are a shorthand notation used to indicate required fields for each action code in Action Codes, page F-3.

To see an example accountActions, see An Example of accountActions, page F-25.

Table F-1 accountActions Fields

Field Name	Mnemonic	Type	Size (Max. Length)	Comments
SequenceId	SI	AutoNumber	32	The unique action ID.
Priority	P	Integer	1	The priority with which this update is to be treated. Zero (0) is the lowest priority.
UserName	UN	String	32	The name of the user to which the transaction applies.
GroupName	GN	String	32	The name of the group to which the transaction applies.
Action	A	Number	$0\text{-}2^{16}$	The action required. (See Action Codes, page F-3.)
ValueName	VN	String	255	The name of the parameter to change.
Value1	V1	String	255	The new value (for numeric parameters, this is a decimal string).
Value2	V2	String	255	The name of a TACACS+ protocol; for example, “ip” or RADIUS VSA Vendor ID.
Value3	V3	String	255	The name of a TACACS+ service; for example, “ppp” or the RADIUS VSA attribute number.
DateTime	DT	DateTime	—	The date and time the action was created.
MessageNo	MN	Integer	—	Used to number related transactions for audit purposes.
ComputerNames	CN	String	32	RESERVED by CSDBSync.
AppId	AI	String	255	The type of configuration parameter to change.
Status	S	Number	32	TRI-STATE:0=not processed, 1=done, 2=failed. This value should normally be set to 0.

accountActions Mandatory Fields

For all actions, the following fields cannot be empty and must have a valid value:

- Action
- SequenceID
- Status

In addition to the previous required fields, the DateTime, UserName and GroupName fields are also often required to have a valid value:

- If a transaction is acting upon a user account, a valid value is required in the UserName field.
- If a transaction is acting upon a group, a valid value is required in the GroupName field.
- If a transaction is acting upon a AAA client configuration, neither the UserName field nor the GroupName field require a value.

Note The UserName and GroupName fields are mutually exclusive; only one of these two fields can have a value and neither field is always required.

accountActions Processing Order

ACS reads rows from accountActions and processes them in a specific order. ACS determines the order first by the values in the Priority fields (mnemonic: P) and then by the values in the Sequence ID fields (mnemonic: SI). ACS processes the rows with the highest Priority field. The lower the number in the Priority field, the higher the priority. For example, if row A has the value 1 in its Priority field and row B has the value 2 in its Priority field, ACS would process row A first, regardless of whether row B has a lower sequence ID or not. If rows have an equal priority, ACS processes them by their sequence ID, with the lowest sequence ID processed first.

Thus, the Priority field (P) enables transactions of higher importance to occur first, such as deleting a user or changing a password. In the most common implementations of RDBMS Synchronization, a third-party system writes to accountActions in batch mode, with all actions (rows) assigned a priority of zero (0).

Note When changing transaction priorities, be careful that they are processed in the correct order; for example, a user account must be created before the user password is assigned.

You can use the MessageNo field (mnemonic: MN) to associate related transactions, such as the addition of a user and subsequent actions to set password values and status. You can use the MessageNo field to create an audit trail for a third-party system that writes to accountActions.

Supported Versions for ODBC Datasources

The following versions are supported for RDBMS synchronization through ODBC.

- MS-SQL version 3.80 later
- ODBC version 3.80 or later

Action Codes

This section provides the action codes valid for use in the Action field (mnemonic: A) of accountActions. The Required column uses the field mnemonic names to indicate which fields should be completed, except for the mandatory fields, which are assumed. For more information about the mnemonic names of accountActions fields, see Table F-1. For more information about the mandatory fields, see accountActions Mandatory Fields, page F-2.

If an action can be applied to a user or group, UN|GN appears, using the vertical bar (|) to indicate that either one of the two fields is required. To make the action affect only the user, leave the group name empty; to make the action affect only the group, leave the user name empty.

This section contains the following topics:

- Action Codes for Setting and Deleting Values, page F-4
- Action Codes for Creating and Modifying User Accounts, page F-4
- Action Codes for Initializing and Modifying Access Filters, page F-9
- Action Codes for Modifying TACACS+ and RADIUS Group and User Settings, page F-12
- Action Codes for Modifying Network Configuration, page F-17

Action Codes for Setting and Deleting Values

The two most fundamental action codes are SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2), described in Table F-2.

The SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2) actions, described in Table F-2, instruct RDBMS Synchronization to assign a value to various internal attributes in ACS. Unless a Cisco representative asks you to use these action codes for other purposes, you can only use these action codes for assigning values to user-defined fields (see User-Specific Attributes, page F-22).

Table F-2 Action Codes for Setting and Deleting Values

Action Code	Name	Required	Description

1	SET_VALUE	UN|GN, AI, VN, V1, V2	Sets a value (V1) named (VN) of type (V2) for App ID (AI).
			App IDs (AI) can be one of the following:
			• APP_CSAUTH
			• APP_CSTACACS
			• APP_CSRADIUS
			• APP_CSADMIN
			Value types (V2) can be one of the following:
			• **TYPE_BYTE**—Single 8-bit number.
			• **TYPE_SHORT**—Single 16-bit number.
			• **TYPE_INT**—Single 32-bit number.
			• **TYPE_STRING**—Single string.
			• **TYPE_ENCRYPTED_STRING**—Single string to be saved encrypted.
			• **TYPE_MULTI_STRING**—Tab-separated set of substrings.
			• **TYPE_MULTI_INT**—Tab-separated set of 32-bit numbers.
			For example:
			`UN = "fred"`
			`AI = "APP_CSAUTH"`
			`VN = "My Value"`
			`V2 = "TYPE_MULTI_STRING"`
			`V1 = "str1`*tab*`str2`*tab*`str3"`

2	DELETE_VALUE	UN|GN, AI, VN	Deletes value (VN) for App ID (AI) and user (UN) or group (GN).

Action Codes for Creating and Modifying User Accounts

Table F-3 lists the action codes for creating, modifying, and deleting user accounts.

Note Before you can modify a user account, such as assigning a password, you must create the user account, in the web interface or by using the ADD_USER action (action code: 100).

Transactions using these codes affect the configuration that appears in the User Setup section of the web interface. For more information about the User Setup section, see Chapter 7, "User Management."

Table F-3 User Creation and Modification Action Codes

Action Code	Name	Required	Description
100	ADD_USER	UN|GN, V1	Creates a user (32 characters maximum). V1 is used as the initial password. Optionally, the user can also be assigned to a group.
101	DELETE_USER	UN	Removes a user.
102	SET_PAP_PASS	UN, V1	Sets the PAP password for a user (64 ASCII characters maximum). CHAP/ARAP will also default to this.
103	SET_CHAP_PASS	UN, V1	Sets the CHAP/ARAP password for a user (64 characters maximum).
104	SET_OUTBOUND_CHAP_PASS	UN, V1	Sets the CHAP/ARAP password for a user (32 characters maximum).
105	SET_T+_ENABLE_PASS	UN, VN, V1, V2, V3	Sets the TACACS+ enable password (V1) (32 characters maximum) and Max Privilege level (V2) (0-15). The enable type (V3) should be one of the following: • **ENABLE_LEVEL_AS_GROUP**—Max privilege taken from group setting. • **ENABLE_LEVEL_NONE**—No T+ enable configured. • **ENABLE_LEVEL_STATIC**—Value set in V2 used during enable level check. You can use VN to link the enable password to an external authenticator, as per action 108 SET_PASS_TYPE.
106	SET_GROUP	UN, GN	Sets the ACS group assignment of the user.
108	SET_PASS_TYPE	UN|GN, V1	Sets the password type of the user. This can be one of the ACS internal database password types or any of the external databases supported: • **PASS_TYPE_CSDB**—CSDB internal password. • **PASS_ TYPE_CSDB_UNIX**—CSDB internal password (UNIX encrypted). • **PASS_TYPE_NT**—External Windows user database password. • **PASS_TYPE_NDS**—External Novell database password. • **PASS_TYPE_LDAP**—External generic LDAP database password. • **PASS_TYPE_LEAP**—External LEAP proxy RADIUS server database password. • **PASS_TYPE_RADIUS_TOKEN**—External RADIUS token server database password.

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
109	REMOVE_PASS_STATUS	UN,V1	Removes a password status flag. This action results in the status states being linked in a logical XOR condition. V1 should contain one of the following: • **PASS_STATUS_EXPIRES**—Password expires on a given date. • **PASS_STATUS_NEVER**—Password never expires. • **PASS_STATUS_WRONG**—Password expires after a given number of login attempts using the wrong password. • **PASS_STATUS_DISABLED**—The account has been disabled.
110	ADD_PASS_STATUS	UN, V1	Defines how a password should be expired by ACS. To set multiple password states for a user, use multiple instances of this action. This action results in the status states being linked in a logical XOR condition. V1 should contain one of the following: • **PASS_STATUS_EXPIRES**—Password expires on a given date. • **PASS_STATUS_NEVER**—Password never expires. • **PASS_STATUS_WRONG**—Password expires after a given number of login attempts by using the wrong password. • **PASS_STATUS_RIGHT**—Password expires after a given number of login attempts by using the correct password. • **PASS_STATUS_DISABLED**—The account has been disabled.
112	SET_PASS_EXPIRY_WRONG	UN,V1	Sets the maximum number of bad authentications allowed (automatic reset on good password if not exceeded) and resets the current count.
113	SET_PASS_EXPIRY_DATE	UN,V1	Sets the date on which the account expires. The date format should be YYYYMMDD.
114	SET_MAX_SESSIONS	UN|GN, V1	Sets the maximum number of simultaneous sessions for a user or group. V1 should contain one of the following values: • MAX_SESSIONS_UNLIMITED • MAX_SESSIONS_AS_GROUP • 1-65534
115	SET_MAX_SESSIONS_GROUP_USER	GN,V1	Sets the max sessions for a user of the group to one of the following values: • MAX_SESSIONS_UNLIMITED • 1-65534

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
260	SET_QUOTA	VN,V1, V2	Sets a quota for a user or group. VN defines the quota type. Valid values are: • **online time**—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. • **sessions**—The quota limits the user or group by the number of sessions on the network for the period defined in V2. V1 defines the quota. If VN is set to sessions, V1 is the maximum number of sessions in the period defined in V2. If VN is set to online time, V1 is the maximum number of seconds. V2 holds the period for the quota. Valid values are: • **QUOTA_PERIOD_DAILY**—The quota is enforced in 24-hour cycles, from 12:01 A.M. to midnight. • **QUOTA_PERIOD_WEEKLY**—The quota is enforced in 7-day cycles, from 12:01 A.M. Sunday until midnight Saturday. • **QUOTA_PERIOD_MONTHLY**—The quota is enforced in monthly cycles, from 12:01 A.M. on the first of the month until midnight on the last day of the month. • **QUOTA_PERIOD_ABSOLUTE**—The quota is enforced in an ongoing basis, without an end.
261	DISABLE_QUOTA	UN|GN, VN	Disables a group or user usage quota. VN defines the quota type. Valid values are: • **online time**—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. • **sessions**—The quota limits the user or group by the number of sessions on the network for the period defined in V2.
262	RESET_COUNTERS	UN|GN	Resets usage quota counters for a user or group.
263	SET_QUOTA_APPLY_TYPE	V1	Defines whether a user usage quota is determined by the user group quota or by a quota unique to the user. V1 makes this specification. Valid values for V1 are: • ASSIGNMENT_FROM_USER • ASSIGNMENT_FROM_GROUP

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
270	SET_DCS_TYPE	UN|GN, VN,V1, Optional-ly V2	Sets the type of device command set (DCS) authorization for a group or user. VN defines the service. Valid service types are: • **shell**—Cisco IOS shell command authorization. • **pixshell**—Cisco PIX command authorization. **Note** If additional DCS types have been added to your ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as: `PIX Shell (pixshell)` V1 defines the assignment type. The valid values for VN are: • **none**—Sets no DCS for the user or group. • **as group**—For users only, this value signifies that the user DCS settings for the service specified should be the same as the user group DCS settings. • **static**—Sets a DCS for the user or group for all devices enabled to perform command authorization for the service specified. If V1 is set to static, V2 is required and must contain the name of the DCS to assign to the user or group for the given service. • **ndg**—Specifies that command authorization for the user or group is to be done on a per-NDG basis. Use action 271 to add DCS to NDG mappings for the user or group. **Note** Changing a user or group assignment type (V1) results in clearing previous data, including NDG to DCS mappings (defined by action 271).

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
271	SET_DCS_NDG_MAP	UN|GN, VN,V1, V2	Use this action code to map between the device command set and the NDG when the assignment type specified by a 270 action code is `ndg`. VN defines the service. Valid service types are: • **shell**—Cisco IOS shell command authorization. • **pixshell**—Cisco PIX command authorization. **Note** If additional DCS types have been added to your ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as: `PIX Shell (pixshell)` V1 defines the name of the NDG. Use the name of the NDG as it appears in the web interface. For example, if you have configured an NDG named *East Coast NASs* and want to use action 271 to apply a DCS to that NDG, V1 should be *East Coast NASs*. V2 defines the name of the DCS. Use the name of the DCS as it appears in the web interface. For example, if you have configured a DCS named *Tier2 PIX Admin DCS* and want to use action 271 to apply it to an NDG, V2 should be *Tier2 PIX Admin DCS*.

Action Codes for Initializing and Modifying Access Filters

Table F-4 lists the action codes for initializing and modifying AAA client access filters. AAA client access filters control Telnet access to a AAA client. Dial access filters control access by dial-up users.

Transactions using these codes affect the configuration that appears in the User Setup and Group Setup sections of the web interface. For more information about the User Setup section, see Chapter 7, "User Management." For more information about the Group Setup section, see Chapter 6, "User Group Management."

Table F-4 Action Codes for Initializing and Modifying Access Filters

Action Code	Name	Required	Description
120	INIT_NAS_ACCESS_CONTROL	UN|GN,V1	Clears the AAA client access filter list and initialize permit or deny for any forthcoming filters. V1 should be one of the following values: • ACCESS_PERMIT • ACCESS_DENY
121	INIT_DIAL_ACCESS_CONTROL	UN|GN,V1	Clears the dial-up access filter list and initialize permit/deny for any forthcoming filters. V1 should be one of the following values: • ACCESS_PERMIT • ACCESS_DENY
122	ADD_NAS_ACCESS_FILTER	UN|GN,V1	Adds a AAA client filter for the user|group. V1 should contain a single (AAA client name, AAA client port, remote address, CLID) tuple; for example: `NAS01,tty0,0898-69696969` Optionally, the AAA client name can be *All AAA clients* to specify that the filter applies to all configured AAA clients and an asterisk (*) to represent all ports.

123	ADD_DIAL_ACCESS_FILTER	UN|GN, V1, V2	Adds a dial-up filter for the user|group.
			V1 should contain one of the following values:
			• Calling station ID
			• Called station ID
			• Calling and called station ID; for example:
			`01732-875374,0898-69696969`
			• NAS IP address, NAS port; for example:
			`10.45.6.123,tty0`
			V2 should contain the filter type as one of the following values:
			• **CLID**—The user is filtered by the calling station ID.
			• **DNIS**—The user is filtered by the called station ID.
			• **CLID/DNIS**—The user is filtered by calling and called station IDs.
			• **NAS/PORT**—The user is filtered by NAS IP and NAS port address.

130	SET_TOKEN_CACHE_SESSION	GN, V1	Enables or disables token caching for an entire session; V1 is 0=disable, 1=enable.
131	SET_TOKEN_CACHE_TIME	GN, V1	Sets the duration that tokens are cached. V1 is the token cache duration in seconds.

Table F-4 Action Codes for Initializing and Modifying Access Filters (continued)

Action Code	Name	Required	Description
140	SET_TODDOW_ACCESS	UN|GN, V1	Sets periods during which access is permitted. V1 contains a string of 168 characters. Each character represents a single hour of the week. A `1` represents an hour that is permitted, while a `0` represents an hour that is denied. If this parameter is not specified for a user, the group setting applies. The default group setting is `111111111111` and so on.
150	SET_STATIC_IP	UN, V1, V2	Configures the (TACACS+ and RADIUS) IP address assignment for this user. V1 holds the IP address in the following format: *xxx.xxx.xxx.xxx* V2 should be one of the following: • **ALLOC_METHOD_STATIC**—The IP address in V1 is assigned to the user in the format xxx.xxx.xxx.xxx. • **ALLOC_METHOD_NAS_POOL**—The IP pool named in V1 (configured on the AAA client) will be assigned to the user. • **ALLOC_METHOD_AAA_POOL**—The IP pool named in V1 (configured on the AAA server) will be assigned to the user. • **ALLOC_METHOD_CLIENT**—The dial-in client will assign its own IP address. • **ALLOC_METHOD_AS_GROUP**—The IP address assignment configured for the group will be used.
151	SET_CALLBACK_NO	UN|GN, V1	Sets the callback number for this user or group (TACACS+ and RADIUS). V1 should be one of the following: • **Callback number**—The phone number the AAA client is to call back. • **none**—No callback is allowed. • **roaming**—The dial-up client determines the callback number. • **as group**—Use the callback string or method defined by the group.

Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Table F-5 lists the action codes for creating, modifying, and deleting TACACS+ and RADIUS settings for ACS groups and users. In the event that ACS has conflicting user and group settings, user settings always override group settings.

Transactions using these codes affect the configuration displayed in the User Setup and Group Setup sections of the web interface. For more information about the User Setup section, see Chapter 7, "User Management." For more information about the Group Setup section, see Chapter 6, "User Group Management."

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Action Code	Name	Required	Description

161	DEL_RADIUS_ATTR	UN|GN, VN, Optionally V2, V3	Deletes the named RADIUS attribute for the group or user, where:
			• VN = "Vendor-Specific"
			• V2 = IETF vendor ID
			• V3 = VSA attribute ID
			For example, to specify the Cisco IOS/PIX vendor ID and the Cisco AV Pair:
			`VN = "Vendor-Specific"`
			`V2 = "9"`
			`V3 = "1"`

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

163	ADD_RADIUS_ ATTR	UN|GN, VN, V1, Optionally V2, V3	Adds to the attribute named (VN) the value (V1) for the user/group (UN|GN). For example, to set the IETF RADIUS Reply-Message attribute (attr. 18) for a group:
			`GN = "Group 1"`
			`VN = "Reply-Message"`
			`V1 = "Greetings"`
			As another example, to set the IETF RADIUS Framed-IP-Address attribute (attr. 9) for a user:
			`UN = "fred"`
			`VN = "Framed-IP-Address"`
			`V1 = "10.1.1.1"`
			To add a vendor-specific attribute (VSA), set VN = "Vendor-Specific" and use V2 and V3 as follows:
			• V2 = IETF vendor ID
			• V3 = VSA attribute ID
			For example, to add the Cisco IOS/PIX RADIUS cisco-av-pair attribute with a value of "addr-pool=pool1":
			`VN="Vendor-Specific"`
			`V1 = "addr-pool=pool1"`
			`V2 = "9"`
			`V3 = "1"`
			RADIUS attribute values can be one of the following:
			• INTEGER
			• TIME
			• IP ADDRESS
			• STRING

170	ADD_TACACS_SERVICE	UN|GN, VN, V1, V3, Optionally V2	Permits the service for that user or group of users. For example:
			`GN = "Group 1"`
			`V1 = "ppp"`
			`V2 = "ip"`
			or
			`UN = "fred"`
			`V1 = "ppp"`
			`V2 = "ip"`
			or
			`UN = "fred"`
			`V1= "exec"`

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

171	REMOVE_TACACS_SERVICE	UN|GN, V1
		Optionally V2
			Denies the service for that user or group of users. For example:
			`GN = "Group 1"`
			`V1 = "ppp"`
			`V2 = "ip"`
			or
			`UN = "fred"`
			`V1 = "ppp"`
			`V2 = "ip"`
			or
			`UN = "fred"`
			`V1 = "exec"`
			This also resets the valid attributes for the service.

172	ADD_TACACS_ATTR	UN|GN, VN, V1, V3
		Optionally V2
			Sets a service-specific attribute. The service must already have been permitted via the web interface or using Action 170:
			`GN = "Group 1"`
			`VN = "routing"`
			`V1 = "ppp"`
			`V2 = "ip"`
			`V3 = "true"`
			or
			`UN = "fred"`
			`VN = "route"`
			`V1 = "ppp"`
			`V2 = "ip"`
			`V3 = 10.2.2.2`

173	REMOVE_TACACS_ATTR	UN|GN, VN, V1
		Optionally V2
			Removes a service-specific attribute:
			`GN = "Group 1"`
			`V1 = "ppp"`
			`V2 = "ip"`
			`VN = "routing"`
			or
			`UN = "fred"`
			`V1 = "ppp"`
			`V2 = "ip"`
			`VN = "route"`

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

174	ADD_IOS_COMMAND	UN|GN, VN, V1	Authorizes the given Cisco IOS command and determines if any arguments given to the command are to be found in a defined set or are not to be found in a defined set. The defined set is created using Actions 176 and 177:
			`GN = "Group 1"`
			`VN = "telnet"`
			`V1 = "permit"`
			or
			`UN = "fred"`
			`VN = "configure"`
			`V1 = "deny"`
			The first example permits the Telnet command to be authorized for users of Group 1. Any arguments can be supplied to the Telnet command as long as they are not matched against any arguments defined via Action 176.
			The second example permits the **configure** command to be authorized for user *fred*, but only if the arguments supplied are permitted by the filter defined by a series of Action 176.

175	REMOVE_IOS_COMMAND	UN|GN, VN	Removes command authorization for the user or group:
			`GN = "Group 1"`
			`VN = "telnet"`
			or
			`UN = "fred"`
			`VN = "configure"`
			Users of Group 1 can no longer use the Cisco IOS **telnet** command.
			User fred can no longer use the **configure** command.

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

176	ADD_IOS_COMMAND_ARG	UN|GN, VN, V1, V2	Specifies a set of command-line arguments that are permitted or denied for the Cisco IOS command contained in VN. The command must have already been added via Action 174:
			`GN = "Group 1"`
			`VN = "telnet"`
			`V1 = "permit"`
			`V2 = "10.1.1.2"`
			or
			`UN = "fred"`
			`VN = "show"`
			`V1 = "deny"`
			`V2 = "run"`
			The first example will allow the **telnet** command with argument 10.1.1.2 to be used by any user in Group 1.
			The second example ensures that user fred cannot issue the Cisco IOS command **show run**.

177	REMOVE_IOS_COMMAND_ARG	UN|GN, VN, V2	Removes the permit or deny entry for the given Cisco IOS command argument:
			`GN = "Group 1"`
			`VN = "telnet"`
			`V2 = "10.1.1.1"`
			or
			`UN = "fred"`
			`VN = "show"`
			`V2 = "run"`

178	SET_PERMIT_DENY_ UNMATCHED_IOS_COMMANDS	UN|GN, V1	Sets unmatched Cisco IOS command behavior. The default is that any Cisco IOS commands not defined via a combination of Actions 174 and 175 will be denied. This behavior can be changed so that issued Cisco IOS commands that do not match any command/command argument pairs are authorized:
			`GN = "Group 1"`
			`V1 = "permit"`
			or
			`UN = "fred"`
			`V1 = "deny"`
			The first example will permit any command not defined by Action 174.

179	REMOVE_ALL_IOS_COMMANDS	UN|GN	This action removes all Cisco IOS commands defined for a particular user or group.
210	RENAME_GROUP	GN,V1	Renames an existing group to the name supplied in V1.

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
211	RESET_GROUP	GN	Resets a group back to the factory default.
212	SET_VOIP	GN, V1	Enables or disables Voice over IP (VoIP) support for the group named: • GN = name of group • V1 = ENABLE or DISABLE

Action Codes for Modifying Network Configuration

Table F-6 lists the action codes for adding AAA clients, AAA servers, network device groups, and proxy table entries. Transactions using these codes affect the configuration that appears in the Network Configuration section of the web interface. For more information about the Network Configuration section, see Chapter 4, "Network Configuration."

Table F-6 Action Codes for Modifying Network Configuration

Action Code	Name	Required	Description

220	ADD_NAS	VN, V1, V2, V3	Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and vendor (V3). Valid vendors are:
			• **VENDOR_ID_IETF_RADIUS**—For IETF RADIUS.
			• **VENDOR_ID_CISCO_RADIUS**—For Cisco IOS/PIX RADIUS.
			• **VENDOR_ID_CISCO_TACACS**—For Cisco TACACS+.
			• VENDOR_ID_AIRESPACE_RADIUS —For Cisco Airespace RADIUS.
			• **VENDOR_ID_ASCEND_RADIUS**—For Ascend RADIUS.
			• **VENDOR_ID_ALTIGA_RADIUS**—For Cisco 3000/ASA/PIX 7.x+ RADIUS.
			• **VENDOR_ID_AIRONET_RADIUS**—For Cisco Aironet RADIUS.
			• **VENDOR_ID_NORTEL_RADIUS**—For Nortel RADIUS.
			• **VENDOR_ID_JUNIPER_RADIUS**—For Juniper RADIUS.
			• **VENDOR_ID_CBBMS_RADIUS**—For Cisco BBMS RADIUS.
			For example:
			`VN = AS5200-11`
			`V1 = 192.168.1.11`
			`V2 = byZantine32`
			`V3 = VENDOR_ID_CISCO_RADIUS`

221	SET_NAS_FLAG	VN, V1	Sets one of the per-AAA client flags (V1) for the named AAA client (VN). Use the action once for each flag required. Valid values for per-AAA client flags are: • FLAG_SINGLE_CONNECT • FLAG_LOG_KEEP_ALIVE • FLAG_LOG_TUNNELS
222	DEL_HOST	VN	Deletes the named AAA client (VN).
223	ADD_NAS_BY_IETF_CODE	VN,V1, V2, V3	Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and the enterprise code for the vendor (V3).
230	ADD_AAA_SERVER	VN, V1, V2	Adds a new AAA server named (VN) with IP address (V1), shared secret key (V2).

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
231	SET_AAA_TYPE	VN, V1	Sets the AAA server type for server (VN) to value in V1, which should be one of the following: • TYPE_ACS • TYPE_TACACS • TYPE_RADIUS The default is AAA_SERVER_TYPE_ACS.
232	SET_AAA_FLAG	VN, V1	Sets one of the per-AAA client flags (V1) for the named AAA server (VN): • FLAG_LOG_KEEP_ALIVE • FLAG_LOG_TUNNELS Use the action once for each flag required.
233	SET_AAA_TRAFFIC_TYPE	VN, V1	Sets the appropriate traffic type (V1) for the named AAA server (VN): • TRAFFIC_TYPE_INBOUND • TRAFFIC_TYPE_OUTBOUND • TRAFFIC_TYPE_BOTH The default is TRAFFIC_TYPE_BOTH.
234	DEL_AAA_SERVER	VN	Deletes the named AAA server (VN).
240	ADD_PROXY	VN, V1, V2, V3	Adds a new proxy markup (VN) with markup type (V1) strip markup flag (V2) and accounting flag (V3). The markup type (V1) must be one of the following: • MARKUP_TYPE_PREFIX • MARKUP_TYPE_SUFFIX The markup strip flag should be TRUE if the markup is to be removed from the username before forwarding. The accounting flag (V3) should be one of the following: • ACCT_FLAG_LOCAL • ACCT_FLAG_REMOTE • ACCT_FLAG_BOTH
241	ADD_PROXY_TARGET	VN, V1	Adds to named proxy markup (VN) the host name (V1). The host should already be configured in ACS. **Note** The order in which proxy targets are added sets the proxy search order; the first target added is the first target proxied to, and so on. The order must be changed through the web interface.
242	DEL_PROXY	VN	Deletes the named proxy markup (VN).
250	ADD_NDG	VN	Creates a network device group (NDG) named (VN).

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
251	DEL_NDG	VN	Deletes the named NDG.
252	ADD_HOST_TO_NDG	VN, V1	Adds to the named AAA client/AAA server (VN) the NDG (V1).
270	SET_DCS_ASSIGNMENT	—	—
271	ADD_NDG_TO_DCS_MAPPING	—	—
300	RESTART_PROTO_MODULES	—	Restarts the CSRadius and CSTacacs services to apply new settings.
350	ADD_UDV	VN, V1, V2	Adds a RADIUS vendor to the ACS vendor database. Vendors added to ACS by this method are know as User-Defined Vendors (UDV). VN contains the name of the Vendor. **Note** ACS adds *RADIUS(...)* to the name entered in the Variable Name field. For example, if you enter the name *MyCo*, ACS displays *RADIUS (MyCo)* in the web interface. V1 contains the user-defined vendor slot number or AUTO_ASSIGN_SLOT. ACS has ten vendor slots, numbered 0 through 9. If you specify AUTO_ASSIGN_SLOT, ACS selects the next available slot for your vendor. **Note** If you want to replicate UDVs between ACSs, you must assign the UDV to the same slot number on both ACSs. V2 contains the IANA-assigned enterprise code for the vendor.
351	DEL_UDV	V1	Removes the vendor with the IETF code specified in V1 and any defined VSAs. **Note** Action code 351 does not remove any instances of VSAs assigned to ACS groups or users. If ACS has AAA clients configured with the UDV specified in V1, the delete operation fails.

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
352	ADD_VSA	VN, V1, V2, V3	Adds a new VSA to the vendor specified by the vendor IETF code in V1. VN is the VSA name. If the vendor name is *MyCo* and the attribute is assigned a group ID, we recommend prefixing the vendor name or an abbreviation to all VSAs. For example, VSAs could be *MyCo-Assigned-Group-Id*. **Note** VSA names must be unique to the vendor and to the ACS dictionary. For example, *MyCo-Framed-IP-Address* is allowed but *Framed-IP-Address* is not, because *Framed-IP-Address* is used by IETF action code 8 in the RADIUS attributes. V2 is the VSA number. This must be in the 0-255 range. V3 is the VSA type as one of following values: • INTEGER • STRING • IPADDR By default, VSAs are assumed to be outbound (or authorization) attributes. If the VSA is either multi-instance or used in accounting messages, use SET_VSA_PROFILE (Action code 353).

353	SET_VSA_PROFILE	V1, V2, V3	Sets the inbound/outbound profile of the VSA. The profile specifies usage IN for accounting, OUT for authorization, or MULTI if more than a singe instance is allowed per RADIUS message. Combinations are allowed.
			
			V1 contains the vendor IETF code.
			
			V2 contains the VSA number.
			
			V3 contains the profile, one of the following:
			
			`IN`
			`OUT`
			`IN OUT`
			`MULTI OUT`
			`MULTI IN OUT`

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description

354	ADD_VSA_ENUM	VN, V1, V2, V3	Sets meaningful enumerated values, if the VSA attribute has enumerated. In the User Setup section, the ACS web interface displays the enumeration strings in a list.
			VN contains the VSA Enum Name.
			V1 contains the vendor IETF code.
			V2 contains the VSA number.
			V3 contains the VSA Enum Value.
			Example:
			`VN = Disabled`
			`V1 = 9034`
			`V2 = MyCo-Encryption`
			`V3 = 0`
			or
			`VN = Enabled`
			`V1 = 9034`
			`V2 = MyCo-Encryption`
			`V3 = 1`

355	ADOPT_NEW_UDV_OR_VSA	—	Restarts the CSAdmin, CSRadius, and CSLog services. These services must be restarted before new UDVs or VSAs can become usable.

ACS Attributes and Action Codes

This section complements the previous section by providing an inverse reference; it provides topics with tables that list ACS attributes, their data types and limits, and the action codes you can use to act upon the ACS attributes.

This section contains the following topics:

- User-Specific Attributes, page F-22
- User-Defined Attributes, page F-24
- Group-Specific Attributes, page F-24

User-Specific Attributes

Table F-7 lists the attributes that define an ACS user, including their data types, limits, and default values. It also provides the action code you can use in accountActions to affect each attribute. Although there are many actions available, adding a user requires only one transaction: ADD_USER. You can safely leave other user attributes at their default values. The term NULL is not simply an empty string, but means not set; that is, the value will not be processed. Some features are processed only if they have a value assigned to them. For more information about action codes, see Action Codes, page F-3.

Table F-7 User-Specific Attributes

Attribute	Actions	Logical Type	Limits	Default
Username	100, 101	String	1-64 characters	—
ASCII/PAP Password	100, 102	String	4-32 characters	Random string
CHAP Password	103	String	4-32 characters	Random string
Outbound CHAP Password	104	String	4-32 characters	NULL
TACACS+ Enable Password	105	String Password	4-32 characters	NULL
		Integer privilege level	0-15 characters	NULL
Group	106	String	0-100 characters	Default Group
Password Supplier	107	Enum	See Table F-3.	LIBRARY_CSDB
Password Type	108	Enum	See Table F-3.	PASS_TYPE_CSDB (password is cleartext PAP)
Password Expiry Status	109, 110	Bitwise Enum	See Table F-3.	PASS_STATUS_ NEVER (never expires)
Expiry Data	112, 113	Short wrong max/current	0-32,767	—
		Expiry date	—	—
Max Sessions	114	Unsigned short	0-65535	MAX_SESSIONS_AS_GROUP
TODDOW Restrictions	140	String	168 characters	111111111111
NAS Access Control	120, 122	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	
		ACL String (See Table F-4.)	0-31 KB	
Dial-Up Access Control	121, 123	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	NULL
		ACL String (See Table F-4.)	0-31 KB	NULL
Static IP Address	150	Enum scheme	(See Table F-4.)	Client
		String IP/Pool name	0-31 KB	NULL
Callback Number	151	String	0-31 KB	NULL
TACACS Attributes	160, 162	Formatted String	0-31 KB	NULL
RADIUS Attributes	170, 173	Formatted String	0-31 KB	NULL
UDF 1	1, 2	String Real Name	0-31 KB	NULL
UDF 2	1, 2	String Description	0-31 KB	NULL
UDF 3	1, 2	String	0-31 KB	NULL

Table F-7 User-Specific Attributes (continued)

Attribute	Actions	Logical Type	Limits	Default
UDF 4	1, 2	String	0-31 KB	NULL
UDF 5	1, 2	String	0-31 KB	NULL

User-Defined Attributes

User-defined attributes (UDAs) are string values that can contain any data, such as social security number, department name, telephone number, and so on. You can configure ACS to include UDAs on accounting logs about user activity. For more information about configuring UDAs, see User Data Configuration Options, page 3-4.

RDBMS Synchronization can set UDAs by using the SET_VALUE action (code 1) to create a value called USER_DEFINED_FIELD_0 or USER_DEFINED_FIELD_1. For accountActions rows defining a UDA value, the AppId (AI) field must contain APP_ CSAUTH and the Value2(V2) field must contain TYPE_STRING.

Table F-8 lists the data fields that define UDAs. For more information about action codes, see Action Codes, page F-3.

Table F-8 User-Defined Attributes

Action	Username (UN)	ValueName (VN)	Value1 (V1)	Value2 (V2)	AppId (AI)
1	fred	USER_DEFINED_FIELD_0	SS123456789	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_1	Engineering	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_2	949-555-1111	TYPE_STRING	APP_CSAUTH

Note If more than two UDAs are created, only the first two are passed to accounting logs.

Group-Specific Attributes

Table F-9 lists the attributes that define an ACS group, including their data types, limits, and default values. It also provides the action code that you can use in your accountActions table to affect each field. For more information about action codes, see Action Codes, page F-3.

Table F-9 Group-Specific Attributes

Attribute	Actions	Logical Type	Limits	Default
Max Sessions	114	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED
Max Sessions for user of group	115	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED
Token caching for session	130	Bool	T/F	NULL
Token caching for duration	131	Integer time in seconds	0-65535	NULL

Table F-9 Group-Specific Attributes (continued)

Attribute	Actions	Logical Type	Limits	Default
TODDOW Restrictions	140	String	168 characters	111111111111
NAS Access Control	120, 122	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	
		ACL String (See Table F-4.)	0-31 KB	
Dial-Up Access Control	121, 123	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	NULL
		ACL String (See Table F-4.)	0-31 KB	NULL
Static IP Address	150	Enum scheme	(See Table F-4.)	Client
		String IP/Pool name	0-31 KB	NULL
TACACS Attributes	160, 162	Formatted String	0-31 KB	NULL
RADIUS Attributes	170, 173	Formatted String	0-31 KB	NULL
VoIP Support	212	Bool disabled	T/F	NULL

An Example of accountActions

Table F-10 presents an sample instance of accountActions that contains some of the action codes described in Action Codes, page F-3. First user *fred* is created, along with his passwords, including a TACACS_ Enable password with privilege level 10. Fred is assigned to *Group 2*. His account expires after December 31, 1999, or after 10 incorrect authentication attempts. Attributes for Group 2 include Time-of-Day/Day-of-Week restrictions, token caching, and some RADIUS attributes.

Note This example omits several columns that should appear in any accountActions table. The omitted columns are Sequence ID (SI), Priority (P), DateTime (DT), and MessageNo (MN).

Table F-10 Example accountActions Table

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	AppId (AI)
100	fred	—	—	fred	—	—	—
102	fred	—	—	freds_password	—	—	—
103	fred	—	—	freds_chap_password	—	—	—
104	fred	—	—	freds_outbound_password	—	—	—
105	fred	—	—	freds_enable_password	10	—	—
106	fred	Group 2	—	—	—	—	—
150	fred	—	—	123.123.123.123	—	—	—

Table F-10 Example accountActions Table (continued)

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	AppId (AI)
151	fred	—	—	01832-123900	—	—	—
109	fred	—	—	PASS_STATUS_NEVER	—	—	—
110	fred	—	—	PASS_STATUS_WRONG	—	—	—
110	fred	—	—	PASS_STATUS_EXPIRES	—	—	—
112	fred	—	—	10	—	—	—
113	fred	—	—	19991231	—	—	—
114	fred	—	—	50	—	—	—
115	fred	—	—	50	—	—	—
120	fred	—	—	ACCESS_PERMIT	—	—	—
121	fred	—	—	ACCESS_DENY	—	—	—
122	fred	—	—	NAS01,tty0,01732-975374	—	—	—
123	fred	—	—	01732-975374,01622-123123	CLID/ DNIS	—	—
1	fred	—	USER_ DEFINED_ FIELD_0	Fred Jones	TYPE_ STRING	—	APP_ CSAUTH
140	—	Group 2	—	[a string of 168 ones (1)]	—	—	—
130	—	Group 2	—	DISABLE	—	—	—
131	—	Group 2	—	61	—	—	—
163	—	Group 2	Reply-Message	Welcome to Your Internet Service	—	—	—
163	—	Group 2	Vendor-Specific	addr-pool=pool2	9	1	—

Internal Architecture

This chapter describes the architectural components of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS. It includes the following topics:

- Windows Services, page G-1
- Windows and SQL Registries, page G-2
- CSAdmin, page G-3
- CSAuth, page G-3
- CSDBSync, page G-3
- CSLog, page G-4
- CSMon, page G-4
- CSTacacs and CSRadius, page G-6

Windows Services

ACS is modular and flexible to fit the needs of simple and large networks. This appendix describes the ACS architectural components. ACS includes the following service modules:

- **CSAdmin**
- **CSAuth**
- **CSDBSync**
- **CSLog**
- **CSMon**
- **CSTacacs**
- **CSRadius**

You can stop or restart ACS services as a group, except for **CSAdmin**, using the ACS web interface. For more information, see Service Control, page 8-1.

Individual ACS services can be started, stopped, and restarted from the Services window, available within Windows Control Panel.

Windows and SQL Registries

In order to create a unified data storage model, ACS has moved from multiple data storages to a standard SQL-based relational database.

Warning **Do not modify the Registry unless you have enough knowledge and experience to edit the file without destroying or corrupting crucial data.**

Windows Registry

Only general ACS application information (such as the installation directory location) will continue to use the Windows registry.

The ACS information is located in the following Windows Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\CISCO

Unless a Cisco representative advises you to do so, we strongly recommend that you do not modify Windows Registry settings pertaining to ACS.

SQL Registry

The SQL registry contains table information on all user and configuration data. SQL data is not made available for viewing and is protected by an encrypted password.

SQL Tables	Description
ConfigKey	Information that is not stored in the other tables. The data corresponds to registry keys.
ConfigValue	Data corresponding to registry values.
DictKey	Tree of attribute keys. The data is corresponds to registry keys of the ACS dictionary.
DictValue	Values for attributes keys from the ACSDictionaryKeys table.
Host	Information regarding all hosts in ACS.
HostService	Additional data for hosts of type remote agent.
Admin	ACS administrators. The permissions for each administrator are represented as a bitset inside a binary blob.
NetworkModel	Network model section.
Users	All user-specific information that was previously stored in the *user.dat* file. This table structure represents ACS UDB_ACCOUNT structure. However, some fields will not appear.
VarsDB	Currently in use but will be moved to a new table.

CSAdmin

CSAdmin is the service that provides the web server for the ACS web interface. After ACS is installed, you must configure it from its web interface; therefore, **CSAdmin** must be running when you configure ACS.

Because the ACS web server uses port 2002, rather than the standard port 80 that is usually associated with HTTP traffic, you can use another web server on the same machine to provide other web services. We have not performed interoperability testing with other web servers, but unless a second web server is configured to use either port 2002 or one of the ports within the range specified in the HTTP Port Allocation feature, you should not encounter port conflicts for HTTP traffic. For more information about the HTTP Port Allocation feature, see Access Policy, page 12-8.

Although you can start and stop services from within the ACS web interface, this does not include starting or stopping **CSAdmin**. If **CSAdmin** stops abnormally because of an external action, you cannot access ACS from any computer other than the Windows server on which it is running. You can start or stop **CSAdmin** from Windows Control Panel.

CSAdmin is multithreaded, which enables several ACS administrators to access it at the same time. Therefore, **CSAdmin** is well suited for distributed, multiprocessor environments.

CSAuth

CSAuth is the authentication and authorization service. It permits or denies access to users by processing authentication and authorization requests. **CSAuth** determines if access should be granted and defines the privileges for a particular user. **CSAuth** is the ACS database manager.

To authenticate users, ACS can use the internal database or one of many external databases. When a request for authentication arrives, ACS checks the database that is configured for that user. If the user is unknown, ACS checks the database(s) configured for unknown users. For more information about how ACS handles authentication requests for unknown users, see About Unknown User Authentication, page 16-3.

For more information about the various database types supported by ACS, see Chapter 13, “User Databases.”

When a user has authenticated, ACS obtains a set of authorizations from the user profile and the group to which the user is assigned. This information is stored with the username in the ACS internal database. Some of the authorizations included are the services to which the user is entitled, such as IP over PPP, IP pools from which to draw an IP address, access lists, and password-aging information. The authorizations, with the approval of authentication, are then passed to the **CSTacacs** or **CSRadius** modules to be forwarded to the requesting device.

CSDBSync

CSDBSync is the service used to synchronize the ACS database with third-party relational database management system (RDBMS) systems. **CSDBSync** synchronizes AAA client, AAA server, network device groups (NDGs) and Proxy Table information with data from a table in an external relational database. For information on RDBMS Synchronization, see RDBMS Synchronization, page 9-17.

CSLog

CSLog is the service used to capture and place logging information. **CSLog** gathers data from the TACACS+ or RADIUS packet and **CSAuth**, and then manipulates the data to be placed into the comma-separated value (CSV) files. CSV files can be imported into spreadsheets that support this format.

CSMon

CSMon is a service that helps minimize downtime in a remote access network environment. **CSMon** works for TACACS+ and RADIUS and automatically detects which protocols are in use.

You can use the ACS web interface to configure the **CSMon** service. The ACS Active Service Management feature provides options for configuring **CSMon** behavior. For more information, see ACS Active Service Management, page 8-13.

Note **CSMon** is not intended as a replacement for system, network, or application management applications but is provided as an application-specific utility that can be used with other, more generic system management tools.

CSMon performs four basic activities, outlined in the following topics:

- Monitoring, page G-4
- Recording, page G-5
- Notification, page G-5
- Response, page G-5

Monitoring

CSMon monitors the overall status of ACS and the system on which it is running. **CSMon** actively monitors three basic sets of system parameters:

- **Generic host system state—CSMon** monitors the following key system thresholds:
  - Available hard disk space
  - Processor utilization
  - Physical memory utilization

  All events related to generic host system state are categorized as warning events.
- **Application-specific performance**
  - **Application viability—CSMon** periodically performs a test login using a special built-in test account (the default period is one minute). Problems with this authentication can be used to determine if the service has been compromised.
  - **Application performance thresholds—CSMon** monitors and records the latency of each test authentication request (the time it takes to receive a positive response). Each time this is performed, **CSMon** updates a variable containing the average response time value. Additionally, it records whether retries were necessary to achieve a successful response. By tracking the average time for each test authentication, **CSMon** can build up a picture of expected

response time on the system in question. **CSMon** can therefore detect whether excess re-tries are required for each authentication or if response times for a single authentication exceed a percentage threshold over the average.

- **System resource consumption by ACS—CSMon** periodically monitors and records the usage by ACS of a small set of key system resources and compares it against predetermined thresholds for indications of atypical behavior. The parameters monitored include the following:
  - Handle counts
  - Memory utilization
  - Processor utilization
  - Thread used
  - Failed log-on attempts

CSMon cooperates with **CSAuth** to keep track of user accounts being disabled by exceeding their failed attempts count maximum. This feature is more oriented to security and user support than to system viability. If configured, it provides immediate warning of brute-force attacks by alerting the administrator to a large number of accounts becoming disabled. In addition, it helps support technicians anticipate problems with individual users gaining access.

Recording

CSMon records exception events in logs that you can use to diagnose problems.

- **CSMon Log**—Like the other ACS services, **CSMon** maintains a CSV log of its own for diagnostic recording and error logging. Because this logging consumes relatively small amounts of resources, **CSMon** logging cannot be disabled.
- **Windows Event Log—CSMon** can log messages to the Windows Event Log. Logging to the Windows Event Log is enabled by default but can be disabled.

Notification

CSMon can be configured to notify system administrators in the following cases:

- Exception events
- Response
- Outcome of the response

Notification for exception events and outcomes includes the current state of ACS at the time of the message. The default notification method is simple mail-transfer protocol (SMTP) e-mail, but you can create scripts to enable other methods.

Response

CSMon detects exception events that affect the integrity of the service. For information about monitored events, see Monitoring, page G-4. These events are application-specific and hard-coded into ACS. The two types of responses are:

- **Warning events**—Service is maintained but some monitored threshold is breached.
- **Failure events**—One or more ACS components stop providing service.

CSMon responds to the event by logging the event, sending notifications (if configured) and, if the event is a failure, taking action. The two types of actions are:

- **Predefined actions**—These actions are hard-coded into the program and are always carried out when a triggering event is detected. Because these actions are hard-coded, they are integral to the application and do not need to be configured. These actions include running the **CSSupport** utility, which captures most of the parameters dealing with the state of the system at the time of the event.

  If the event is a warning event, it is logged and the administrator is notified. No further action is taken. **CSMon** also attempts to fix the cause of the failure after a sequence of retries and individual service restarts.

- **Customer-Definable Actions**—If the predefined actions built into **CSMon** do not fix the problem, **CSMon** can execute an external program or script.

CSTacacs and CSRadius

The **CSTacacs** and **CSRadius** services communicate between the **CSAuth** module and the access device that is requesting authentication and authorization services. For **CSTacacs** and **CSRadius** to work properly, the system must meet the following conditions:

- **CSTacacs** and **CSRadius** services must be configured from **CSAdmin**.
- **CSTacacs** and **CSRadius** services must communicate with access devices such as access servers, routers, switches, and firewalls.
- The identical shared secret (key) must be configured both in ACS and on the access device.
- The access device IP address must be specified in ACS.
- The type of security protocol being used must be specified in ACS.

CSTacacs is used to communicate with TACACS+ devices and **CSRadius** to communicate with RADIUS devices. Both services can run at the same time. When only one security protocol is used, only the applicable service needs to be running; however, the other service will not interfere with normal operation and does not need to be disabled. For more information about TACACS+ AV pairs, see Appendix B, “TACACS+ Attribute-Value Pairs.” For more information about RADIUS+ AV pairs, see Appendix C, “RADIUS Attributes.”

A

AAA 1
  See also AAA clients
  See also AAA servers
  pools for IP address assignment 7
AAA clients 1
  adding and configuring 11
  configuring 7
  deleting 14
  editing 13
  IP pools 7
  multiple IP addresses for 8
  number of 20
  searching for 6
  table 1
  timeout values 6
AAA protocols
  TACACS+ and RADIUS 3
AAA servers 3
  adding 16
  configuring 15
  deleting 19
  editing 18
  enabling in interface (table) 6
  functions and concepts 2
  in distributed systems 2
  master 2
  overview 15
  primary 2
  replicating 2
  searching for 6
  secondary 2
  troubleshooting 1
accessing Cisco Secure ACS
  how to 3
  URL 18
  with SSL enabled 18
access policies
  See administrative access policies
accountActions table 19, 20
account disablement
  Account Disabled check box 3
  manual 38
  resetting 39
  setting options for 13
accounting
  See also logging
  administrative 15
  overview 14
  RADIUS 15
  TACACS+ 15
ACLs
  See downloadable IP ACLs
ACS
  additional features 4
  extended replication components 5
  features, functions and concepts 2
  internal database 3
  introduction to 1
  managing and administrating 15
  scalability improvements 5
  specifications 19
  Windows Services 20
ACS internal database
  See also databases

overview 1
password encryption 2
ACS internal database replication
See replication
action codes
for creating and modifying user accounts 4
for initializing and modifying access filters 9
for modifying network configuration 17
for modifying TACACS+ and RADIUS settings 12
for setting and deleting values 4
in accountActions 3
Active Service Management
See Cisco Secure ACS Active Service Management
adding
external servers 24
ADF
importing for vendors 5
Administration Audit log
configuring 9
CSV file directory 11
viewing 12
Administration Control
See also administrators
audit policy setup 12
administrative access policies
See also administrators
configuring 9
limits 8
options 8
overview 8
administrative accounting 15
administrative sessions
and HTTP proxy 2
network environment limitations of 1
session policies 11
through firewalls 2
through NAT (network address translation) 2
administrators
See also Administration Audit log
See also Administration Control
See also administrative access policies
adding 4
deleting 7
editing 5
locked out 7
locking out 11
overview 1
privileges 2
separation from general users 9
troubleshooting 2
unlocking 7
advanced options in interface 7
AES 128 algorithm 2
age-by-date rules for groups 18
Aironet
AAA client configuration 9
RADIUS parameters for group 30
RADIUS parameters for user 28
ARAP 9
in User Setup 4
attribute definition file
see also ADF 5
attributes
enabling in interface 4
group-specific (table) 24
logging of user data 2
per-group 4
per-user 4
user-specific (table) 24
attribute-value pairs
See AV (attribute value) pairs
audit policies
See also Administration Audit log
overview 12
audit server
functionality 40
audit servers
setting up 25

authentication 6
configuration 19
configuring policies 27
considerations 6
denying unknown users 9
functionality 12
options 19
overview 6
protocol-database compatibility 7
request handling 3
user databases 7
via external user databases 4
Windows 8
authorization 12
configuring policies 43
ordering rules 46
rules 43
setsSee command authorization sets
AV (attribute value) pairs
See also RADIUS VSAs (vendor specific attributes)
RADIUS
Cisco IOS 3
IETF 11
TACACS+
accounting 3
general 1
Available Credentials 38

B

Backup and Restore log directory
See Cisco Secure ACS Backup and Restore log
backups
components backed up 8
directory management 8
disabling scheduled 10
filenames 11
locations 8
manual 9
options 9
overview 7
reports 8
scheduled vs. manual 7
scheduling 9
vs. replication 6
with CSUtil.exe 3
browsers
troubleshooting 3

C

cached users
See discovered users
CA configuration 27
callback options
in Group Setup 5
in User Setup 6
cascading replication 4, 9
cautions
significance of 27
certificate authority, trusted root 13
certificate trust list
see CTL
certification
See also EAP-TLS
See also PEAP
adding certificate authority certificates 27
background 1
backups 8
Certificate Revocation Lists 28
certificate signing request generation 31
editing the certificate trust list 27
replacing certificate 35
self-signed certificates
configuring 34
NAC 5
overview 33
server certificate installation 25

updating certificate 35
Certification Revocation List (CRL) 5
CHAP 9
in User Setup 4
Cisco
Identity-Based Networking Services (IBNS) 2
Cisco IOS
RADIUS
AV (attribute value) pairs 2
group attributes 28
user attributes 26
TACACS+ AV (attribute value) pairs 1
troubleshooting 3
Cisco NAC support 4
Cisco Secure ACS Active Service Management
event logging configuration 15
overview 13
system monitoring
configuring 14
custom actions 14
Cisco Secure ACS Active Service Monitoring logs
file location 11
viewing 12
Cisco Secure ACS administration overview 15
Cisco Secure ACS Backup and Restore log
CSV (comma-separated values) file directory 11
viewing 12
Cisco Secure ACS backups
See backups
Cisco Secure ACS system restore
See restore
CiscoSecure Authentication Agent 16
CLID-based filters 19
cloning
Network Access Profiles 9
policies or rules 21
codes
See action codes
command authorization sets
See also shell command authorization sets
adding 28
configuring 24, 28
deleting 30
editing 29
overview 24
pattern matching 27
PIX command authorization sets 24
command-line database utility
See CSUtil.exe
condition sets, defining 19
configuring
internal policies 18
configuring advanced filtering
Network Access Profiles 7
conventions 26
copying
policies or rules 21
creating
external servers 24
Credential Validation Databases 30
CRLs 28
CSAdmin
Windows Services 20
CSAuth
Windows Services 20
CSDBSync 19
Windows Services 20
CSLog
Windows Services 20
CSMon
See also Cisco Secure ACS Active Service Management
Cisco Secure ACS Service Monitoring logs 23
configuration 4
log 5
windows Services 20
CSNTacctInfo 40, 41, 42
CSNTAuthUserPap 38
CSNTerrorString 40, 41, 42

CSNTExtractUserClearTextPw 39
CSNTFindUser 39
CSNTgroups 40, 41, 42
CSNTpasswords 40, 41
CSNTresults 40, 41, 42
CSNTusernames 40, 41, 42
CSRadius 6
  Windows Services 20
CSTacacs 6
  Windows Services 20
CSUtil.exe
  decoding error numbers with 17
  import text file (example) 15
  overview 1
CSV (comma-separated values) files
  downloading 12
  filename formats 10
  logging format 1
  viewing 12
CTL
  external policy servers
CTL editing 27
custom attributes
  in group-level TACACS+ settings 22
  in user-level TACACS+ settings 16
customer support
  collecting data for 25

D

database group mappings
  configuring
    for token servers 2
    for Windows domains 6
    no access groups 4
    order 8
  deleting
    group set mappings 7
    Windows domain configurations 7
Database Replication log
  CSV (comma-separated values) file directory 11
  viewing 12
databases
  See also external user databases
  ACS internal database 1
  authentication search process 3
  compacting 8
  deleting 54
  deployment considerations 10
  external
    See also external user databases
    See also Unknown User Policy
  replication
    See replication
  search order 7
  search process 7
  selecting user databases 1
  synchronization
    See RDBMS synchronization
  token cards
    See token servers
  troubleshooting 6, 14
  types
    See generic LDAP user databases
    See LEAP proxy RADIUS user databases
    See Novell NDS user databases
    See ODBC features
    See RADIUS user databases
    See RSA user databases
  unknown users 1
  user databases 2
  user import methods 2
  Windows user databases 5
data source names
  configuring for ODBC logging 17
  for RDMBS synchronization 24
  using with ODBC databases 34, 43, 44
data types, NAC attribute 8

date format control 3
DbSync log directory 11
debug logs
  detail levels 24
  frequency 24
default group
  in Group Setup 2
  mapping for Windows 4
default time-of-day/day-of-week specification 6
default time-of-day access settings for groups 5
deleting 10
  external audit servers 27
  external servers 25
  logged-in users 7
  Network Access Profiles 10
  policies or rules 23
deployment
  overview 1
  sequence 11
device command sets
  See command authorization sets
device management applications support 13
DHCP with IP pools 29
dial-in permission to users in Windows 18
dial-in troubleshooting 8
dial-up networking clients 7
dial-up topologies 2
digital certificates
  See certification
Disabled Accounts report
  viewing 8
Disabled Accounts reports
  description 6
discovered users 2
Distinguished Name Caching 26
distributed systems
  See also proxy
  AAA servers in 2
  overview 2
  settings
    configuring 23
    default entry 3
    enabling in interface 6
distribution table
  See Proxy Distribution Table
DNIS-based filters 19
documentation
  conventions 26
  objectives 25
  online 18
  related 28
Domain List
  configuring 21
  inadvertent user lockouts 9, 21
  overview 9
  unknown user authentication 5
domain names
  Windows operating systems 9
downloadable IP ACLs 5
  adding 15
  assigning to groups 22
  assigning to users 14
  deleting 17
  editing 16
  enabling in interface
    group-level 6
    user-level 5
  overview 13
draft-ietf-radius-tunnel-auth 3
dump files
  loading a database from a dump file 7
dynamic usage quotas 13
dynamic users
  removing 40

E

EAP (Extensible Authentication Protocol)

Configuration 29
overview 9
supported protocols 9
with Windows authentication 10
EAP authentication
protocol 8
EAP-FAST 9
enabling 17
identity protection 10
logging 9
master keys
definition 10
states 10
master server 16
overview 8
PAC
automatic provisioning 13
definition 11
manual provisioning 14
refresh 15
states 13
password aging 20
phases 9
replication 15
EAP-Flexible Authentication via Secure Tunneling (FAST) 5
EAP-TLS 9
See also certification
authentication configuration 19
comparison methods 3
domain stripping 10
enabling 4
limitations 4
options 21, 24
overview 2
editing
external audit servers 26
external posture validation servers 25
internal policies 20
Network Access Profiles 9
enable password options for TACACS+ 23
enable privilege options for groups 13
entity field 8
error number decoding with CSUtil.exe 17
Event log
configuring 15
exception events 5
exception events 5
exemption list
external audit 15
exports
of user lists 15
Extensible Authentication Protocol
See EAP (Extensible Authentication Protocol)
Extensible Authentication Protocol (EAP) 2
external audit policy
what triggers an 15
external audit server
setting up 25
external audit servers
about 14
deleting 27
editing 26
external policies 11
exemption list support 15
external servers
creating 24
deleting 25
editing 25
external token servers
See token servers
external user databases
See also databases
authentication via 4
configuring 3
deleting configuration 54
latency factors 6
search order 6, 8

supported 7
Unknown User Policy 1

F

Failed Attempts log
configuring
CSV (comma-separated values) 14
ODBC 17
CSV (comma-separated values) file directory 11
enabling
log 11
ODBC 17
viewing 12
failed log-on attempts 5
failure events
customer-defined actions 5
predefined actions 5
fallbacks on failed connection 4
finding users 37

G

gateways 2
Generic LDAP 7
generic LDAP user databases
authentication 22
configuring
database 30
options 26
directed authentications 24
domain filtering 24
failover 25
mapping database groups to AAA groups 3
mutiple instances 23
organizational units and groups 23
Global Authentication Setup 19
global authentication setup
enabling posture validation 5
grant dial-in permission to users 6, 18
greeting after login 18
group-level interface enabling
downloadable IP ACLs 6
network access restrictions 6
network access restriction sets 6
password aging 6
group-level network access restrictions
See network access restrictions
groups
See also network device groups
assigning users to 5
configuring RADIUS settings for
See RADIUS
Default Group 2, 4
enabling VoIP (Voice-over-IP) support for 4
exporting group information 16
listing all users in 40
mapping order 8
mappings 1
no access groups 4
overriding settings 4
relationship to users 4
renaming 40
resetting usage quota counters for 40
settings for
callback options 5
configuration-specific 12
configuring common 3
device management command authorization sets 26
enable privilege 13
IP address assignment method 21
management tasks 39
max sessions 9
network access restrictions 6
password aging rules 15
PIX command authorization sets 25
shell command authorization sets 24

TACACS+ 2, 3, 22
time-of-day access 5
token cards 14
usage quotas 10
setting up and managing 1
specifications by ODBC authentications 40, 41, 42

H

handle counts 5
hard disk space 4
host system state 4
HTML interface
encrypting 9
logging off 3
HTTP port allocation
configuring 9
for administrative sessions 16
HTTPS 9

I

IEEE 802.1x 2
IETF 802.1x 9
IETF RADIUS attributes 4
importing passwords 9
imports with CSUtil.exe 9
inbound
authentication 10
password configuration 10
installation
related documentation 28
troubleshooting 11
Interface Configuration
See also HTML interface
advanced options 5
configuring 1
customized user data fields 4
security protocol options 9
internal architecture 1
internal policies
configuration options 10
editing 20
rules 10
steps to set up 18
IP ACLs
See downloadable IP ACLs
IP addresses
in User Setup 7
multiple IP addresses for AAA client 8
requirement for CSTacacs and CSRadius 6
setting assignment method for user groups 21
IP pools
address recovery 33
deleting 32
DHCP 29
editing IP pool definitions 31
enabling in interface 6
overlapping 29, 30
refreshing 30
resetting 32
servers
adding IP pools 30
overview 28
replicating IP pools 29
user IP addresses 7

L

LAN manager 9
latency in networks 10
LDAP
Admin Logon Connection Management 26
Distinguished Name 26
LEAP 9
LEAP proxy RADIUS user databases
configuring external databases 47

group mappings 1
overview 46
RADIUS-based group specifications 8
list all users
in Group Setup 40
in User Setup 37
local policies
see internal policies
log files
storage directory 3
Logged-In Users report
deleting logged-in users 7
description 6
viewing 7
logging
See also Reports and Activity
accounting logs 4
Administration Audit log 9
administration reports 6
configuring 15
CSV (comma-separated values) files 1
custom RADIUS dictionaries 2
debug logs
detail levels 24
frequency 24
Disabled Accounts reports 6
domain names 2
external user databases 2
Failed Attempts logs 4
formats 1
Logged-In Users reports 6
ODBC logs
enabling in interface 7
overview 1
working with 16
overview 4
Passed Authentication logs 4
RADIUS logs 4
RDBMS synchronization 2
remote logging
centralized 20
configuring 21
disabling 22
enabling in interface 6
logging hosts 19
options 21
overview 19
service logs 12
services
configuring service logs 24
list of logs generated 23
system logs 8
TACACS+ logs 4
troubleshooting 12
user data attributes 2
VoIP logs 4
watchdog packets 3
login process test frequency 13
logins
greeting upon 18
password aging dependency 17
logs
See logging
See Reports and Activity

M

MAC-Authentication Bypass 29
Machine Access Restrictions (MAR) 6
machine authentication
enabling 16
overview 11
with Microsoft Windows 14
management application support 13
mappings
database groups to AAA groups 3
databases to AAA groups 1
master AAA servers 2

master key
definition 10
states 10
max sessions 12
enabling in interface 6
group 12
in Group Setup 9
in User Setup 11
overview 12
troubleshooting 11
user 12
memory utilization 4
monitoring
configuring 14
CSMon 4
overview 13
MS-CHAP 9
configuring 19
overview 9
protocol supported 8
multiple IP addresses for AAA clients 8

N

NAC 2
agentless host see also NAH 14
attributes
about 7
adding 28
data types 8
deleting 28
exporting 28
configuring ACS for support for 4
credentials
about 7
implementing 4
logging 5
overview
policies
about 18
external 11
internal 9
results 18
remediation server
url-redirect attribute 6
rules
about 10, 6
default 11
operators 6
self-signed certificates 5
tokens
definition 3
descriptions of 3
returned by internal policies 9
NAC Agentless Host 25
NAC L2 IP 17
NAC L3 IP 15
NAFs
See network access filters
NAH
policies 14
NAR
See network access restrictions
NAS
See AAA clients
Network Access Filter (NAF)
editing 5
Network Access Filters (NAF) 6, 4
adding 3
deleting 6
overview 2
Network Access Profiles 5, 1, 10, 28
cloning 9
configuring advanced filtering 7
editing 9
setting up 3
network access quotas 13
network access restrictions

deleting 23
editing 22
enabling in interface
group-level 6
user-level 5
in Group Setup 6
interface configuration 6
in User Setup 6, 8
non-IP-based filters 19
overview 18
network access servers
See AAA clients
Network Admission Control
see NAC
network configuration 1
network device groups
adding 20
assigning AAA clients to 21
assigning AAA servers to 21
configuring 19
deleting 22
enabling in interface 6
reassigning AAA clients to 21
reassigning AAA servers to 21
renaming 22
network devices
searches for 6
networks
latency 10
reliability 10
network topologies
deployment 2
wireless 4
noncompliant devices 2
non-EAP authentication
protocol 7
Novell NDS user databases
mapping database groups to AAA groups 3

O

ODBC features
accountActions table 21
authentication
CHAP 37
EAP-TLS 37
overview 34
PAP 37
preparation process 36
process with external user database 35
result codes 43
case-sensitive passwords 38
CHAP authentication sample procedure 39
configuring 44
data source names 17, 34
DSN (data source name) configuration 43
EAP-TLS authentication sample procedure 39
features supported 35
group mappings 1
group specifications
CHAP 41
EAP-TLS 42
PAP 40
vs. group mappings 2
PAP authentication sample procedures 38
password case sensitivity 38
stored procedures
CHAP authentication 41
EAP-TLS authentication 42
implementing 37
PAP authentication 40
type definitions 38
user databases 34
ODBC logs
See logging
One-time Passwords (OTPs) 6
online documentation 18
online help 18

location in HTML interface 17
using 18
online user guide 19
Open Database Connectivity (ODBC) 7
ordering rules, in policies 10
outbound password configuration 10
overview of Cisco Secure ACS 1

P

PAC
automatic provisioning 13
definition 11
manual provisioning 14
refresh 15
package.cab file 25
PAP 9
in User Setup 4
vs. ARAP 9
vs. CHAP 9
Passed Authentications log
configuring CSV (comma-separated values) 14
CSV (comma-separated values) file directory 11
enabling CSV (comma-separated values) logging 11
viewing 12
password
automatic change password configuration 16
password aging 11
age-by-uses rules 17
Cisco IOS release requirement for 16
EAP-FAST 17
interface configuration 6
in Windows databases 19
MS-CHAP 17
overview 11
PEAP 17
rules 15
password configurations
basic 10
passwords
See also password aging
case sensitive 38
CHAP/MS-CHAP/ARAP 5
configurations
caching 10
inbound passwords 10
outbound passwords 10
separate passwords 10
single password 10
token caching 10
token cards 10
encryption 2
expiration 17
import utility 9
local management 4
password change log management 5
post-login greeting 18
protocols supported 8
remote change 5
user-changeable 11
validation options in System Configuration 4
pattern matching in command authorization 27
PEAP 9
See also certification
configuring 19
enabling 7
identity protection 6
options 20
overview 5
password aging 19
phases 6
with Unknown User Policy 7
performance monitoring 4
performance specifications 19
per-group attributes
See also groups
enabling in interface 4
per-user attributes

enabling in interface 4
TACACS+/RADIUS in Interface Configuration 5
PIX ACLs
See downloadable IP ACLs
PIX command authorization sets
See command authorization sets
PKI (public key infastructure)
See certification
Point-to-Point Protocol (PPP) 20
policies
cloning 21
configuring 17
copying 21
deleting 23
external 11
configuration options 12
internal 9
local
see internal policies
NAH 14
overview 7
renaming 22
rule order 10
setting up an external audit server 25
setting up external servers 24
Populate from Global 28
Network Access Profiles 28
port 2002
in HTTP port ranges 9
in URLs 18
port allocation
See HTTP port allocation
ports
See also HTTP port allocation
See also port 2002
RADIUS 3
TACACS+ 3
Posture Validation
for Agentless Hosts 41
posture validation
attributes 7
configuring ACS for 4
credentials 7
CTL 5
enabling 5
failed attempts log 5
implementing 4
internal policy configuration options 10
options 17
passed authentications log 5
policy overview 7
process flow 6
and profile-based policies 27
profiles, adding user groups 5
rule
assigning posture tokens 6
rules, about 10
server certificate requirement 4
Posture Validation Policies
configuring 35
PPP password aging 16
privileges
See administrators
processor utilization 4
profile 1
Profile-based Policies 2
profile components
See shared profile components
profiles 47
profile templates 13
protocols supported 8
protocol support
EAP authentication 8
non-EAP authentication
7
protocol types
Network Access Profiles 5
proxy

See also Proxy Distribution Table
character strings
defining 4
stripping 4
configuring 23
in enterprise settings 5
overview 3
sending accounting packets 5
troubleshooting 11
Proxy Distribution Table
See also proxy
adding entries 24
configuring 23
default entry 3, 24
deleting entries 26
editing entries 25
match order sorting 25
overview 23

Q

quotas
See network access quotas
See usage quotas

R

RAC and Groups 47
RADIUS 3
See also RADIUS VSAs (vendor specific attributes)
accounting 15
attributes
See also RADIUS VSAs (vendor specific attributes)
in User Setup 24
AV (attribute value) pairs
See also RADIUS VSAs (vendor specific attributes)
Cisco IOS 3
IETF 11
overview 1
Cisco Aironet 9
compliant token servers 7
IETF
in Group Setup 27
interface configuration 12
in User Setup 25
interface configuration overview 9
password aging 19
ports 3
specifications 3
token servers 49
troubleshooting 15
tunneling packets 12
vs. TACACS+ 3
RADIUS Accounting log
configuring
CSV (comma-separated values) 14
ODBC 17
configuring CSV (comma-separated values) 12
CSV (comma-separated values) file directory 11
enabling
ODBC 17
enabling CSV (comma-separated values) 11
RADIUS user databases
configuring 50
group mappings 1
RADIUS-based group specifications 8
RADIUS VSAs (vendor specific attributes)
Ascend
in Group Setup 32
in User Setup 29
supported attributes 21
Cisco Aironet
in Group Setup 30
in User Setup 28
Cisco BBSM (Building Broadband Service Manager)
in Group Setup 38
in User Setup 35

supported attributes 10
Cisco IOS/PIX
in Group Setup 28
interface configuration 13
in User Setup 26
supported attributes 4
Cisco VPN 3000
in Group Setup 33
in User Setup 30
supported attributes 6
Cisco VPN 5000
in Group Setup 34
in User Setup 31
supported attributes 10
custom
about 19
in Group Setup 39
in User Setup 35
Juniper
in Group Setup 37
in User Setup 34
supported attributes 28
Microsoft
in Group Setup 35
in User Setup 32
supported attributes 19
Nortel
in Group Setup 36
in User Setup 33
supported attributes 28
overview 1
user-defined
about 19, 18
action codes for 12
adding 18
deleting 19
import files 21
listing 20
replicating 19, 18
RDBMS synchronization
accountActions table as transaction queue 21
configuring 26
data source name configuration 23, 24
disabling 28
enabling in interface 6
group-related configuration 18
import definitions 1
log
CSV (comma-separated values) file directory 11
viewing 12
manual initialization 25
network configuration 19
overview 17
partners 25
preparing to use 22
report and error handling 22
scheduling options 25
user-related configuration 18
Registry 2
Regular Expressions Syntax 14
rejection mode
general 3
Windows user databases 4
related documentation 28
reliability of network 10
remote access policies 7
remote logging
See logging
Remove Dynamic Users 40
removing
external audit servers 27
external servers 25
policies or rules 23
removing dynamic users 40
renaming
policies 22
replication
ACS Service Management page 2

auto change password settings 16
backups recommended (Caution) 7
cascading 4, 9
certificates 2
client configuration 11
components
  overwriting (Caution) 11
  overwriting (Note) 7
  selecting 8
configuring 14
corrupted backups (Caution) 7
custom RADIUS dictionaries 2
disabling 15, 16
EAP-FAST 15
encryption 4
external user databases 2
frequency 5
group mappings 2
immediate 12
implementing primary and secondary setups 10
important considerations 5
in System Configuration 14
interface configuration 6
IP pools 2, 29
logging 7
manual initiation 12
master AAA servers 2
notifications 16
options 7
overview 2
partners
  configuring 15
  options 9
process 3
scheduling 14
scheduling options 9
selecting data 8
unsupported 2
user-defined RADIUS vendors 6
  vs. backup 6
Reports and Activity
  See also logging
  configuration privileges 4
  configuring 15
  CSV (comma-separated values) logs 8
  in interface 17
  overview 4
request handling
  general 3
  Windows user databases 4
Required Credential Types 38
resource consumption 5
restarting services 2
restore
  components restored
    configuring 12
    overview 12
  filenames 11
  in System Configuration 11
  on a different server 11
  overview 11
  performing 12
  reports 12
  with CSUtil.exe 4
RFC2138 3
RFC2139 3
RSA SecurID Token Server 7
RSA user databases
  configuring 53
  group mappings 1
rules
  about 10
  internal policy 10

S

search order of external user databases 8
security policies 8

security protocols
CSRadius 6
CSTacacs 6
interface options 9
RADIUS 3, 1
TACACS+
custom commands 8
overview 3
time-of-day access 8
Selected Credentials 38
server certificate installation 25
service control in System Configuration 24
Service Monitoring logs
See Cisco Secure ACS Service Monitoring logs
services
determining status of 2
logs
configuring 24
list of logs generated 23
management 13
starting 2
stopping 2
session policies
configuring 11
options 11
overview 11
setting up
Network Access Profiles 3
shared profile components
See also command authorization sets
See also downloadable IP ACLs
See also network access filters
See also network access restrictions
overview 1
Shared Profile Components (SPC) 13
Shared RAC 46
shared secret 6
shell command authorization sets
See also command authorization sets
in Group Setup 24
in User Setup 17
Simple Network Management Protocol (SNMP) 12
single password configurations 10
SMTP (simple mail-transfer protocol) 5
specifications
RADIUS
RFC2138 3
RFC2139 3
system performance 19
TACACS+ 3
SSL (secure socket layer) 9
starting services 2
static IP addresses 7
stopping services 2
stored procedures
CHAP authentication
configuring 45
input values 41
output values 41
result codes 43
EAP-TLS authentication
configuring 46
input values 42
output values 42
implementing 37
PAP authentication
configuring 45
input values 40
output values 40
result codes 43
sample procedures 38
type definitions
integer 38
string 38
supplementary user information
in User Setup 4
setting 4
support

Cisco Device-Management Applications 13
supported password protocols 8
synchronization
See RDBMS synchronization
system
configuration
advanced 1
authentication 1
basic 1
certificates 1
privileges 3
health 4
messages in interface 17
monitoring
See monitoring
performance specifications 19
services
See services
system performance
specifications 19

T

TACACS+ 3
accounting 15
advanced TACACS+ settings
in Group Setup 2, 3
in User Setup 22
AV (attribute value) pairs
accounting 3
general 1
custom commands 8
enable password options for users 23
enable privilege options 22
interface configuration 7
interface options 9
outbound passwords for users 24
ports 3
SENDAUTH 10
settings
in Group Setup 2, 3, 22
in User Setup 15, 16
specifications 3
time-of-day access 8
troubleshooting 15
vs. RADIUS 3
TACACS+ Accounting log
configuring
CSV (comma-separated values) 14
ODBC 17
CSV (comma-separated values) file directory 11
enabling CSV (comma-separated values) 11
enabling for ODBC 17
viewing 12
TACACS+ Administration log
configuring
CSV(comma-separated values) 14
ODBC 17
CSV (comma-separated values) file directory 11
enabling
ODBC 17
enabling CSV (comma-separated values) 11
viewing 12
Telnet
See also command authorization sets
password aging 16
test login frequency internally 13
thread used 5
time-of-day/day-of-week specification
See also date format control
enabling in interface 6
timeout values on AAA clients 6
TLS (transport level security)
See certification
token caching 10, 49
token cards 20
password configuration 10
settings in Group Setup 14

token servers
ISDN terminal adapters 49
overview 49
RADIUS-enabled 49
RADIUS token servers 50
RSA 53
supported servers 7
token caching 49
topologies
See network topologies
troubleshooting 47
AAA servers 1
administration issues 2
browser issues 3
Cisco IOS issues 3
database issues 6
debug logs 23
dial-in issues 8
installation issues 11
max sessions issues 11
proxy issues 11
RADIUS issues 15
report issues 12
TACACS+ issues 15
third-party server issues 14
upgrade issues 11
user issues 14
trusted root certificate authority 13
trust lists
See certification
trust relationships 7

U

UNIX passwords 12
unknown service user setting 21
Unknown User Policy 18
See also unknown users
configuring 8
in external user databases 2, 7
turning off 9
unknown users
See also Unknown User Policy
authentication 3
authentication performance 6
authentication processing 6
network access authorization 6
unmatched user requests 10
update packets
See watchdog packets
upgrade troubleshooting 11
usage quotas
in Group Setup 10
in Interface Configuration 6
in User Setup 12
overview 13
resetting
for groups 40
for single users 39
user-changeable passwords
overview 11
with Windows user databases 17
user databases
See databases
User Data Configuration 4
user groups
See groups
user guide
online 19
user-level
downloadable ACLs interface 5
network access restrictions
See also network access restrictions
enabling in interface 5
User Password Changes log location 11
users
See also User Setup
adding

basic steps 3
methods 2
assigning client IP addresses to 7
assigning to a group 5
callback options 6
configuring 1
configuring device management command authorization sets for 20
configuring PIX command authorization sets for 19
configuring shell command authorization sets for 17
customized data fields 4
data configuration
See User Data Configuration
deleting 7
deleting accounts 38
disabling accounts 3
finding 37
import methods 2
in multiple databases 4
listing all users 37
number allowed 10
number of 20
RDBMS synchronization 18
relationship to groups 4
removing dynamic 40
resetting accounts 39
saving settings 41
supplementary information 4
troubleshooting 14
types
discovered 2
known 2
unknown 2
VPDN dialup 1
User Setup
account management tasks 36
basic options 2
configuring 1
deleting user accounts 38
saving settings 41
Users in Group button 40

V

validation of passwords 4
vendors
adding audit 25
vendor-specific attributes
See RADIUS VSAs (vendor specific attributes)
vendor-specific attributes (VSAs) 4
viewing logs and reports
See logging
Virtual Private Dial-Up Networks (VPDNs) 12
Voice-over-IP
See VoIP (Voice-over-IP)
VoIP (Voice-over-IP)
accounting configuration 7, 15
Accounting log
enabling csv log 11
viewing 12
enabling in interface 6
group settings in Interface Configuration 6
in Group Setup 4
VoIP (Voice-over-IP) Accounting log
configuring
CSV (comma-separated values) 14
ODBC 17
CSV (comma-separated values) file directory 11
enabling
ODBC 17
VPDN
advantages 6
authentication process 1
domain authorization 2
home gateways 2
IP addresses 2
tunnel IDs 2
users 1

VSAs
See RADIUS VSAs (vendor specific attributes)

W

warning events 4, 5
warnings
significance of 27
watchdog packets
configuring on AAA clients 12
configuring on AAA servers 17
logging 3
web interface
See also Interface Configuration
layout 16
security 15
uniform resource locator 18
Windows Callback 18
Windows Database Callback 18
Windows operating systems
authentication order 5
Cisco Secure ACS-related services
services 2
dial-up networking 7
dial-up networking clients
domain field 7
password field 7
username field 7
Domain List effect 5
domains
domain names 9, 4
Event logs 5
Registry 2
Windows Services 20
CSAdmin 20
CSAuth 20
CSDBSync 20
CSLog 20
CSMon 20
CSRadius 20
CSTacacs 20
overview 20
Windows user database 7
passwords 8
Windows user databases
See also databases
Active Directory 18
configuring 21
Domain list
inadvertent user lockouts 21
domain mapping 6
domains
trusted 7
grant dial-in permission to users 6, 18
group mappings
editing 6
limitations 3
no access groups 4
remapping 6
mapping database groups to AAA groups 3
overview 5
password aging 19
rejection mode 4
request handling 4
trust relationships 7
user-changeable passwords 17
user manager 18
wireless network topologies 4