



Cisco Secure Access Control Server Troubleshooting Guide

May 2008

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.

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

Text Part Number: OL-12555-02

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

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

Cisco Secure Access Control Server Troubleshooting Guide
© 2008 Cisco Systems, Inc. All rights reserved.

Preface	ix
Audience	ix
Organization	ix
Conventions	ix
Product Documentation	x
Related Documentation	x
Obtaining Documentation	xi
Cisco.com	xi
Product Documentation DVD	xi
Ordering Documentation	xi
Documentation Feedback	xi
Cisco Product Security Overview	xi
Reporting Security Problems in Cisco Products	xii
Product Alerts and Field Notices	xiii
Obtaining Technical Assistance	xiii
Cisco Technical Support & Documentation Website	xiii
Submitting a Service Request	xiv
Definitions of Service Request Severity	xiv
Obtaining Additional Publications and Information	xv
Troubleshooting Procedures and Tools	1
How to Troubleshoot ACS	1
Checking Installation Integrity	1
Did the Installation Encounter Problems?	1
Are the Services Running?	2
What is the Status of the Services?	2
Checking Authentication	2
Are Requests and Authentications Succeeding?	2
Is the Problem on a Device?	3
Is the Problem on ACS?	3
Additional Testing for User Authentication	4
Resources for Additional Information	5
Using Online Help	5
Accessing and Using Cisco.com	5
Preparing Diagnostic Information for the TAC	6
Before Creating package.cab Files	6
Conditions on Your Network	6
Setting Logging Levels	7
Check the Number of Files	7
ACS Service Status When Creating a File	7
Testing Your Application	7
Creating package.cab Files	7
Creating package.cab Files in ACS for Windows	8
Creating package.cab Files for the ACS Solution Engine	8

Example: Support Dialog from the Remote Console (ACS SE) 8
Locating the package.cab File on the Remote Agent 9
The Contents of a package.cab File 9
Analyzing the Contents of package.cab 10
Examples of package.cab Analysis 10
Locating and Troubleshooting Database Files 12
Sybase Files 13
Modifications to the ACS Database Using CSUpdate 13
LDAP Databases 13
Logging 14
Log File Size 14
ACS for Windows 14
Solution Engine 14
Services that Generate Log Files 14
Services that Log and Monitor ACS 15
Service Log Files on the Remote Agent 16
Examples of Logs 16
Administration Report 16
Administration Diagnostic Log 17
CSAuth Log File 18
EAP Logging 19
Command Line Utilities 19
CSUtil.exe (Windows Only) 20
Lotcaion and Syntax 20
Backing Up and Restoring the ACS Internal Database 20
Creating a Dump Text File 21
Exporting User and Group Information 22
The Remote Agent CLI (Solution Engine Only) 22
CLI Commands 22
Diagnostic Output from the Show Command 23
Using the Web Interface with the Solution Engine 24
Common Problems 1
Administration 1
Administrator Locked Out 2
Unauthorized Users Logging In 2
Restart Services Does Not Work 3
Event Notification E-Mail Not Received 3
Remote Administrator Cannot Access Browser 3
Remote Administrators Cannot Log In 4
Remote Administrator Receives Logon Failed... Message 4
Remote Administrator Cannot Access ACS 4
Authentication and Authorization 5
Windows Authentication Problems 5

Dial-in Not Disabled 6
Settings Not Inherited 6
Retry Interval Too Short 6
AAA Client Times Out 6
Unknown NAS Error 7
Key Mismatch Error 7
Unexpected Authorizations 7
RADIUS Extension DLL Rejected User Error 7
Request Does Not Appear in an External Database 8
TACACS+ Authentication is Failing 8
Browser 8
Cannot Access the Web Interface 9
Pages Do Not Appear Properly 9
Browser crash when trying to open ACS 9
Session Connection Lost 10
Administrator Database Corruption (Netscape) 10
Remote Administrator Cannot Browse 10
Cisco Network Admission Control 10
Posture Problems 11
Cisco IOS Commands Not Denied 11
EAP Request Has Invalid Signature 12
Administrator Locked Out of Client 12
Cannot Enter Enable Mode 12
Nonresponsive Endpoint Limit Reached 13
NAC Posture Problem 13
Authorization Policy 13
Databases 14
RDBMS Synchronization Not Properly Operating 14
Database Replication Not Properly Operating 14
External User Database Not Available 15
Unknown Users Not Authenticated 15
User Problems 15
Cannot Implement the RSA Token Server 16
ACE SDI Server Does Not See Incoming Request 16
External Databases Not Properly Operating (ACS Solution Engine) 17
Group Mapping (ACS Solution Engine) 17
Configuration of Active Directory 18
NTLMv2 Does Not Work 19
Dial-In Connections 19
Cannot Connect to AAA Client (No Report) 20
Cannot Connect to the AAA Client (Windows External Database) 20
Cannot Connect to AAA Client (ACS Internal Database) 21
Cannot Connect to AAA Client (Telnet Connection Authenticated) 22

Cannot Connect to AAA Client (Telnet Connection Not Authenticated) 22
Callback Not Working 22
Authentication Fails When Using PAP 23
EAP Protocols 23
GAME Protocol 23
GAME Configuration Problem 24
GAME Troubleshooting Setup 24
Expected Device-Type is Not Matched 25
Device-type Attribute is Not Returned by the Audit Server 25
Failure Returned by the Audit Server 25
Installations and Upgrades 26
System Requirements 26
rad_mon.dll and tac_mon.dll In Use Condition 26
During Upgrade the ACS Folder is Locked 27
During Uninstall the ACS Folder is Locked 27
After Restart ACS Cannot Start Services 27
Upgrade or Uninstall Cannot Complete 28
Invalid File or Data 28
Accounting Logs Missing 28
Upgrade Command Does Not Work (ACS Solution Engine) 29
On Solaris, **autorun.sh** Does Not Execute (ACS Solution Engine) 29
Interoperability 29
Interoperation Between Builds 29
Proxy Requests Fail 29
Logging 30
Too Many Log Files 30
Logging Messages 31
MAC Authentication Bypass Problems 31
The MAC Address Exists in LDAP but Always Maps to the Default User Group 31
The MAC Exists in the Internal Database but is Mapped to the Wrong User Group 32
Request is Rejected 32
Remote Agent (ACS Solution Engine) 32
RPC Timeouts 32
Reports 32
Blank Reports 33
Unknown User Information Missing 33
Two Entries Logged for One User Session 33
Old Format Dates Persist 33
Logging Halted 34
Logged in Users Report Works Only with Certain Devices 34
User Group Management 34
MaxSessions Not Working Over VPDN 35
MaxSessions Fluctuates 35

MaxSessions Does Not Take Effect 35
TACACS+ and RADIUS Attributes Missing 35
Error Codes 1
1



Preface

Revised: May 18, 2011, OL-12555-02

This guide provides troubleshooting information for the Cisco Secure Access Control Server, Releases 4.1 and 4.2, hereafter referred to as ACS.

Audience

This document is for administrators of ACS.

Organization

This document contains:

- **Chapter 1, “Troubleshooting Procedures and Tools”**—Important tools for troubleshooting.
- **Chapter 2, “Common Problems”**—Troubleshooting information for specific problems.
- **Appendix A, “Error Codes”**—A list of ACS error codes.

Conventions

Conventions in this document include:

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	<i>italic font</i>
Displayed session and system information, paths and file names	<code>screen font</code>
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>

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

You should use this troubleshooting guide with the following documentation:

- **ACS for Windows**—<http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html>
- **ACS Solution Engine**—<http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html>

**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.

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. This section explains the product documentation resources that Cisco offers.

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

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — 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 non-emergencies.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key 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.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <https://www.cisco.com/web/siteassets/account/index.html>

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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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 request.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box

and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 channel product 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 magazine for Cisco networking professionals. 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 studies, certification and training information, and links to scores of in-depth online resources. You can subscribe to *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 where networking professionals 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>

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>

- 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>



CHAPTER 1

Troubleshooting Procedures and Tools

Revised: May 18, 2011, OL-12555-02

This chapter describes troubleshooting procedures and tools for the Cisco Secure Access Control Server, hereafter referred to as ACS.

This chapter contains:

- [How to Troubleshoot ACS, page 1-1](#)
- [Resources for Additional Information, page 1-5](#)
- [Preparing Diagnostic Information for the TAC, page 1-6](#)
- [Logging, page 1-14](#)
- [Command Line Utilities, page 1-19](#)

How to Troubleshoot ACS

Use this section as a general framework for troubleshooting ACS.

This section contains:

- [Checking Installation Integrity, page 1-1](#)
- [Checking Authentication, page 1-2](#)

Checking Installation Integrity

If a problem occurs during the installation, ACS does not properly operate. You can use the information in this section to check the integrity of your installation.

Did the Installation Encounter Problems?

If you encounter problems during installation, check the Installation Guide that accompanies your release. For information on common installation and upgrade problems, see [Installations and Upgrades, page 2-26](#). You should also check the Release Notes that accompany your release. For the most recent version of the Release Notes, refer to Cisco.com.

Are the Services Running?

The ACS services are:

- **CSAdmin**
- **CSAuth**
- **CSDbSync**
- **CSLog**
- **CSMon**
- **CSRADIUS**
- **CSTacacs**

Check that the ACS services are running by using the:

- **Microsoft Control Panel**—Choose **Start > Control Panel > Administrative Tools > Services**, to control individual services.
- **ACS Command Line Utilities**—See [Command Line Utilities, page 1-19](#). To generate service startup errors, start the appropriate services from the command line, and watch for errors.

What is the Status of the Services?

You should regularly monitor service status by using the:

- **Windows Event Viewer (ACS for Windows)**—Monitors service events and other events that are associated with ACS.
- **Status Page (ACS Solution Engine)**—Monitors the resources that the ACS services use.
- **Event Viewer Log (ACS Solution Engine)**—Shows events that are associated with the Solution Engine. The support utility generates a package.cab file that includes the event viewer log. For more information, see [Preparing Diagnostic Information for the TAC, page 1-6](#).

For information on logging and monitoring, see [Services that Log and Monitor ACS, page 1-15](#).

Checking Authentication

You can use the information in this section to check authentications.

Are Requests and Authentications Succeeding?

The Failed Attempts logs under Reports and Activity in the web interface show the reasons for authentication failure. By default, ACS turns on the Failed Attempts logs. You can display the Failed Attempts logs by choosing **Reports and Activity > Failed Attempts**.

If you want to add additional fields to the log:

-
- Step 1** Choose **System Configuration > Logging > Configure** for the Comma Separated Value (CSV) Failed Attempts log.
 - Step 2** On the **Configuration** page, move attributes from the **Attributes** column to the **Logged Attributes** column, and click **Submit**.
-

You use the Passed Authentications logs to troubleshoot authorization or Network Access Restriction (NAR) issues. By default, ACS does not enable the Passed Authentications logs.

To enable these logs:

-
- Step 1** Choose **System Configuration > Logging > Configure** for the CSV Passed Authentication logs.
- Step 2** Check the **Log to CSV Passed Authentication report** check box in the Enable Logging pane.
-

To interpret the logs:

- Check to be certain that authentications are getting through.
- Check to be certain that the user is visible in the Passed Authentications or the Failed Attempts logs.
- Look for Reason Codes (text strings), and see what the string tells you.

**Note**

ACS provides additional reports in the System Configuration pane, such as CSV log files for Database Replication. See [Locating and Troubleshooting Database Files, page 1-12](#) for more information.

For a list of common problems related to authentication and authorization, see [Authentication and Authorization, page 2-5](#).

Is the Problem on a Device?

If requests are succeeding, check devices such as access points, routers, and VPN devices by:

- Running the device in debug mode.
- Logging the debugging information from the device.
- Running a packet analyzer to capture and analyze packets.

Because each device is unique, check the vendor documentation for further information.

Is the Problem on ACS?

If requests are succeeding and devices are properly running:

- Check the online help for information pertaining to the problem. For information on online help, see [Resources for Additional Information, page 1-5](#).
- Generate a package.cab file and open a case with the Cisco Technical Assistance Center (TAC). The package.cab file copies the files that are most useful to the TAC.
- If you not determine whether the problem is on a device or on ACS, see [Additional Testing for User Authentication, page 1-4](#).
- If you not determine the source of the problem, see [Resources for Additional Information, page 1-5](#) and [Preparing Diagnostic Information for the TAC, page 1-6](#).

Additional Testing for User Authentication

The **Radtest** and **Tactest** tools simulate the AAA requests to the ACS server in order to eliminate any possibility of Network Access Server (NAS) configuration issues. These tools are part of the ACS installation files at \<ACS_install_dir>\CiscoSecure ACS v4.x\bin. You use these tests when the communicating device is not producing useful debugging information, or, if you still cannot determine whether the problem is with Cisco Secure ACS Windows problem or a device.



Note

In the **Radtest** and **Tactest** examples, the username is **abcde**.

Testing RADIUS with Radtest.exe

Starting from the command line, enter:

```
>radtest.exe

1...Set Radius IP, secret & timeout
2...authenticate user
3...authenticate from file
4...authenticate with CHAP
5...authenticate with MSCHAP
6...Replay log files
7...Drive authentication and accounting from file
8...Accounting start for user
9...Accounting stop for user
A...Extended Setup
B...Customer Packet Builder
0...Exit
Defaults server:172.18.124.99 secret:secret_value timeout:2000mSec auth:1645 acct:1646
port:999 cli:999
Choice>2
User name><>abcde
User password><>abcde
Cli><999>
NAS port id><999>
State><>
User abcde authenticated
Request from host 172.18.124.99:1645 code=2, id=0, length=44 on port 1645
  [080] Signature value: A6 10 00 96 6F C2 AB 78 B6 9F D9 01 E3 D7 C6
  [008] Framed-IP-Address value: 10.1.1.5
Press Enter to continue.
```

Testing TACACS+ with Tactest.exe

Starting from the command line, enter:

```
>tactest -H 127.0.0.1 -k secret

TACACS>
Commands available:
authen action type service port remote [user]
action <login,sendpass,sendauth>
type <ascii,pap,chap,mschap,arap>
service <login,enable,ppp,arap,pt,rcmd,x25>
author arg1=value1 arg2=value2 ...
acct arg1=value1 arg2=value2 ...
```

```
TACACS> authen login ascii login tty0 abcde
Username: abcde
Password: abcde
Authentication succeeded :
TACACS>
```

Resources for Additional Information

If problems do not occur with the installation, and authentication and replication are working, you can use the resources in this section to find additional information.

This section contains:

- [Using Online Help, page 1-5](#)
- [Accessing and Using Cisco.com, page 1-5](#)

Using Online Help

ACS provides several varieties of online help:

- The Help pane on the right side of the web interface.
- The online help interface. Click **Online Documentation** in the navigation bar to open the ACS Online Help page.
- A PDF version of the *User Guide for Cisco Secure Access Control Server*. Click the **View PDF** button on the ACS Online Help interface to open the User Guide.

Accessing and Using Cisco.com

To get ACS troubleshooting information from Cisco.com, use the URL:
<http://www.cisco.com/techsupport> > [registration or login] > Documentation > Network Management.

-
- Step 1** Under Security and Identity Management, click the link for the ACS product.
- Step 2** Click **Troubleshoot and Alerts**.
-

On a regular basis, use:

- Field Notices to find summaries of recent problems.
- Security Advisories, Responses and Notices for to find important security vulnerabilities.
- The links in the Product Literature section for Marketing information.

For specific problems, click:

- Troubleshooting TechNotes for procedural information from the TAC. The list is alphabetical. Look for links that can solve your problem.

- Troubleshooting Guides for problem solving tools, including the:
 - Bug toolkit
 - Networking Professionals Connection Discussion Forum

**Note**

The **Error Message Decoder** and the **Output Interpreter** do not support ACS.

Preparing Diagnostic Information for the TAC

ACS services store information into logging subdirectories. The ACS State Collector utility collects the log files needed for troubleshooting into a single file package cab. The utility also collects system information and user database information. The ACS State Collector utility is:

- **cssupport.exe** on ACS for Windows.
- Running the **support** command from the ACS Solution Engine CLI.

This section contains information on:

- [Before Creating package.cab Files, page 1-6](#)
- [Creating package.cab Files, page 1-7](#)
- [Locating and Troubleshooting Database Files, page 1-12](#)

Before Creating package.cab Files

The information in this section applies to ACS for Windows and the ACS Solution Engine before you create the package.cab file.

Conditions on Your Network

You must account for conditions on your network that are outside of the scope of ACS. You should be prepared to answer questions, such as:

- What was the username?
- What was the timestamp?
- What were the network conditions?
- Have there been any recent changes on the network?

You may be asked for more detailed information, including:

- The installation log.
- Hardware information, such as memory, CPU, and disk size.
- Operating system status and patch level.
- Firewall configuration.
- Active Directory (AD) configuration.
- External database version.
- Replication instances.

- Certificates (style, size, source of generation).
- The Network Access Control (NAC) environment.
- Authentication methods, supplicants, and clients.



Note Is additional software running on the ACS server? Cisco does not recommend running additional software on the ACS server.

Setting Logging Levels

By default, the logging level in the system configuration is set to Low. When you encounter a problem, you must log all messages by setting the logging level to Full. The Full setting uses ACS to collect all debugging information.



Note The Full logging level can use the log files to get quite large. When you return to normal operation, be certain to reset the logging level.

To enable Full logging on ACS for Windows or the ACS Solution Engine:

-
- Step 1** Choose **System Configuration > Service Control**.
- Step 2** Click **Full** under the Level of Detail in the Service Log File Configuration pane.
- Step 3** Click **Restart** to restart services. Service restart can take some time.
-

Check the Number of Files

Check the number of files that ACS should collect. If the number of files is large, the download time will be longer. See [Log File Size, page 1-14](#) for more information.

ACS Service Status When Creating a File

ACS services stop while the utility collects information. ACS cannot process authentication requests while the services are stopped.

Testing Your Application

Run tests that can expose the problem in your application to the package.cab file.

Creating package.cab Files

Use the information in this section to create package.cab files.

Creating package.cab Files in ACS for Windows

From the command line, run **cssupport.exe** from C:\Program Files\CiscoSecure ACS v4.x\bin\cssupport.exe. The default location for the package.cab file is \<ACS_install_dir>\Utils\Support. See [Examples of Logs, page 1-16](#).

If you cannot solve the problem, open a case with the TAC.

Creating package.cab Files for the ACS Solution Engine

The ACS Solution Engine provides two options that can create the package.cab file:

- **Web interface**—Choose **System Configuration > Support > Run Support Now**. This option downloads the package.cab file to the administrator's PC.
- **CLI**—Run the **support** command.

When you run the **support** command:

1. The **support** command opens a dialog. For an example of the dialog, see [Example: Support Dialog from the Remote Console \(ACS SE\), page 1-8](#).
2. The **support** utility then creates the file on your FTP server. If you are running the remote agent on an external PC, see [Locating the package.cab File on the Remote Agent, page 1-9](#) for more information.
3. Download the file from your FTP server.
4. Use [Examples of Logs, page 1-16](#).
5. If you cannot solve the problem, open a case with the TAC.

Example: Support Dialog from the Remote Console (ACS SE)

[Table 1-1](#) shows the arguments to the **support** command.

Table 1-1 Arguments for the support command

Arguments and Options	Description
-d n	Collect the previous <i>n</i> days of logs.
-u-	Collect user database information.
server	Hostname for the FTP server to which to send the file.
filepath	Location under the FTP root for the server into which to send the package.cab file.
username	Account used to authenticate the FTP session.

To generate a package.cab file of log and system registry information from a remote console:

-
- Step 1** Log in to the ACS SE.
 - Step 2** Enter **support** and the appropriate arguments.
 - Step 3** Press **Enter**.
 - Step 4** To collect user database information, at the Collect User Data? prompt, enter **Y** and then press **Enter**.

- Step 5** At the `Enter FTP Server directory` prompt, enter the pathname to the location on your FTP server to which you want to send the file.
- Step 6** Press **Enter**.
- Step 7** At the `Collect previous days logs?` prompt, enter the number of days for which you want to collect information (from 1 to 9999).
- Step 8** Press **Enter**.
- Step 9** At the `Enter FTP Server Hostname or IP address` prompt, enter your FTP server hostname or IP address.
- Step 10** Press **Enter**.
- Step 11** At the `Enter FTP Server Username` prompt, enter your FTP server user account name.
- Step 12** Press **Enter**.
- The next step stops and restarts all services. Service restart interrupts use of the ACS SE.
- Step 13** At the `Enter FTP Server Password` prompt, enter your FTP server password
- Step 14** Press **Enter**.
- The ACS SE now displays a series of messages detailing the writing and dumping of the files, and the stopping and starting of services. At file-transfer conclusion, the system displays the message:
`Transferring `Package.cab' completed. Press any key to finish.` This message indicates that the ACS SE has packaged and transferred the `package.cab` file as specified and restarts services.
- Step 15** Press **Enter**.
- The system returns to the system prompt.
-

Locating the package.cab File on the Remote Agent

When the remote agent is running on an external computer, the **support** utility forces the remote agent to collect log files into one support file. The filename is `<Pack_<computer name>_date_time>.b` (for example, `Pack_ACS-SUS-A2_10-Sep-2006_15-50-48.b`). To retrieve the `package.cab` file, download the file. From the computer running the remote agent, open the Cisco Secure ACS Agent folder in the remote agent installation directory and download the `package.cab` file to the administrator's PC.

The Contents of a package.cab File

The `package.cab` file contains a large amount of information that can be overwhelming. Use the guidelines in this section for interpreting a `package.cab` file.

The `package.cab` file can include:

- **Service Log Files**—Every service has a corresponding log file. These files contain extensive information about each service. For example, the `Auth.log` file contains all current log information from the **CSAuth** service. ACS creates the log files every day, and the current active log file is the file that does not have a date in its filename. For more information, see [Logging, page 1-14](#).
- **CSV Files**—CSV files contain the information about Audit, Accounting, and Failed and Passed Authentication logs. Most of the CSV files contain statistics. To troubleshoot issues, the Failed and Passed Authentication CSV files are often used in conjunction with the service log files. ACS creates the CSV files every day, and the active CSV file is the file that does not have a date in its filename.

- **Registry File**—ACS.reg contains the registry information for the ACS server. Therefore, this file may be required for troubleshooting. Do not import this file onto another server; instead, open it with a text editor.
- **Additional Files**—The package.cab file also includes a set of text files:
 - Microsoft Windows Info.txt contains server and operating system information.
 - Microsoft Windows Event Viewer files (SecEventDump.txt, AppEventDump.txt, and SysEventDump.txt) that contain an additional event dump from the server. You can use these files to troubleshoot issues on the server.
 - The resource.txt file contains resource usage information for ACS services that are running on the server.

Analyzing the Contents of package.cab

To analyze package.cab:

-
- Step 1** Set the Service Logs to Full detail.
 - Step 2** Check the protocol traffic (**CSRradius** and **CSTacacs**). You can use a packet analyzer or a network sniffer to analyze the traffic.
 - Step 3** For every AAA request failure, look at the Failed Attempts log.
 - Step 4** Search for the username in the Auth.log file; also, check for errors or hangs.
 - Step 5** Correlate the timestamps. For example, you can correlate the timestamps associated with the protocol modules (**CSRradius** and **CSTacacs**) with **CSAuth** timestamps, or for the Solution Engine you can correlate **CSAuth** timestamps with the timestamps in the CSWinAgent log.
 - Step 6** If you need additional detail, analyze TCS.log or RDS.log. **CSTacacs** and **CSRradius** form the communication bridge between the NAS and ACS, and **CSAuth** is the communication bridge between the **CSTacacs** and **CSRradius**, and any internal or external user databases, such as AD and LDAP.
-

Examples of package.cab Analysis

The examples in this section show how to analyze the contents of the package.cab file.

Example: Windows Authentication Fails (First Failure)

In this example:

- Windows user authentication fails.
- The user entered the right name and password.
- The debug output from the NAS does not indicate the reason for the failure.

-
- Step 1** You examine the Failed Attempts active.csv log and see the record of the failed authentication, as [Table 1-2](#) shows:

Table 1-2 Failed Authentication Record

Date	Time	Message-Type	User-Name	Group-Name	Iler-ID	Network Access Profile Name	Authen-Failure-Code
04/22/2007	14:44:58	Authen failed	user1	DefaultGroup	..	(Default)	External DBuser invalid or bad password

This description does not explain the exact reason for the failure; therefore, you continue the analysis.

Step 2 The first ACS service that receives the packet is **CSRADIUS**. You examine RDS.log and discover that the authentication message was delivered to the **CSAuth** service.

Step 3 You examine the Auth.log file, and you find that the **CSAuth** service tried to authenticate the user by the internal ACS database (CSDB), but the authentication attempt failed. Then the **CSAuth** service tried to authenticate the user by Microsoft Active Directory, but the Active Directory authentication failed with error 1331L.

For example, AUTH 04/22/2007 14:44:58 I 0396 2892 External DB [NTAuthenDLL.dll]: Attempting Windows authentication for user user1 AUTH 04/22/2007 14:44:58 E 0396 2892 External DB [NTAuthenDLL.dll]: Windows authentication FAILED (error 1331L).

Step 4 You search Microsoft support for error 1331L, and you find: 1331L ERROR_ACCOUNT_DISABLED. The referenced account is currently disabled and cannot be accessed.

Now you know that the user account was disabled in Active Directory due to an administrative policy rule; therefore, you forward the exact problem description to the system administrator.

Example: Windows Authentications Failed (After Previous Successes)

In this example:

- Windows user authentications that were successful in the past are now failing.
- The debug output from the NAS does not indicate the reason for the failure.
- Successive accounting requests fail due to a timeout condition.

You conclude that the AAA server does not acknowledge accounting requests, so:

Step 1 You examine the Failed Attempts active.csv log, but the log does not contain a record that indicates failed authentication.

Step 2 You examine the Passed Authentications active.csv log, and you find that the authentication was successful.

Step 3 **CSRADIUS** is the first ACS service that receives the packet. You examine RDS.log and discover that the authentication message was delivered to the **CSAuth** service. A successful indication was returned to the NAS RDS: 04/22/2007 14:05:23 D 4264 5256 Sending response code 2, id 5 to 64.103.112.190 on port 3467. In addition, an accounting message was delivered to the **CSAuth** service, but the accounting message was not approved, and a response was not sent to NAS: RDS 04/22/2007 14:05:41 E 0896 5100 Error processing accounting request - no response sent to NAS.

- Step 4** You examine the Auth.log file and discover that processing of the authentication request was successful, but processing of the accounting request failed. After investigation, you find that the **CSAuth** service was trying to use the **CSLog** service to log an accounting message about the new authentication, but the **CSLog** service returned the message: AUTH 04/22/2007 14:05:56 E 0351 2892 Failed to log accounting packet to logger local CSLog.
- Step 5** You examine CSLog.log and you find that the **CSLog** service cannot send the accounting message to a remote logger that is configured as critical logger: CSLog 04/22/2007 14:06:27 E 0351 21696 Failed to log accounting packet to logger ACS-log1.
Then you recall that you recently added rules to your firewall.
- Step 6** You examine your firewall log, and you find that it blocked packets sent from ACS servers on port 2001. These messages are necessary for communicating between the ACS server and the critical accounting remote logger. Therefore, you decide to change the firewall rule to allow transfer of accounting packets between ACS servers.
- Step 7** Check the authentication and accounting processes again.
-

Example: A Regular TELNET Login Authentication by the ACS Server is Failing.

In this example:

- The communication protocol configured between the NAS and ACS is TACACS+.
 - NAS debug does not indicate the reason for the failure.
 - The first ACS service that receives the packet is **CSTacacs**.
-

- Step 1** Look at the Failed Attempts active.csv file to see why the user is failing. The information in this file can often provide the reason for failure. However, for this example, the Failed Attempts active.csv file does not provide the information: 04/22/2007,15:47:25,Authen failed,user1,Default Group,64.103.112.222,(Default),Users Access Filtered, ?.
- Step 2** Search for the username in the Auth.log file. In this case, you receive no results from the search for the username. Therefore, the problem may be that the **CSTacacs** service cannot process and forward the authentication request to the **CSAuth** service. Because you see the authentication failure in the Failed Attempts active.log, the authentication request must be reaching ACS.
- Step 3** Analyze the TCS.log file, which contains all the activities that **CSTacacs** performs. As expected, you see the user request coming from the NAS. However, the user request is not being forwarded to the **CSAuth** service: TCS 04/22/2007 16:03:14 I 0043 10268 type=AUTHEN status=2 (AUTHEN/FAIL) flags=0x0.

After a little investigation, you find that a NAR is configured for this user and, therefore, the **CSTacacs** service is dropping packets. You conclude that you do not see the user in the Auth.log file because the packets are not being forwarded to the **CSAuth** service.

Locating and Troubleshooting Database Files

This section provides information on locating and troubleshooting database files.

Sybase Files

ACS 4.x uses Sybase as its database system. When you must send the database files to the TAC, the database files are:

- **Database**—<ACS_install_dir>\CSDB\ACS.db.
- **Uncommitted transactions**—ACS.log.

**Note**

When you configure antivirus (AV) software and Sybase with ACS, do not include the database file for monitoring by the AV software.

Modifications to the ACS Database Using CSUpdate

ACS used the Microsoft Jet database and the Windows registry prior to ACS release 4.0. ACS 4.0 and later releases use Sybase. ACS protects the Sybase database with a locked password, encryption, and restriction of access to the web interface and **CSUtil.exe**. In some cases, you may require special configuration, such as changing attributes in the ACS internal RADIUS dictionary, or changing RADIUS ports. If you cannot fulfill the configuration by using the web interface or **CSUtil.exe**, the TAC engineers can supply a special db-patch file that can modify the database.

Applying db-patch (ACS for Windows)

To apply db-patch on ACS for Windows:

-
- Step 1** Copy the patch to <ACS_install_dir>\bin.
 - Step 2** Stop ACS services.
 - Step 3** Bring up a Command prompt.
 - Step 4** Change directory to <ACS_install_dir>\bin.
 - Step 5** Run `CSUpdate -upgrade <patch-filename>`.
 - Step 6** Start ACS services.
-

Applying db-patch (ACS Solution Engine)

Apply the patch by using the standard ACS SE patch process. The patch will:

- Stop ACS services.
- Run **CSUpdate**.
- Restart ACS services.

Rollback is not available for this kind of patch.

LDAP Databases

To check LDAP databases, use the **LDP.exe** utility. For information on using **LDP.exe**, see the articles at the Microsoft website.

Logging

ACS provides a number of logging resources. You can use this section for guidelines on troubleshooting information that is available in the logs.

This section contains:

- [Log File Size, page 1-14](#)
- [Services that Generate Log Files, page 1-14](#)
- [Services that Log and Monitor ACS, page 1-15](#)
- [Service Log Files on the Remote Agent, page 1-16](#)
- [Examples of Logs, page 1-16](#)

Log File Size

Configuration of log file size differs between platforms.

ACS for Windows

The service log files can become large when running at a logging level of Full. Therefore, you should limit the log file size to 10 MB or less on ACS for Windows.

To set log file size limits on ACS for Windows:

-
- Step 1** Choose **System Configuration > Logging**.
 - Step 2** In the CSV column for ACS Service Monitoring, click **Configure**.
 - Step 3** Click the **When size is greater than option**, and set the size (in KB).
-

You can limit the size of other CSV log files by using the same steps.

**Note**

You should reset the logging level after collection of the troubleshooting information.

Solution Engine

ACS presets logging levels on the Solution Engine.

Services that Generate Log Files

The ACS services can generate the log files in [Table 1-3](#):

Table 1-3 ACS for Windows Log Files

Service	Location and File
CSAdmin	<ACS_install_dir>\CSAdmin\logs. The last file is ADMN.log.
CSRADIUS	<ACS_install_dir>\CSRADIUS\logs. The last file is RDS.log.
CSTacacs	<ACS_install_dir>\CSTacacs\logs. The last file is TCS.log.
CSAuth	<ACS_install_dir>\CSAuth\logs. The last file is Auth.log.
CSMon	<ACS_install_dir>\CSMon\logs. The last file is CSMon.log.
CSDBSync	<ACS_install_dir>\CSDBSync\logs. The last file is CSDBSync.log.
CSLog	<ACS_install_dir>\CSLog\logs. The last file is CSLog.log.
CSUtil	<ACS_install_dir>\utils\logs. The last file is CSUtil.log.

Services that Log and Monitor ACS

Services log and monitor ACS include:

- **CSLog**—A logging service for audit-trailing, accounting of authentication, and authorization packets. **CSLog** collects data from the **CSTacacs** or **CSRADIUS** and **CSAuth**, and then processes the data so that the data can be stored into CSV files or forwarded to databases:
 - ACS for Windows can forward data to an Open DataBase Connectivity (ODBC)-compliant database.
 - ACS for Windows and the Solution Engine can forward data when using the **syslog** protocol.

ACS copies remote agent log files to the server that is running the remote agent. For complete information on configuring log files for the remote agent, see the *User Guide for Cisco Secure Access Control Server*.

- **CSMon**—Responsible for the monitoring, recording, and notification of ACS performance, including automatic response to some scenarios. For example, if the TACACS+ or the RADIUS service stops functioning, ACS by default restarts all the services, unless otherwise configured.

Monitoring includes the overall status of ACS and the system on which ACS is running. **CSMon** actively monitors three basic sets of system parameters:

- **Generic host system state**—Monitors disk space, processor utilization, and memory utilization.
- **Application-specific performance**—Periodically performs a test login each minute by using a special built-in test account by default.
- **System resource consumption by ACS**—**CSMon** periodically monitors and records the usage by ACS of a small set of key system resources. Handles counts, memory utilization, processor utilization, thread used, and failed login attempts; and, compares these to predetermined thresholds for indications of a typical behavior.

CSMon works with **CSAuth** to track user accounts that are disabled for exceeding their failed-attempts count maximum. If configured, **CSMon** provides immediate warning of brute-force attacks by alerting the administrator that a large number of accounts have been disabled.

By default, **CSMon** records exception events in logs in the CSV file and Windows Event Log. You can also configure event notification by e-mail, so that notification for exception events and outcomes includes the current state of ACS at the time of the message transmission. The default notification method is Simple Mail Transfer Protocol (SMTP) e-mail, but you can create scripts to enable other methods.

However, if the event is a failure, **CSMon** takes the actions that are hard-coded when ACS detects the triggering event. Running the **CSUtil.exe** utility, which captures most of the parameters that deal with the state of the system at the time of the event, is one such example. If the event is a warning event, it is logged, the administrator is notified if it is configured, and no further action is taken. After a sequence of retries, **CSMon** also attempts to fix the use of the failure and individual service restarts. You can integrate custom-defined actions with **CSMon** service, so that a user-defined action occurs based on specific events.

Service Log Files on the Remote Agent

The remote agent generates these service log files:

- CSAgent.log
- CSWinAgent.log
- CSLogAgent.log

These logs should be correlated to the corresponding timestamp in the Auth.log file on the appliance.



Note

You can find and copy these files on the machine that is running the remote agent.

Examples of Logs

The examples in this section show the output of various logging activities.

Administration Report

Choose **Reports and Activity > Administration Audit** to display the administration report log. The examples in this section show typical administration report log entries:

Setting Up

```
09/01/2006,13:27:57,freezer,local_login,127.0.0.1,Administration session started
09/01/2006,13:28:33,freezer,local_login,127.0.0.1,"Administration Control" Added new
administrator account (admin)
09/01/2006,13:29:46,freezer,local_login,127.0.0.1,"Administration Control" Added new
administrator account (test)
09/01/2006,13:30:31,freezer,local_login,127.0.0.1,Updated "Administration Control -
Password Policy."
09/03/2006,13:31:14,freezer,local_login,127.0.0.1,Administration session finished
```

Login After Two Days

```
09/03/2006,13:31:44,freezer,-SECURITY-,127.0.0.1,Administrator 'test' password change
forced.
09/03/2006,13:31:55,freezer,-SECURITY-,127.0.0.1,Administrator 'test' password changed.
09/03/2006,13:31:55,freezer,test,127.0.0.1,Administration session started
09/03/2006,13:32:16,freezer,test,127.0.0.1,Administration session finished
```

Login After Four Days

```
09/07/2006,13:32:42,freezer,-SECURITY-,127.0.0.1,Administrator 'test' account locked out.
09/07/2006,13:32:56,freezer,admin,127.0.0.1,Administration session started
```

Administration Diagnostic Log

Find `<ACS_install_dir>/CSAdmin/Logs/ADMIN.log` to open the administration diagnostic log. The examples in this section show typical administration diagnostic log entries:

Login FAIL

```
LOGIN PROCESS: Start: Admin 'test'. Details: Never Exp. Flag:0x0 Attempt Lock:0x0 Attempt  
Count:0x0  
LOGIN PROCESS: Admin 'test' Invalid Credentials
```

Login FAIL and LOCK

```
LOGIN PROCESS: Start: Admin 'test'. Details: Never Exp. Flag:0x0 Attempt Lock:0x0 Attempt  
Count:0x1  
LOGIN PROCESS: Admin 'test' Invalid Credentials  
LOGIN PROCESS: Administrator 'test' has been locked out.
```

Login After LOCK

```
LOGIN PROCESS: Start: Admin 'test'. Details: Never Exp. Flag:0x0 Attempt Lock:0x1 Attempt  
Count:0x8  
LOGIN PROCESS: Locked Administrator 'test' has attempted login.
```

Force Change to Password

```
LOGIN PROCESS: Start: Admin 'test'. Details: Never Exp. Flag:0x0 Attempt Lock:0x0 Attempt  
Count:0x0  
LOGIN PROCESS: Admin 'test' Password Policy Results in Password Change Required.
```

Lock Through Password Age or Inactivity

```
LOGIN PROCESS: Start: Admin 'test'. Details: Never Exp. Flag:0x0 Attempt Lock:0x0 Attempt
Count:0x0
LOGIN PROCESS: Admin 'test' Password Policy Results in Locked Account.
```

CSAuth Log File

The **CSAuth** service logs contain the output from the various user databases modules. However, you must increase the logging level to capture all of the information.

CSAuth log file example:

```
AUTH 30/01/2008 13:05:20 I 1742 1300 0x1e pvauthenticateUser: authenticate 'permit202'
against CSDB
AUTH 30/01/2008 13:05:20 I 5448 1300 0x1e Done UDB_authenticate_USER, client 1, status
UDB_PASSWORD_REQUIRED
AUTH 30/01/2008 13:05:23 I 5803 1300 0x1e Worker 2 processing message 92.
AUTH 30/01/2008
13:05:23 I 2780 1300 0x1e Start UDB_authenticate_USER, client 1 (127.0.0.1)
```

To interpret the log file entries:

- **Timestamp**—The time that is associated with the entry.
- **Entry Type**—I means Information. E means Error. You can use the command **CSUtil.exe -e** to get a description of the error.
- **Source Line Number**—A four digit number such as 5081 (for internal reference only).
- **Thread ID**—A four digit number such as 1300. You can use this number to identify the work of individual worker threads. You can filter these logs in Excel to make identification easier.
- **Session ID**—A four digit hexadecimal number such as 0x1e. You can use this number to correlate between the Auth.log and TCS.log file, or between the Auth.log and RDS.log files.
- **Mnemonic commands and error codes**—Mnemonic commands and error codes improve readability of diagnostic logs. For example, `auth 30/01/2008 13:05:23 | 1300 0x1f Done UDB_USER_LOCN_CHECK, client 1, status UDB_USER_CLI_FILTERED`. A conversation starts with `Start RQnnnn` and is not complete until `Done RQnnnn` by the same thread ID. The command might handle multiple events.
 - A `Start` request without a corresponding `Done` (after a long time), indicates a block.
 - `AlloteThread failed with -1` means that the system is using the maximum worker threads. Ensure that your external databases are not using excessive delays.

In the previous **CSAuth** log file example, **CSAuth** challenges for the user's password. The following example shows the reaction of **CSTacacs** continuing session 0x1e, as it is seen in TCS.Log:

```
TCS 30/01/2008 13:05:20 I 0043 2060 0x1e <<< PACKET TO CLIENT:82.210.204.202
TYPE:AUTHEM/GETPASS, SEQ 4, FLAGS 1
TCS 30/01/2008 13:05:20 I 0043 2060 0x1e SESSIONID -2126998506 (0x81389416), DATALEN
16 (0x10)
TCS 30/01/2008 13:05:20 I 0043 2060 0x1e type=AUTHEM status=5 (AUTHEM/GETPASS)
flags=0x1
TCS 30/01/2008 13:05:20 I 0043 2060 0x1e msg_len=10, data_len=0
TCS 30/01/2008 13:05:20 I 0043 2060 0x1e MSG=Password:
TCS 30/01/2008 13:05:20 I 0043 2060 0x1e End >>>
```

EAP Logging

In ACS 4.x, EAP logging now displays messages in hexadecimal numbers (instead of ASCII characters). Use an external interpreter to get the detailed EAP message information.



Note

You can use a packet analyzer or a network sniffer to interpret EAP events.

Detailed logging of the EAP process in the Auth.log file produces output similar to:

```
EAP: PEAP-TLS: Process TLS data: SSL negotiation finished successfully
EAP: PEAP: next state = PROCESS_RESPONSE
EAP: PEAP: INNER: <-- EAP Request/EAP-Type=EAP-TLS (TLS Message (L bit set))
EAP: PEAP: <-- EAP Request/TLS Message (No bits set (last fragment))
EAP: EAP state: action = send
EAP: <-- EAP Request/EAP-Type=PEAP (identifier=11, seq_id=11)
Done UDB_SEND_RESPONSE, client 50, status UDB_CHALLENGE_REQUIRED
Worker 1 processing message 12.
Start UDB_SEND_RESPONSE, client 50 (127.0.0.1)
AuthenProcessResponse: process response for '0User301_107'
EAP: --> EAP Response/EAP-Type=PEAP (identifier=11, seq_id=11)
EAP: PEAP: --> EAP Response/TLS Message (No bits set (last fragment))
EAP: PEAP: INNER: --> EAP Response/EAP-Type=EAP-TLS (ACK)
EAP: PEAP: curr state = PROCESS_RESPONSE
EAP: PEAP: next state = PROCESS_RESPONSE
EAP: EAP state: action = authenticate pvauthenticateUser: authenticate '0User301_107'
against CSDB
EAP: PEAP: curr state = PROCESS_RESPONSE
EAP: PEAP-TLS: Comparing username from DB = 0User301_107 with username from certificate =
0User301_107
EAP: PEAP: next state = PROCESS_RESPONSE, inner protocol status = FPV
EAP: PEAP: INNER: <-- EAP Request/EAP-Type=EAP-TLV (TLV Type=RESULT, TLV Result=Success)
EAP: PEAP: <-- EAP Request/TLS Message (No bits set (last fragment))
EAP: EAP state: action = send
EAP: <-- EAP Request/EAP-Type=PEAP (identifier=12, seq_id=12)
Done UDB_SEND_RESPONSE, client 50, status UDB_CHALLENGE_REQUIRED
Worker 1 processing message 13.
Start UDB_SEND_RESPONSE, client 50 (127.0.0.1)
AuthenProcessResponse: process response for '0User301_107'
EAP: --> EAP Response/EAP-Type=PEAP (identifier=12, seq_id=12)
EAP: PEAP: --> EAP Response/TLS Message (No bits set (last fragment))
EAP: PEAP: INNER: --> EAP Response/EAP-Type=EAP-TLV (TLV Type=RESULT, TLV Result=Success)
EAP: PEAP: curr state = PROCESS_RESPONSE
EAP: PEAP: next state = FINISHED, inner protocol status = DONE
EAP: PEAP: curr state = FINISHED, inner protocol status = DONE EAP: PEAP: Second phase:
EAP-TLS authentication finished SUCCESSFULLY
EAP: PEAP: <-- EAP Success EAP: EAP state: action = send_done
EAP: <-- EAP Success/EAP-Type=PEAP (identifier=12, seq_id=13)
[PDE]: PolicyMgr::Process: request type=3; context id=1; applied default profiles (0) - do
nothing [PDE]: PdeAttributeSet::addAttribute: PDE-Group-ID-16=0
[PDE]: PolicyMgr::Process: request type=4; context id=1; applied default profiles (0) - do
nothing
Done UDB_SEND_RESPONSE, client 50, status UDB_OK
```

Command Line Utilities

ACS provides command line utilities for ACS for Windows and the Solution Engine. You can use the information in this section to troubleshoot by using the command line utilities. In addition, this section provides information on database backup and replication.

This section describes how to use:

- [CSUtil.exe \(Windows Only\)](#), page 1-20
- [The Remote Agent CLI \(Solution Engine Only\)](#), page 1-22

CSUtil.exe (Windows Only)

ACS provides the **CSUtil.exe** utility, which you can use for troubleshooting as well as for other activities. You can also use **CSUtil.exe** for database backup and replication.

Location and Syntax

You can find the **CSUtil.exe** utility at: `<ACS_install_directory>\bin\`.

The command syntax is:

```
CSUtil.exe [-q] [-b <backup filename> ] [-c] [-e <number>] [-g] [-i <file>]
[-d [-p <secret key>] <database dump filename>] [-l <file> [-passwd <secret key>]] [-n]
[-r <all|users|config> <backup file> ] [-s] [-u] [-y] [-listUDV] [-addUDV <slot>
<filename.ini>] [-delUDV <slot>] [-t] [-filepath <full filepath>] [-passwd <password>]
[-machine] [-a | -g <group number> | -u <user name> | -f <user list filepath>]
```

Some options require that you to stop the services. To stop services, you use the **net stop** command. The next example shows typical output from the **net stop** command:

```
C:\> net stop CSAuth
The CSAuth service is stopping.
The CSAuth service was stopped successfully.
C:\>
```

For complete information on the **CSUtil.exe** utility, see the *User Guide for Cisco Secure Access Control Server*.

Backing Up and Restoring the ACS Internal Database

Choose **System Configuration** and then click **ACS Backup** or **ACS Restore** to backup or restore the ACS internal database. If you want to backup or restore an external script, use **CSUtil.exe**. The command syntax for database backup by using **CSUtil.exe** is:

```
C:\Program Files\CiscoSecure ACS v4.x\bin\CSUtil -b filename.
```

[Table 1-4](#) describes the options that support backup and restore.

Table 1-4 Backup and Restore Options

Option	Description
-b	Back up system to a named file.
-d	Dump user and group information to a text file (default: dump.txt).
-e	Decode error number to ASCII message.
-g	Dump only group information to a text file (default: group.txt).
-i	Import user or NAS information (default: import.txt).
-l	Load internal data from a text file (created by the <i>-d</i> option).
-n	Create or initialize the ACS database.

Table 1-4 Backup and Restore Options (continued)

Option	Description
-q	Run CSUtil.exe in quiet mode.
-r	Restore system from a named file (created by using the <i>-b</i> option).
-u	List users by group (default: users.txt).

For example:

```
C:\Program Files\CiscoSecure ACS v4.x\bin\CSUtil -b backup.dat
CSUtil v4.1, Copyright 1997-2006, Cisco Systems Inc
All running services will be stopped and re-started automatically.
Are you sure you want to proceed? (Y or N) (Y)
Done
C:\Program Files\CiscoSecure ACS v4.x\bin>
```

To restore a database, enter:

```
C:\> CSUtil -r [users|config | all] filename
```

The Backup Process

During backup:

- ACS stops services, which means that user authentication does not occur during the backup.
- You are prompted for confirmation. You use the quiet mode to bypass this confirmation.

The backup contains:

- User and group information.
- System configuration.

If a component of the backup is empty, a `Backup Failed` message appears for the empty component. To un-install or upgrade, copy the backup file to a safe location; otherwise, it will be removed.

The Restore Process

During restore, ACS stops services. You can restore user and group information, or system configuration, or both.

Creating a Dump Text File

A dump text file contains only the user and group information. This file is useful for troubleshooting user profile issues. Cisco support may be able to download your dump file for troubleshooting of user configuration issues.

Before creating a dump file, you must manually stop the **CSAuth** service by entering:

```
C:\> net stop CSAuth
```

User authentication stops while the **CSAuth** service is stopped. You must manually start the service when you are finished creating the dump file by entering:

```
C:\> net start CSAuth
```

To create the dump file, enter:

CSUtil -d filename

You use the *-l* option to load the dump file and the *-p* option to reset password aging counters. For example:

```
CSUtil -p -l filename
C:\Program Files\CiscoSecure ACS v4.1\bin\CSUtil -r all backup.dat
CSUtil v4.1, Copyright 1997-2006, Cisco Systems Inc.
Reloading a system backup will overwrite ALL current configuration information All Running
services will be stopped and re-started automatically.
Are you sure you want to proceed? (Y or N)(Y)
CSBackupRestore(IN) file C:\Program Files\CiscoSecure ACS v4.x\bin\System Back
up\CRL Reg.RDF not received, skipping..
Done
```

The loading of a dump file replaces existing data.

Exporting User and Group Information

You can export user or group information to a text file for troubleshooting of configuration issues.

Before exporting, you must manually stop the **CSAuth** service by entering:

```
C:\> net stop CSAuth
```

User authentication stops while the **CSAuth** service is stopped. You must manually start the service when you are finished with the export, by entering:

```
C:\> net start CSAuth
```

To export user information to users.txt, enter:

```
CSUtil.exe -u
```

To export group information to groups.txt, enter:

```
CSUtil.exe -g
```

The Remote Agent CLI (Solution Engine Only)

ACS provides the Remote Agent CLI, which you can use for troubleshooting as well as other activities. You can also use the Remote Agent CLI for database backup and replication.

CLI Commands

ACS Solution Engine 4.x CLI commands are useful for troubleshooting. When direct access to the operating system is blocked, the CLI incorporates some additional commands as described in [Table 1-5](#).

Table 1-5 CLI Commands

CLI Command	Description
help	List commands.
show	Show appliance status.
support	Collect logs, registry, and other useful information. Send package.cab to FTP server.

Table 1-5 CLI Commands (continued)

CLI Command	Description
backup	Back up Appliance database to FTP server.
restore	Restore Appliance from FTP server.
download	Download ACS Install Package from distribution server.
upgrade	Upgrade appliance (stage II).
rollback	Roll back patched package.
exportgroups	Export group information to FTP server.
exportusers	Export user information to FTP server.
exportlogs	Export appliance diagnostic logs to FTP server.
ping	Verify connections to remote computers.
tracert	Determine the route taken to a destination.
set admin	Set administrator's name.
set domain	Set DNS domain.
set hostname	Set the appliance hostname.
set ip	Set IP configuration.
set password	Set administrator's password.
set dbpassword	Set database encryption password.
set time	Set timezone, enable Network Time Protocol (NTP) synchronization or set date and time.
set timeout	Set the timeout for serial console with no activity.
start <service>	Start an ACS service.
stop <service>	Stop an ACS service.
reboot	Soft reboot appliance.
restart	Restart ACS services.
shutdown	Shut down the appliance.
unlock	Unlock administrator.
remove	Remove administrator.
add	Add administrator.

Diagnostic Output from the Show Command

The show command provides diagnostic information that can be very helpful when you are resolving problems on the Solution Engine. Output from the show command resembles:

```
acs-sus-a1> show

acs-sus-a1
Cisco Secure ACS: 4.0.1.42
Appliance Management Software: 4.0.1.42
Appliance Base Image: 4.0.1.1
CSA build 4.0.1.543.2: (Patch: 4_0_1_543)
ACS Appliance GUI Logon: (Patch: 4_0_1_44)
Session Timeout: 10
```

```

Last Reboot Time: Thu Apr 12 00:19:33 2007

Current Date & Time: 4/19/2007 19:00:13
Time Zone: (GMT+01:00) Paris
NTP Server(s): NTP Synchronization Disabled.

CPU Load          Free Disk          Free Physical Memory
0.00%             16.2 GB           656 MB

Appliance IP Configuration
  DHCP Enabled. . . . . : No
  IP Address. . . . . : 10.56.24.91
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.56.24.1

CPU Load          Free Disk          Free Physical Memory
0.00%             16.2 GB           656 MB

Appliance IP Configuration
  DHCP Enabled. . . . . : No
  IP Address. . . . . : 10.56.24.91
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.56.24.1

--- Please press enter to continue ---
  DNS Servers . . . . . : 64.103.101.184
                       144.254.71.184

CSAdmin          running
CSAuth           running
CSDbSync         running
CSLog            running
CSMon            running
CSRADIUS         running
CSTacacs         running

CSAgent          stopped

```

Using the Web Interface with the Solution Engine

You can use the web interface with the Solution Engine to:

- **Set and view system information**—Choose **System Configuration > Appliance Configuration** to:
 - Edit the host name and domain name.
 - Reset the timer or to synchronize with the NTP server.
 - Start or stop the **CSAgent** service.
 - Configure SNMP.
 - Reboot or shut down the appliance.
- **View appliance software versions**—Choose **System Configuration > Appliance Upgrade Status** to view:
 - Appliance Base Image (OS + MS-hotfixes).
 - Appliance Management Software (CLI).
 - ACS software versions.
 - List of patches that were installed on that appliance.

You can also download and upgrade patches.

- **View appliance diagnostic logs**— Choose **System Configuration > View Diagnostic Logs** to view the:
 - AcsInstallLog
 - AcsApplianceInstallLog
 - ApplianceLog
 - CSAlog
 - CSSecurityLog
- **View services usage**— Choose **System Configuration > Support** screen to:
 - View all running ACS services and resource usage (CPU, Virtual Memory, Handle Count, Thread Count).
 - Configure the package.cab collector. Choose **Run Support Now** to immediately execute the collector.



CHAPTER 2

Common Problems

This chapter describes common problems associated with the Cisco Secure Access Control Server, hereafter referred to as ACS.

This chapter contains:

- [Administration, page 2-1](#)
- [Authentication and Authorization, page 2-5](#)
- [Browser, page 2-8](#)
- [Cisco Network Admission Control, page 2-10](#)
- [Databases, page 2-14](#)
- [Dial-In Connections, page 2-19](#)
- [EAP Protocols, page 2-23](#)
- [GAME Protocol, page 2-23](#)
- [Installations and Upgrades, page 2-26](#)
- [Interoperability, page 2-29](#)
- [Logging, page 2-30](#)
- [MAC Authentication Bypass Problems, page 2-31](#)
- [Remote Agent \(ACS Solution Engine\), page 2-32](#)
- [Reports, page 2-32](#)
- [User Group Management, page 2-34](#)

Administration

This section contains:

- [Unauthorized Users Logging In, page 2-2](#)
- [Restart Services Does Not Work, page 2-3](#)
- [Event Notification E-Mail Not Received, page 2-3](#)
- [Remote Administrator Cannot Access Browser, page 2-3](#)

- [Remote Administrators Cannot Log In](#), page 2-4
- [Remote Administrator Receives Logon Failed... Message](#), page 2-4
- [Remote Administrator Cannot Access ACS](#), page 2-4

**Note**

For information on using the command line interface (CLI) to execute administrative commands, see the “Administering Cisco Secure ACS Solution Engine” chapter of the appropriate installation guide.

Administrator Locked Out

Condition

ACS has locked out an administrator.

Action

- For ACS for Windows:
 - Option 1—Re-enable Local Login, then reset accounts through the web interface.
 - Option 2—Enter:

```
CSUtil -s a unlock <Admin> <Password>
```

- For the ACS Solution Engine, enter the CLI **unlock** command:

```
unlock-guiadmin <Admin> <Password>
```

**Tip**

If compliance permits, click the **Account Never Expires** option for one account to prevent lockout.

**Note**

For information on using the CSUtil utility, see the appropriate user guide. For information on using the command line interface (CLI) to execute administrative commands, see the “Administering Cisco Secure ACS Solution Engine” chapter of the appropriate installation guide.

Unauthorized Users Logging In

Condition

Unauthorized users can log in.

Action

-
- Step 1** List the start and end IP addresses for the **Reject listed IP addresses** option.
 - Step 2** Choose **Administrator Control > Access Policy**.
 - Step 3** Specify the **Start IP Address** and **End IP Address**.
-

Restart Services Does Not Work

Condition

The Restart Services option in the web interface does not restart the services.

Action (ACS for Windows)

The system is not responding. To manually restart services:

1. From the Windows **Start** menu, choose **Settings > Control Panel > Administrative Tools > Services**.
2. Choose *service_name* > **Stop > Start**, where *service_name* can be **CSAdmin, CSAuth, CSDBSync, CSLog, CSMon, CSRADIUS, CSTacacs**.

If the services do not respond when manually restarted, reboot the server.

Action (ACS Solution Engine)

The system is not responding to the **restart** command on the System Configuration > Service Control page. Open a console and use the **show** command to determine server status. If necessary, use the CLI to stop the service. See [Chapter 1, “The Remote Agent CLI \(Solution Engine Only\).”](#)

To manually restart services, log in to the ACS console and enter the **restart** command, a space and the name of the ACS service that you want to restart.

Event Notification E-Mail Not Received

Condition

The administrator is configured for event notification but is not receiving event notification e-mails.

Action

Be certain that the:

- SMTP server name is correct.
- Computer that runs ACS can **ping** the SMTP server.
- Computer that runs ACS can send e-mail by using a third-party e-mail software package.



Note

The e-mail address cannot contain underscores (_).

Remote Administrator Cannot Access Browser

Condition

A remote administrator cannot bring up the ACS web interface in a browser, or receives a warning that access is not permitted.

Action

To recover from this condition:

1. Verify that you are using a supported browser. Refer to the Installation Guides for a list of supported browsers.

2. Use the **show** command with the Remote Agent console.
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.

Remote Administrators Cannot Log In

Condition

Remote administrators cannot log in.

Action

-
- Step 1** List no start or end IP addresses for the **Allow only listed IP addresses to connect** option.
- Step 2** Choose **Administrator Control > Access Policy**.
- Step 3** Specify the **Start IP Address** and **End IP Address**.
-

Remote Administrator Receives Logon Failed... Message

Condition

When browsing, a remote administrator receives the `Logon failed . . . protocol error message`.

Action (ACS for Windows)

Restart the **CSAdmin** service. To restart the **CSAdmin** service:

1. From the Windows **Start** menu, choose **Control Panel > Services**.
2. Choose **CSAdmin > Stop > Start**.
3. If necessary, restart the server.

Action (ACS Solution Engine)

Restart the **CSAdmin** service. To restart the **CSAdmin** service, use the CLI **restart** command with **CSAdmin** as the argument. If necessary, reboot the appliance.

Remote Administrator Cannot Access ACS

Condition

A remote administrator cannot bring up ACS from the browser, or receives a warning that access is not permitted.

Action

If Network Address Translation (NAT) is enabled on the Project Information Exchange (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.

Authentication and Authorization

This section contains:

- [Windows Authentication Problems, page 2-5](#)
- [Dial-in Not Disabled, page 2-6](#)
- [Settings Not Inherited, page 2-6](#)
- [Retry Interval Too Short, page 2-6](#)
- [AAA Client Times Out, page 2-6](#)
- [Unknown NAS Error, page 2-7](#)
- [Key Mismatch Error, page 2-7](#)
- [Unexpected Authorizations, page 2-7](#)
- [RADIUS Extension DLL Rejected User Error, page 2-7](#)
- [Request Does Not Appear in an External Database, page 2-8](#)

Windows Authentication Problems

Condition

Problems diagnosing Windows authentications.

Action

Log in to the ACS server (by using the normal interactive Login field) with the same user credentials that you want ACS to validate. If the logon does not work, then ACS cannot authenticate. This condition indicates an AD configuration issue.

If the login works, but ACS does not authenticate, this condition indicates permission problems. Check the Auth.log file for the username, and look for errors. Review the permission requirements and be certain that ACS is running with proper privileges.

Dial-in Not Disabled

Condition

After the administrator disables the Dialin Permission setting, Windows database users can still dial in and apply the callback string that is configured under the Windows user database. (To locate the Dialin Permission check box, choose **External User Databases > Database Configuration > Windows Database > Configure.**)

Action

Restart the ACS services.

Settings Not Inherited

Condition

Users moved to a new group inherit new group settings, but they keep their existing user settings. Users did not inherit settings from the new group.

Action

Manually change the settings in the User Setup section.

Retry Interval Too Short

Condition

The retry interval is too short, and authentication fails.

Action

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.

AAA Client Times Out

Condition

The Authentication, Authorization, and Accounting (AAA) client times out when authenticating against a Windows user database.

Action

Increase the TACACS+ or RADIUS timeout interval from the default (5) to 20 by entering these Cisco IOS commands:

```
tacacs-server timeout 20
radius-server timeout 20
```

Unknown NAS Error

Condition

Authentication fails; the error `Unknown NAS` appears in the Failed Attempts log.

Action

To be certain that the Network Access Service (NAS) is recognized:

-
- Step 1** Verify that the AAA client is configured under the Network Configuration section.
- Step 2** If you have a 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 specified interface.
-

Key Mismatch Error

Condition

Authentication fails; the error `Key mismatch` appears in the Failed Attempts log.

Action

To be certain that the keys match:

-
- Step 1** Verify that the TACACS+ or RADIUS keys are identical in the AAA client and ACS (case sensitive).
- Step 2** Re-enter the keys to confirm that they are identical.
-

Unexpected Authorizations

Condition

The user can authenticate, but authorizations do not match expectations.

Action

Different vendors use different AV pairs. One vendor protocol may ignore the AV pairs used in another protocol, for example. Be certain that the user settings reflect the correct vendor protocol; for example, RADIUS (Cisco IOS/PIX).

RADIUS Extension DLL Rejected User Error

Condition

LEAP authentication fails. The error `Radius extension DLL rejected user` appears in the Failed Attempts log.

Action

To verify configured authentication type:

-
- Step 1** Verify that the correct Authentication type has been set on the Access Point. Be certain that, at a minimum, you checked the Network-EAP check box.
- Step 2** If you are using an external user database for authentication, verify that ACS supports the database. For information on the external databases that ACS supports, see *User Databases*, in the *User Guide for Cisco Secure Access Control Server*.
-

Request Does Not Appear in an External Database

Condition

An authentication request does appear in an external database.

Action

To verify that the authentication request is being forwarded:

-
- Step 1** Set logging to Full. Choose **System Configuration > Service Control** to set the logging.
- Step 2** Check the Auth.log file for confirmation that the authentication request is being forwarded to the third-party server. If the authentication request is not being forwarded, confirm that the external database configuration is correct, as well as the unknown user policy settings.
-

TACACS+ Authentication is Failing

Condition

TACACS+ authentication is failing.

Action

Examine the Failed Attempts log. If you observe unusual strings in place of the username, then check for a configuration error in the TACACS+ client NAS, and correct the configuration of the device.

Browser

This section contains:

- [Cannot Access the Web Interface, page 2-9](#)
- [Pages Do Not Appear Properly, page 2-9](#)
- [Browser crash when trying to open ACS, page 2-9](#)

- [Session Connection Lost](#), page 2-10
- [Administrator Database Corruption \(Netscape\)](#), page 2-10
- [Remote Administrator Cannot Browse](#), page 2-10

Cannot Access the Web Interface

Condition

The browser cannot display the ACS web interface.

Action

To fix the display:

-
- Step 1** Open Internet Explorer or Netscape Navigator. Choose **Help > About**, and determine the version of the browser. See the Installation Guide for a list of supported browsers, and the Release Notes for known issues with a particular browser version.
- Step 2** Check that **CSAdmin** service is running.
-

Pages Do Not Appear Properly

Condition

Parts of pages do not appear properly, parts of the page are missing, or the page is corrupted.

Action

To correct this condition:

-
- Step 1** Check that the Java Runtime Environment (JRE) is installed on the client machine.
- Step 2** Check for the correct JRE for applets in the browser advance option. See installation guide for web client requirements.
-

Browser crash when trying to open ACS

Condition

When opening ACS, the browser crashes.

Action

If you are using the JRE 1.5.0_00, upgrade to the current version of the JRE at the Java website.

Session Connection Lost

Condition

- The browser displays a Java message indicating that your session connection is lost.
- You cannot use the browser.

Action

To correct this condition:

1. Check the **Session idle timeout** value for remote administrators.
2. Choose **Administration Control Session Policy Setup**.
3. Increase the timeout value as needed.

Administrator Database Corruption (Netscape)

Condition

The administrator database appears to be corrupted when using Netscape.

Action

The remote Netscape client is caching the password. If you specify an incorrect password, it is still cached. When you attempt to re-authenticate with the correct password, Netscape sends the incorrect password. Clear the cache before attempting to re-authenticate, or close the browser and open a new session.

Remote Administrator Cannot Browse

Condition

Remote administrator intermittently cannot browse in the ACS web interface.

Action

To correct this condition:

1. Confirm that the client browser does not contain a proxy server configuration, because ACS does not support the HTTP proxy for remote administrative sessions.
2. Disable the proxy server settings.

Cisco Network Admission Control

This section contains:

- [Posture Problems, page 2-11](#)
- [Cisco IOS Commands Not Denied, page 2-11](#)
- [EAP Request Has Invalid Signature, page 2-12](#)
- [Administrator Locked Out of Client, page 2-12](#)
- [Cannot Enter Enable Mode, page 2-12](#)

- [Nonresponsive Endpoint Limit Reached, page 2-13](#)
- [NAC Posture Problem, page 2-13](#)
- [NAC Posture Problem, page 2-13](#)

Posture Problems

Condition

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 a line of hyphens (-----) instead of a posture.

Action

If you see a line of hyphens (-----), 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, be certain that the Cisco IOS/PIX `cisco-av-pair` VSA is correctly configured. For example, in a group configured to authorize NAC clients receiving a healthy SPT, be certain that the `[009\001] cisco-av-pair` check box is checked and that the SPT 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 the posture-token can send the incorrect SPT to the AAA client; or, if the AV pair name is mistyped, the AAA client is 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 the *User Guide for Cisco Secure Access Control Server*.

Cisco IOS Commands Not Denied

Condition

Under EXEC Commands, ACS is not denying Cisco IOS commands when checked.

Action

Examine the Cisco IOS configuration at the AAA client. If necessary, enter this Cisco IOS command into 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

Condition

ACS receives traffic from an EAP-enabled device that has the wrong shared secret, and ACS logs the error.

Action

Check whether:

- 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 Locked Out of Client

Condition

An administrator has been locked out of the AAA client because of an incorrect configuration setup in the AAA client.

Action

To correct this condition:

-
- Step 1** If you have a fallback method configured on your AAA client, disable connectivity to the AAA server and log in with the local or line username and password.
- Step 2** Try to connect directly to the AAA client at the console port.
- Step 3** If the direct connection is not successful, see your AAA client documentation or see the [Password Recovery Procedures](#) page on Cisco.com for information regarding your particular AAA client.
-

Cannot Enter Enable Mode

Condition

Unable to enter Enable Mode after performing `aaa authentication enable default tacacs+`. The system returns the error message: `Error in authentication on the router.`

Action

Check the Failed Attempts log. If the log reads `CS password invalid`, it may be that the user has no enable password set up. If you do not see the Advanced TACACS+ Settings section among the user setup options:

-
- Step 1** Choose **Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features**.
- Step 2** Select the option that configures the TACACS+ settings to appear in the user settings.

- Step 3** Choose **Max privilege for any AAA Client** (this will typically be 15).
- Step 4** Enter the **TACACS+ Enable Password** for the user.
-

Nonresponsive Endpoint Limit Reached

Condition

The system reaches the NAC Nonresponsive Endpoint (NRE) Guest Access Limit (GAL) of 100 endpoints.

Action

A feature in the EAPoUDP state table prevents denial of service (DoS) attacks on the ACS server by limiting RADIUS requests.

When the system reaches the maximum limit of 100 unauthorized nonresponsive endpoints per NAD, a warning 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 the Cisco Trust Agent, with default network access. The default access is whatever the router interface Access Control List (ACL) allows.

This message appears because 100 (or more) EAPoUDP sessions are in the INIT state. Normally, when 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 if the:

- NAD has more than 100 concurrently unauthorized endpoints.
- Router receives an Access-Reject from ACS.
- Router fails to receive a response from ACS.

Based on this behavior, your options are:

- Properly configure ACS for NAC to minimize unintentional Access-Rejects.
- When passively deploying NAC (monitor-only mode), configure ACS to accept all NREs by using a Media Access Control (MAC) or IP address wildcard with NARs in ACS.
- You should never have more than 100 unauthorized endpoints behind a single NAC-enabled router because they will prevent access for Cisco Trust Agent-enabled endpoints.
- Set the default hold period to a low value.

NAC Posture Problem

In ACS Release 4.1, the SPT is no longer configured in **Group Mapping for NAC Databases**. The posture result automatically sends the in the `cisco-av-pair`.

Authorization Policy

When you configure an authorization policy and choose Any in the user group or the posture token, you may want to configure None. For a group, Any refers to cases of posture only (no authentication). For a posture token, Any refers to cases of authentication only (no posture).

Databases

This section contains:

- [RDBMS Synchronization Not Properly Operating](#), page 2-14
- [Database Replication Not Properly Operating](#), page 2-14
- [External User Database Not Available](#), page 2-15
- [Unknown Users Not Authenticated](#), page 2-15
- [User Problems](#), page 2-15
- [Cannot Implement the RSA Token Server](#), page 2-16
- [ACE SDI Server Does Not See Incoming Request](#), page 2-16
- [External Databases Not Properly Operating \(ACS Solution Engine\)](#), page 2-17
- [Group Mapping \(ACS Solution Engine\)](#), page 2-17
- [Configuration of Active Directory](#), page 2-18
- [NTLMv2 Does Not Work](#), page 2-19

RDBMS Synchronization Not Properly Operating

Condition

RDBMS synchronization is not properly operating.

Action

Be certain that the correct server appears in the Partners list.

Database Replication Not Properly Operating

Condition

Database replication is not properly operating.

Action

- Be certain that you have correctly set the server as Send or Receive.
- On the sending server, be certain that the receiving server is in the Replication list.
- On the receiving server, be certain that the sending server is chosen in the Accept Replication from list. Also, be certain that the sending server is not in the replication partner list.
- Be certain that no ACS server is associated with a master server (in the right column) in order to avoid loops.
- Be certain 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 an AAA server to the AAA Servers table in the Network Configuration for every IP address of the receiving server.

External User Database Not Available

Condition

The external user database is not available in the Group Mapping section.

Action

The external database has not been configured in the External User Databases section; or, the username and password have been incorrectly typed. Click the applicable external database. Be certain that the username and password are correct.

Unknown Users Not Authenticated

Condition

Unknown users are not authenticated.

Action



Note

If you are using the ACS Unknown User feature, external databases can only authenticate by using the Password Authentication Protocol (PAP).

To authenticate unknown users:

-
- Step 1** Choose **External User Databases > Unknown User Policy**.
 - Step 2** Click the **Check the following external user databases** option.
 - Step 3** From the External Databases list, choose the database(s) against which to authenticate unknown users.
 - Step 4** Click the **right arrow** key to add the database to the Selected Databases list.
 - Step 5** Click **Up** or **Down** to move the selected database into the correct position in the authentication hierarchy.
-

User Problems

Condition

The same user appears in multiple groups or duplicate users exist in the ACS internal database. You cannot delete the user from the database.

Action

To clean up the database, you use **CSUtil.exe** from the command line and enter:

```
CSUtil -q -d -n -l dump.txt
```

This command uses the database to be unloaded and reloaded to clear the counters.

**Tip**

When you install ACS in the default location, **CSUtil.exe** is located in:
C:\Program Files\CiscoSecure ACS vX.X\bin.

For more information on using the **CSUtil.exe** command, see the *User Guide for Cisco Secure Access Control Server*.

Cannot Implement the RSA Token Server

Condition

You cannot successfully implement the RSA token server.

Action

To recover from this problem:

-
- Step 1** Log in to the computer that is running ACS. (Be certain that your login account has administrative privileges.)
 - Step 2** Be certain that the RSA client software is installed on the same computer as ACS.
 - Step 3** Follow the setup instructions. Do not restart at the end of the installation.
 - Step 4** Get the file named `sdconf.rec` from the `\data` directory of the RSA ACE server.
 - Step 5** Place the `sdconf.rec` file in the `%SystemRoot%\system32` directory.
 - Step 6** Be certain 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.)
 - Step 7** Verify that support for RSA is enabled in the External User Database > Database Configuration in the ACS.
 - Step 8** Run **Test Authentication** from the Windows control panel for the ACE client application.
 - Step 9** From ACS, add the token server to the external database list.
-

ACE SDI Server Does Not See Incoming Request

Condition

On the Active Collaboration Engine (ACE) Systems Development and Integration (SDI) server, no incoming request is seen from ACS, although the RSA agent authentication works.

Action (ACS for Windows, ACS Solution Engine)

For dial-up users, be certain that you are using PAP and not Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) or Challenge Handshake Authentication Protocol (CHAP). RSA SDI does not support CHAP and ACS does not send the request to the RSA server; rather, ACS will log an error for external database failure.

External Databases Not Properly Operating (ACS Solution Engine)

Condition

External databases are not properly operating.

Action

Run **cssupport.exe** to generate a package.cab file in order to collect logging information for the SE.

Be certain that the Remote Agent is properly installed and configured. See the *Installation and Configuration Guide for Cisco Secure Remote Agents 4.x*.

Be certain that a two-way trust (for dial-in check) is established between the ACS domain and the other domains. Check the Auth.log file for any debug messages beginning with [External DB].

Group Mapping (ACS Solution Engine)



Note

On some servers, you should configure ACS services with the Local System account. On other servers, it will be necessary to configure a domain account (for example, create an account called ACS in the AD domain and assign appropriate privileges). In some extreme cases, it may be necessary to make this account a member of Domain Administrators.

Condition

During configuration of group mapping, the user sees a failure message in a popup window:

Failed to enumerate Windows groups. If you are using AD consult the installation guide for information

Action

This problem may occur if:

- ACS services do not have privileges to execute the **NetGroupEnum** function. For information go to MSDN on the Microsoft website.
- NetBIOS over TCP is not enabled.
- DNS is not correctly working. You can try reregistering by entering **ipconfig /flushdns** and then **ipconfig /registerdns** from a DOS prompt. Otherwise, go to the Microsoft website for more information.
- RPC is not correctly working (for example, after Blaster Update). Go to the Microsoft website and check for these hot fixes:
 - kb822831
 - kb823980
 - kb824105
 - kb824146
- The domain controllers are not synchronized. To synchronize, use the **net time** command from a DOS prompt: **net time /Domain: <DomainName>**.
- Different SPs are running on different domain controllers.
- The **NetLogon** service is not up and running on all domain controllers.

- Check that packet filters are installed.
- Choose **yes** on the DNS properties to **Allow Dynamic Updates**.

Configuration of Active Directory



Note

On some servers, ACS services should be configured with the Local System account. On other servers, it will be necessary to configure a domain account (for example, create an account called ACS in the AD domain and assign appropriate privileges). In some extreme cases, you might have to make this account a member of Domain Administrators.

Condition

You must configure Active Directory for ACS.

Action

On the domain controller serving the ACS server:

-
- Step 1** Create a user and provide a strong password.
 - Step 2** Make the user a member of Domain Admins group.
 - Step 3** Make the user a member of the Administrators group.
 - Step 4** On the Windows 2000 server that is running ACS:
 - a. Add a new user to the local group.
 - b. Choose **Administrative Tools** from the Windows control panel.
 - c. Choose **Computer Management > Local Users and Groups > Groups**.
 - d. Double-click the **Administrators** group, and then click **Add**.
 - e. Choose the domain from the **Look in** box.
 - f. Double-click the user created earlier to add the user, and then click **OK**.
 - Step 5** Give the new user special rights on ACS server:
 - a. Choose **Administrative Tools** from the control panel.
 - b. Choose **Local Security Policy > Local Policies**.
 - c. Open **User Rights Assignment**.
 - d. Double-click on **Act as part of the operating system** and click **Add**.
 - e. Choose the domain from the **Look in** box.
 - f. Double-click the user that you created earlier to add it and click **OK**.
 - g. Double-click on **Log on as a service**, and click **Add**.
 - h. Choose the domain from the **Look in** box.
 - i. Double-click the user created earlier to add the user, and click **OK**.
 - Step 6** Set the ACS services to run as the created user:
 - a. Choose **Open Administrative Tools** from the control panel.
 - b. Choose **Services**.

- c. Double-click the **CSAdmin** entry.
 - d. Click the **Log On** tab, and then click **This Account** and **Browse**.
 - e. Choose the domain, double-click the user created earlier. Click **OK**.
- Step 7** Repeat the steps for the rest of the CS services.
- Step 8** Wait for Windows to apply the security policy changes, or reboot the server. If you rebooted the server, skip the rest of these instructions.
- Step 9** Stop and then start the **CSAdmin** service.
- Step 10** Open the ACS web interface.
- Step 11** Choose **System Config > Service Control > Restart**.
- Step 12** If the **Domain Security Policy** is set to override settings for the **Act as part of the operating system** and **Log on as a service** rights, you must also make the user rights changes listed previously to the policy.
-

NTLMv2 Does Not Work

Condition

NTLMv2 does not work.

Action

You must have the appropriate version of Windows installed (or a certain service pack) and configure the domain controllers registry to request NTLMv2. For additional information, see Microsoft article #239869.

Dial-In Connections

This section contains:

- [Cannot Connect to AAA Client \(No Report\)](#), page 2-20
- [Cannot Connect to the AAA Client \(Windows External Database\)](#), page 2-20
- [Cannot Connect to AAA Client \(ACS Internal Database\)](#), page 2-21
- [Cannot Connect to AAA Client \(Telnet Connection Authenticated\)](#), page 2-22
- [Cannot Connect to AAA Client \(Telnet Connection Not Authenticated\)](#), page 2-22
- [Callback Not Working](#), page 2-22
- [Authentication Fails When Using PAP](#), page 2-23

Cannot Connect to AAA Client (No Report)

Condition

A dial-in user cannot connect to the AAA client.

No record of the attempt appears in the TACACS+ or RADIUS Accounting Report. From the navigation bar, click **Reports and Activity**, then click **TACACS+ Accounting** or **RADIUS Accounting** or **Failed Attempts** to check for the record.

Action

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 modem configuration on an AAA client, not ACS.
- LAN connections for the AAA client and the computer that is 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 keys in the AAA client and ACS are identical (case sensitive).
- Command **ppp authentication pap** is entered for each interface, if you are using a Windows user database.
- Command **ppp authentication chap pap** is entered for each interface, if you are using the ACS internal database.
- 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
- ACS Services (**CSAdmin**, **CSAuth**, **CSDBSync**, **CSLog**, **CSRADIUS**, **CSTacacs**) are running on the computer that is running ACS.

Cannot Connect to the AAA Client (Windows External Database)

Condition

A dial-in user cannot connect to the AAA client, and you configured the Windows user database for authentication.

ACS creates a record of a failed attempt in the Failed Attempts Report in the Reports and Activity section.

Action

Create a local user in the ACS internal database and test whether authentication is successful. If it is successful, the issue is user information that is not correctly configured for authentication in Windows or ACS.

From 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 disable the account.
- User Properties for the dial-in window does not disable dial-in permission, if ACS is using this option for authentication.

From within ACS confirm that:

- If the username is already entered into ACS, a Windows user database is configured for the user in the Password Authentication list on the User Setup page.
- If the username is already entered into ACS, the ACS group to which the user is assigned has the correct authorization enabled (such as IP and PPP, IPX and PPP or Exec and Telnet). Click **Submit + Restart** if you make a change.
- The user expiration information in the Windows user database has not used a failed authentication. For troubleshooting purposes, disable password expiry for the user in the Windows user database.

Then:

-
- Step 1** Click **External User Databases > Database Configuration**.
 - Step 2** Click **List All Databases Configured**, and then be certain that the database configuration for Windows is listed.
 - Step 3** Click **External User Databases > Unknown User Policy** to be certain that the Fail the attempt option is not chosen. And be certain that the Selected Databases list reflects the necessary database.
 - Step 4** Verify that the Windows group to which the user belongs has not been mapped to No Access.
-

Cannot Connect to AAA Client (ACS Internal Database)

Condition

A dial-in user cannot connect to the AAA client, and the ACS internal database is being used for authentication.

A record of a failed attempt appears in the Failed Attempts Report (choose **Reports and Activity**, then click **Failed Attempts**).

Action

In ACS, confirm that the:

- Username is entered into ACS.
- ACS internal database is chosen from the Password Authentication list and a password has been entered in User Setup for the user.
- ACS group to which the user is assigned has the correct authorization protocols enabled (such as IP and PPP, IPX and PPP or Exec and Telnet). Click **Submit + Restart** if you made a change.
- Expiration information has not used a failed authentication. Change the option to **Expiration: Never** for troubleshooting.

Cannot Connect to AAA Client (Telnet Connection Authenticated)

Condition

A dial-in user cannot connect to the AAA client; however, a Telnet connection can be authenticated across the LAN.

Action

Isolate the problem area. The possibilities are:

- A 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. You can modify authorization rights 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.

Cannot Connect to AAA Client (Telnet Connection Not Authenticated)

Condition

A dial-in user cannot connect to the AAA client, and a Telnet connection cannot be authenticated across the LAN.

Action

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, look for:

- 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 Not Working

Condition

Callback is not working.

Action

Be certain that Callback works on the AAA client when using local authentication; then, add AAA authentication.

Authentication Fails When Using PAP

Condition

User authentication fails when using PAP.

Action

Outbound PAP is not enabled. If the Failed Attempts report shows that you are using outbound PAP:

-
- Step 1** Go to the Interface Configuration section and check the **Per-User Advanced TACACS+ Features** check box.
- Step 2** Choose the **TACACS+ Outbound Password** section of the **Advanced TACACS+ Settings** table on the **User Setup** page.
- Step 3** Enter and confirm the password in the boxes.
-

EAP Protocols

Condition

Problems with EAP protocols.

Action

The general troubleshooting strategy is the same for all EAP methods:

-
- Step 1** Examine the ACS the Auth.log file.
- Step 2** Enable debug logging on the NAD and examine the output.
- Step 3** Use a sniffer to get a protocol wire trace.
- Step 4** Examine any trace information that the client may provide.
- Step 5** Verify configurations throughout the network.
- Step 6** Confirm that credentials (certificates) are valid and installed.
-

**Note**

You can use the Microsoft Management Console (MMC) to examine user-based and machine-based certificates. For information on using the MMC, go to the Microsoft website.

GAME Protocol

This section contains:

- [GAME Configuration Problem, page 2-24](#)
- [GAME Troubleshooting Setup, page 2-24](#)

- [Expected Device-Type is Not Matched, page 2-25](#)
- [Device-type Attribute is Not Returned by the Audit Server, page 2-25](#)
- [Failure Returned by the Audit Server, page 2-25](#)

GAME Configuration Problem

Condition

The Generic Authorization Message Exchange (GAME) configuration is incorrect.

Action

To check the configuration, choose:

- **Network Access Profiles > Protocols** to be certain that you have checked **Allow Agentless Request Processing**.
- **Network Access Profiles > Posture Validation > Select Audit** to be certain that you checked an Audit Server to set up the appropriate device-type rules.
- **Posture Validation > External Posture Validation Audit Setup**, and verify that:
 - The Audit Server is configured with the correct URL.
 - The group and host are configured in Which Groups and Hosts are Audited.
 - Game Group Feedback is configured and Request Device Type from Audit Server is checked. The device-type attribute must be present in the ACS dictionary. If the attribute is not in the ACS dictionary, the Request Device Type from Audit Server check box is unchecked.

GAME Troubleshooting Setup

Condition

You need to troubleshoot the GAME feature.

Action

Assign policies and groups:

-
- Step 1** Be certain that the host to audit is configured or that Audit All Hosts is chosen.
- Step 2** Choose Audit all user groups.
- Step 3** Configure these unique groups:
- a. Configure a group for Assign this Group if Audit Server Did not Return a Device-Type.
 - b. Configure a Match-all rule and assign a group for all device-type strings that the audit server returns.
 - c. Choose **Network Access Profiles > Authentication** and configure a group for If Agentless Request was not Assigned.
-

Configure these logs:

- Passed and Failed Attempts
- Audit Device-Type (as a column to log)

Expected Device-Type is Not Matched

Condition

ACS cannot match a device-type.

Action

Check these configuration items:

- Configure the Game Troubleshooting Setup. See [GAME Troubleshooting Setup, page 2-24](#).
- After audit, the Group configured for **Match -all** is assigned.
- Audit Device-Type column shows the device type.
- Device-type as seen by ACS is reported in the Pass Authen log.

Device-type as seen by ACS is also reported in the CSAuth log and the output from the debugging mode of **CSAuth: DZAuth -p -z -v**.

```
[PDE]: PdeAttributeSet::addAttribute: Unix:Audit:Device-Type=IP Phone
[PDE]: AuditAction::Received device-type=IP Phone
[PDE]: PdeAttributeSet::addAttribute: PDE-Audit-Req-Device-Type-34=TRUE
```

Device-type Attribute is Not Returned by the Audit Server

Condition

The audit server does not return a device-type attribute.

The Auth.log file indicates that the Audit Server did not Return Device Type.

```
[PDE]: PdeAttributeSet::addAttribute: PDE-Audit-Req-Device-Type-34=TRUE
[PDE]: Device type requested but Audit Server did not return device type
[PDE]: AuditAction::Invoking GAMEGroupMappingPolicy
```

Action

Verify configuration items and logging:

- Configure the GAME Troubleshooting setup. See [GAME Troubleshooting Setup, page 2-24](#).
- Be certain that the Audit Device-Type column is . . . (empty) in Passed Authentications Report.
- Be certain that, after audit, the Group configured for Assign this Group if AuditServer Did not Return a Device-Type is assigned.
- Check for a device type for a known device.

Failure Returned by the Audit Server

Condition

The audit server returns a failure.

The Auth.log file indicates Audit Server return zero length device type or an error parsing GAME response.

```
[PDE]: PdeAttributeSet::addAttribute:Unix:Audit:Device-Type=
[PDE]: Audit Server return zero length device type ...
[PDE]: PolicyMgr::Process: last action result=-2147 Audit policy failed (-2147),
attempting fail open
```

```
[PDE]: Error parsing GAME response: Could not find element AttributeValue under element
saml:Attribute
[PDE]: PolicyMgr::Process: last action result=-2165 Audit policy failed (-2165),
attempting fail open
```

Action

Verify these configuration items:

- GAME Troubleshooting setup. See [GAME Troubleshooting Setup, page 2-24](#).
- Audit Device-Type column is . . . (empty) in the Pass Authen Report.
- The Group configured for “If agentless request was not assigned a user-group” is assigned, after the audit.
- Audit Server is accessible and functional (that is, posture audit works with the same server).

Installations and Upgrades

This section contains:

- [rad_mon.dll and tac_mon.dll In Use Condition, page 2-26](#)
- [During Upgrade the ACS Folder is Locked, page 2-27](#)
- [During Uninstall the ACS Folder is Locked, page 2-27](#)
- [After Restart ACS Cannot Start Services, page 2-27](#)
- [Upgrade or Uninstall Cannot Complete, page 2-28](#)
- [Invalid File or Data, page 2-28](#)
- [Accounting Logs Missing, page 2-28](#)
- [Upgrade Command Does Not Work \(ACS Solution Engine\), page 2-29](#)
- [On Solaris, autorun.sh Does Not Execute \(ACS Solution Engine\), page 2-29](#)

System Requirements

Be certain that you have installed your release according to the requirements in the Installation Guide and Release Notes that accompany the release.

rad_mon.dll and tac_mon.dll In Use Condition

Condition

The *rad_mon.dll* and *tac_mon.dll* files remain in use after uninstall and **clean.exe**. The in-use condition then prevents a new installation of ACS.

Action

Restart the computer in order to clear the in-use condition, or stop any service that is using the *.dll* files, such as **AgentSrv.exe**. You can use third-party tools, such as the Process Explorer, to find the processes that are using the *.dll* files.

During Upgrade the ACS Folder is Locked

Condition

When upgrading ACS, **setup.exe** hangs and displays an error message: The CiscoSecure ACS folder appears to be locked by another application... . Please close any applications that are using any files or directories and re-run Uninstall.

Action

-
- Step 1** Remove excess log files. ACS stores log files in \CiscoSecure ACS v.x.x\Logs. If any log file folder gets too large, and you cannot upgrade, you must first delete all but the last three log files from the folder. When ACS starts up, choose **System Configuration > Service Control**.
- Step 2** In the Services Log File Configuration, check **Manage Directory**, and choose **Keep only the last <n> files**. Set <n> to 3.
- Step 3** If **PNLogAgent** is running, stop that service to release any locks that the service might have on the folder.
-

During Uninstall the ACS Folder is Locked

Condition

When uninstalling, the ACS folder is locked.

Action

Check for:

Condition	Solution
A CSUtil.exe process from an aborted restore is still in a created but not started state.	Restart.
Another application such as Notepad has an file open.	Close the application.
An explorer has a subfolder of ACS install open.	Close the explorer.

After Restart ACS Cannot Start Services

Condition

When the Windows Firewall Internet Connection Sharing (ICS) service has started on Windows 2003, SP1, ACS cannot start these services:

- **CSAuth**
- **CSRADIUS**
- **CSTacacs**
- **CSAdmin**

Action

Manually start the services, or disable the ICS service.

To disable the ICS service:

- Step 1** Locate the Windows Firewall and Internet Connection Sharing (ICS) service.
 - Step 2** Right-click on the service and choose **Properties**.
 - Step 3** Change the **Startup Type** to **Disabled**.
-

Upgrade or Uninstall Cannot Complete

Condition

Upgrade or uninstall cannot finish.

Action

Close:

- Step 1** All ACS files.
 - Step 2** All log files, for example, the Auth.log file.
 - Step 3** All programs.
 - Step 4** Programs such as **Reddest**, and close any binaries that are running.
 - Step 5** Microsoft Management Console (MMC) tools such as the **Performance Monitor**. For information on how to use the MMC, go to the Microsoft website.
-

Invalid File or Data

Condition

An error message appears when you try to upgrade or uninstall ACS: The following file is invalid or the data is corrupted "DelsL1.isu".

Action

From the Windows Registry, delete the following Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CiscoSecure

Accounting Logs Missing

Condition

All previous accounting logs are missing.

Action

When reinstalling or upgrading the ACS software, these files are deleted; unless they have been moved to an alternative directory location.

Upgrade Command Does Not Work (ACS Solution Engine)

Condition

From the serial console, the **upgrade** command has no effect.

Action

You must first obtain an appliance upgrade. Choose **System Configuration > Appliance Upgrade**.

On Solaris, autorun.sh Does Not Execute (ACS Solution Engine)

Condition

While performing an upgrade when using a Solaris distribution server, **autorun.sh** cannot be executed.

Action

Enter the Unix command **chmod +x autorun.sh** to grant execution permissions to **autorun.sh**.

Interoperability

This section contains:

- [Interoperation Between Builds, page 2-29](#)
- [Proxy Requests Fail, page 2-29](#)

Interoperation Between Builds

Condition

Interoperation between different builds of ACS does not work.

Action

Interoperation between different builds is not supported. The builds must match.

Proxy Requests Fail

Condition

Proxy requests to another server fail.

Action

Be certain that the:

- Direction on the remote server is set to Incoming and Outgoing or Incoming, and that the direction on the authentication forwarding server is set to Incoming and Outgoing or Outgoing.
- Shared secret (key) matches the shared secret of one or both ACSs.
- Character string and delimiter match the stripping information configured in the Proxy Distribution table, and the position is set correctly to Prefix or Suffix.

If the previous conditions are met, one or more servers is probably down; or, no fallback server is configured. Click **Network Configuration** from the navigation bar 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.

Logging

This section describes troubleshooting procedures for log files. For related information, see [Reports, page 2-32](#).

This section contains:

- [Too Many Log Files, page 2-30](#)
- [Logging Messages, page 2-31](#)

Too Many Log Files

Condition

When upgrading ACS, **setup.exe** hangs and displays an error message: `The CiscoSecure ACS folder appears to be locked by another application Please close any applications that are using any files or directories and re-run Uninstall.`

Action

If the problem still exists after closing applications and re-running the uninstall program, it could be that the folder is locked because of large number of log files.

Remove excess log files. ACS stores log files in `\CiscoSecure ACS v.4.x\Logs`. If a log file folder becomes too large, and you cannot upgrade, you must:

-
- Step 1** Delete all but a small number of files from the folder (for example, 3).
 - Step 2** When ACS starts up, choose **System Configuration > Service Control**.
 - Step 3** In the Services Log File Configuration, check **Manage Directory**, and check **Keep only the last <n> files**.
 - Step 4** Set <n> to a small number (for example, 3).
-

Logging Messages

Table 2-1 provides detailed explanations of certain logging messages.

Table 2-1 Logging Message Explanations

Message	Explanation
No such session	A NAS requests session resumption, but ACS does not have a related cached session.
External DB account locked out	An external user database such as AD or LDAP has locked the account.
External DB user invalid or bad password	An external user database has found an invalid user name or password. For security reasons the database responds with the error message and separate error messages such as <code>user name invalid</code> or <code>password invalid</code> .
External DB account restriction	The external database (AD or LDAP) has locked or disabled the account.
NAS duplicate authentication attempt	ACS is set to a low timeout value and the device is expected a reply in a short time.

MAC Authentication Bypass Problems

This section contains:

- [The MAC Address Exists in LDAP but Always Maps to the Default User Group, page 2-31](#)
- [The MAC Exists in the Internal Database but is Mapped to the Wrong User Group, page 2-32](#)
- [Request is Rejected, page 2-32](#)

The MAC Address Exists in LDAP but Always Maps to the Default User Group

Condition

MAC exists in LDAP but always maps to the default user-group.

Action

To correct this condition:

1. Check the LDAP configuration.
2. Check the LDAP Group Mapping settings.
3. Verify that the MAC address format stored in the LDAP server is one of the supported formats.
4. Check that the LDAP server is reachable.

The MAC Exists in the Internal Database but is Mapped to the Wrong User Group

Condition

The MAC exists in the internal database but is mapped to the wrong user-group.

Action

Check that the MAC address or a prefix of the address does not exist in a previous mapping.

Request is Rejected

Condition

Request is rejected.

Action

To correct this condition:

- Be certain that the Agentless Request Processing in the Protocols page is enabled.
- Check that the User-Group mapped by the MAC address is not disabled.
- Check the NAP authorization rules.

Remote Agent (ACS Solution Engine)

This section describes troubleshooting for the Remote Agent.

RPC Timeouts

When the appliance sends requests to the Remote Agent, it will wait no more than 60 seconds for a reply.

Reports

This section contains:

- [Blank Reports, page 2-33](#)
- [Unknown User Information Missing, page 2-33](#)
- [Two Entries Logged for One User Session, page 2-33](#)
- [Old Format Dates Persist, page 2-33](#)
- [Logging Halted, page 2-34](#)
- [Logged in Users Report Works Only with Certain Devices, page 2-34](#)

For related information, see [Logging, page 2-30](#).

Blank Reports

Condition

A report is blank.

Action

Be certain that you choose **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**.

Condition

The *lognameactive.csv* report is blank.

Action

You changed protocol configurations recently.

Whenever protocol configurations change, the existing *lognameactive.csv* report file is renamed to *lognameyyyy-mm-dd.csv*, and a new, blank *lognameactive.csv* report is generated.

Unknown User Information Missing

Condition

No Unknown User information is included in reports.

Action

The Unknown User database was changed. Accounting reports will still contain unknown user information.

Two Entries Logged for One User Session

Condition

Two entries are logged for one user session.

Action

Be certain 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.

Old Format Dates Persist

Condition

After you have changed the date format, the Logged-In User list and the **CSAdmin** log still display old format dates.

Action

To see the changes that you made, you must restart the **CSAdmin** services and log on again.

Logging Halted

Condition

Unavailability of logging affects authentication functionality.

Action

When local or remote logging normal operation is halted, authentication functionality will stop after a very short time because all worker threads are busy with logging assignments. Fixing the logging functionality will restore authentication; thus, troubleshooting the logging service logs is necessary.

Logged in Users Report Works Only with Certain Devices

Condition

The Logged in Users report works with some devices, but not with others.

Action

For the Logged in Users report to work (and this also applies to most other features involving sessions), packets should include:

- **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 limited time between the start and stop packets (for example, HTTP through the PIX Firewall), the Logged in Users report may fail.

User Group Management

This section contains:

- [MaxSessions Not Working Over VPDN, page 2-35](#)
- [MaxSessions Fluctuates, page 2-35](#)
- [MaxSessions Does Not Take Effect, page 2-35](#)
- [TACACS+ and RADIUS Attributes Missing, page 2-35](#)

MaxSessions Not Working Over VPDN

Condition

MaxSessions over a Virtual Private Dialup Network (VPDN) is not working.

Action

The use of MaxSessions over VPDN is not supported.

MaxSessions Fluctuates

Condition

User MaxSessions fluctuates or is unreliable.

Action

Services were restarted, possibly because the connection between the ACS and the AAA client is unstable. Uncheck the **Single Connect TACACS+ AAA Client** check box.

MaxSessions Does Not Take Effect

Condition

User MaxSessions not taking effect.

Action

Be certain that you have accounting configured on the AAA client, and that you are receiving accounting start or stop records.

TACACS+ and RADIUS Attributes Missing

Condition

TACACS+ and RADIUS attributes do not appear on the Group Setup page.

Action

Be certain that you have configured at least one RADIUS or TACACS+ AAA client in the Network Configuration. Be certain that you have enabled the appropriate attributes in the Interface Configuration.

**Note**

Some attributes are not customer-configurable; instead, ACS sets their values.



APPENDIX A

Error Codes

Revised: May 18, 2011, OL-12555-02

Table A-1 provides an alphabetized list of the ACS error codes. For complete information on error codes, see the Microsoft website.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
ACS Failed Attempts:EAP type not configured Username = "anonymous"	The Allow Anonymous In-Band PAC Provisioning option is not enabled.	Check whether a valid certificate has been installed on the ACS server as the ACS server must have the correct certificate installed.
A valid EAP-FAST master key does not exist; make sure EAP-FAST replication is operational	Failed to get the master key for Protected Access Credentials (PAC) construction.	Check the EAP-FAST replication configuration.
Access denied because no profile matched	The authentication request does not match any NAP.	Check the NAP configuration.
Access denied to Voice-Over-IP group	If the user is present in the Voice-Over-IP (VOIP) group, the authentication fails.	Enable access to a VOIP group; or, assign a new group for the user.
Access denied: fast-reconnect was successful, but user was not found in cache	Fast-Reconnect is enabled and the dynamic user is removed from ACS.	Disable Fast-Reconnect and try authenticating. Re-enable Fast Reconnect.
Access rejected due to authorization policy in the network access profiles	The request for NAP authorization policy failed.	Check the NAP configuration policy.
ACS account disabled	The administrator has disabled the account.	The administrator must enable the account.
ACS ARAP password invalid	Incorrect ARAP password.	Provide the correct ARAP password.
ACS CHAP password invalid	The password provided for CHAP is invalid.	Provide a valid password.
ACS login time restriction	The user is denied access at a specific time.	Change the login time restriction or ensure that the authentication occurs only during the specified time.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
ACS MSCHAP password is invalid	The password provided for MS-CHAP is invalid.	Provide a valid password.
ACS password invalid	Invalid password.	Use a valid password.
ACS User Account Expired	The user account has expired.	Create a new user account.
ACS User exceeded max sessions	The ACS user has exceeded the maximum session.	Wait for the current session to end and try again.
ACS user unknown	The user is not present in the ACS internal DB.	Create the user in the ACS internal DB.
ACS user's password has expired	Configure a new password.	Configure a new password.
ACS account disabled	The administrator has disabled the account.	The administrator must enable the account.
Audit Server returned an error	The audit server returned an error.	Check the audit server configuration.
Authentication protocol is not allowed for this network access profile	Protocol is not allowed for the current NAP.	Check the NAP configuration and modify it, if required.
Authentication session invalidated	The session does not exist.	Check the NAS configuration and open a new session.
Authentication type not supported by ExternalDB	The external DB does not support the specified authentication type.	Use an authentication that the external DB supports.
Badly formed Downloadable ACL request from device	The download request for ACL contains a missing Message-Authenticator or AAA: event VSA.	Use the correct ACL format.
Cached token rejected/expired	The cached token has expired or is rejected.	Use a new token.
Certificate name or binary comparison failed	Machine certificates do not match or the name in the certificate and the user account do not match.	Use correct certificates.
CLI user unknown	The given CLI user is unknown.	Use a valid user name.
Could not access password aging state in ACS internal DB	Unable to access the password state after age check.	Restart ACS and try again.
Could not check password aging state in ACS internal DB	Unable to check the password-aging state in the ACS internal DB.	Check the ACS configuration for password aging.
Could not communicate with external policy server - authentication failure	Unable to reach the external policy server; or, the server is down.	Check the connection to the external policy server.
Could not communicate with external policy server - wrong HCAP version	Unable to communicate with the external policy server; wrong Host Credentials Authorization Protocol (HCAP) version.	The HCAP version of ACS and the external policy server are different.
Could not communicate with the Audit Server	The audit server cannot be reached or is down.	Check the connection to the external audit server.
Could not connect to external policy server - timeout error	Unable to communicate with the external policy server.	Check the external policy server configuration.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
Could not open a connection to external policy server	Unable to reach the external policy server or the sever is down.	Check the connection to the external policy server.
Could not open a connection to external policy server - Could not validate server certificate	Unable to open a connection with the external policy server.	Unable to validate server certificate. Check the validity of the server certificate.
DB object lock not granted	Unable to access the DB.	Try accessing the DB again.
EAP-FAST anonymous in-band provisioning is disabled	The Allow Anonymous In-Band PAC Provisioning option is disabled in the EAP-FAST configuration settings.	Enable the option.
EAP-FAST authenticated in-band provisioning is not disabled	The EAP-FAST Authenticated In-Band Provisioning option is not disabled.	Check the ACS EAP-FAST configuration.
EAP-FAST Type not configured	The supplicant requesting for EAP-FAST authentication, is not configured in ACS.	Enable EAP-FAST at the global level; or, at the matched profile (NAP) level.
EAP-FAST user ID does not match to initiators ID presented inside the PAC	The client sends a PAC with an initiator ID that does not match the user ID.	Check the configuration of the supplicant.
EAP-FAST users PAC is invalid	The client sends an expired PAC.	The client sends an expired PAC.
EAP_LEAP Type not configured	The supplicant requesting for EAP-LEAP authentication, is not configured in ACS.	Enable LEAP at global level.
EAP_MSCHAP Type not configured	The supplicant requesting for authentication from EAP-PEAP or EAP-FAST with EAP-MSCHAP as the inner method, is not configured in ACS.	Enable EAP-MSCHAP as the inner method for PEAP; or EAP-FAST, at the global level or matched profile (NAP) level.
EAP_PEAP Type not configured	The supplicant requesting for EAP-PEAP authentication is not configured in ACS.	Enable EAP-PEAP at the Global level; or, at matched profile (NAP) level.
EAP-TLS or PEAP authentication failed during SSL handshake	This failure occurs when: <ul style="list-style-type: none"> The server validation is not configured correctly on the client. The machine certificate is not provisioned on the machine (when used with EAP-TLS). Unable to provide a user certificate for authentication. The AAA server certificate has expired. The Root CA certificate is not installed or is not installed correctly on the client. The same CA certificate is used for intermediate CA or Root CA certificate: Root CA duplication. 	If the Certification Authority (CA) or ACS certificates have expired or are missing, distribute, renew, or update the certificates to the clients trusted root certificate store. Check if NTP is enabled on the client and ACS. Install the appropriate CA certificate on your system as Authenticated in-band PAC Provisioning requires a valid Trusted Root CA certificate. We do not recommend self-signed certificates. Use a CA instead.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
EAP_TLS Type not configured	The supplicant requesting for EAP-TLS authentication is not configured in ACS.	Enable EAP-TLS at global level; or, at NAP.
EAP-TLS or PEAP authentication failed due to unknown CA certificate during SSL handshake	The supplicant used an invalid certificate.	Install the correct certificate in ACS; or, in the supplicant.
EAP-TLS or PEAP authentication failed due to different protocol version during SSL handshake	This error occurs when there is a difference in the TLS version.	No configuration required for ACS.
EAP-TLS or PEAP authentication failed due to invalid certificate during SSL handshake	The supplicant used an expired, or revoked, or invalid certificate.	Install the correct certificate in the supplicant.
Enabling TACACS+ is not allowed for this Access Server	The Enable Privilege option is set in the TACACS+ Advanced options.	Check the access server configuration.
Error assigning RADIUS Authorization Components to a user	Unable to locate RADIUS Authorization Components (RAC) for the user.	Check the RAC configuration.
Error communicating with the audit server, or invalid response was returned	Unable to reach the audit server; or, the server is down.	Check the audit server connectivity and configuration.
Error parsing Audit Server Response	The audit server displayed an error while parsing the request.	Check the version of the audit server and ACS supports it.
External DB account disabled	The External User Account is disabled.	The windows administrator must reset this option.
External DB account expired	The External User Account has expired.	The windows administrator must reset this option.
External DB account locked out	The External User Account is locked.	The windows administrator must reset this option.
External DB account restriction	The Windows User Account is restricted.	The windows administrator must reset this option.
External DB ARAP password is invalid	The ARAP password is invalid.	Provide the correct password.
External DB CHAP password is invalid	The CHAP password is invalid.	Use the correct password.
External DB did not return MPPE key material	If the remote RADIUS server does not return the MSCHAP-MPPE-Keys attribute, the MPPE key material cannot be extracted and returned to CSAuth. This is required for an Aironet LEAP authentication.	If the remote RADIUS server does not return the MSCHAP-MPPE-Keys attribute, the MPPE key material cannot be extracted and returned to CSAuth. This is required for an Aironet LEAP authentication.
External DB EAP authentication failed	When an invalid EAP password is used, authentication fails.	Check the configuration of the supplicant.
External DB is not configured	The supplier key is not present in the registry; or, the external DB does not exist for the user.	The supplier key is not present in the registry or the external DB does not exist for the user.
External DB is not configured for this network access profile	An external DB is not configured for the unknown user policy.	Configure the external DB.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
External DB is not operational	An external server such as the RSA token server is not operational or does not respond.	Check if the external server is working or is correctly configured.
External DB MSCHAP password is invalid	The MSCHAP password is invalid.	Use a valid password.
External DB password expired	The user password has expired.	Reset the user's windows password.
External DB password invalid	If an invalid or empty password is provided during RSA token authentication, the PIN is rejected.	Provide the correct PIN.
External DB reports about an error condition	<p>This error occurs when:</p> <ul style="list-style-type: none"> • The DSN fails to open. • The ODBC authentication occurs again and CSAuth tries a reload or initialize. • The LDAP interface initialization fails; or, winsock initialization fails for RADIUS authentication. • The external ODBC DB is not available while checking for an unknown user policy. • Any error occurs during authentication. <p>When these conditions occur, ACS discards or rejects the configuration.</p>	Configure the external DB in ACS correctly. Check the connectivity and functioning of the external DB by using another tool.
External DB user invalid or bad password	An authentication failure has occurred in NTAauth.	Check the configuration of the supplicant.
External DB user unknown	Invalid user.	Enter a valid user.
External user not found	User is not present.	Check for the user in the DB.
Failed to allocate IP address for a user	Check the configuration of the IP address pool.	Check the configuration of the IP address pool.
Internal error	An unknown error code is generated when the auth failure code is not found.	Check the logs.
Internal error assigning RADIUS Authorization Components attributes	Iterator for RAC is not created.	Check the RAC configuration.
Internal error during Downloadable ACL exchange	Internal error.	Check the logs in full mode.
Internal error while assigning Downloadable ACL to a user	The ACL is not present in the Shared Profile Component (SPC) database.	Check the ACL configuration.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
Internal Error due to Invalid Password Type	This error occurs due to an: <ul style="list-style-type: none"> Invalid external DB Corrupted DB Un-supported upgrade path or restore 	Reconfigure the external DB, remove the dynamic user and re-authenticate it.
Internal Error due to Invalid Service control data	This error occurs when services crash or hang.	Restart the services.
Internal Error due to NDG Creation Error	This error occurs when the internal data or memory handling is invalid.	Restart the services.
Internal Error due to Invalid State	This error occurs when the internal data or memory handling is invalid.	Restart the services.
Internal Error due to initialization failure	This error occurs when the DLL is not found; or, is not loaded.	Check for the correct DLL.
Internal Error due to Invalid Authentication Type	This error occurs due to an invalid authentication type.	Check the authentication type and external DB.
Internal Error due to Failure of Replication	This error occurs due to an exception in the replication.	Restart the services.
Internal Error due to raise of exception	This error occurs due to high stress.	Restart the services.
Internal Error due to logging activity	This error occurs when there is a failure in logging.	Restart the services.
Internal Error due to invalid context handle	This error occurs when there is a delay in receiving the challenge.	The supplicant must send the challenge at the appropriate time.
Internal Error due to Authentication failure	This error occurs when invalid credentials are used.	Use valid credentials.
Internal Error due to Crypto Failure	This error occurs when the service does not have the required privileges.	The user must change the local policies related to crypt32.
Internal Error due to packet fragment handling error	This error occurs when the supplicant sends an invalid mail-packet.	The supplicant must send a valid packet.
Internal Error due to Registry Access Failure	This failure is caused by external APIs.	The supplicant must run the service with valid privileges.
Internal Error due to invalid user-id	This error occurs if the user-profile is not present in ACS.	Use a valid username.
Invalid API Data received	CSAuth uses an error code while processing a request from CSTACACS or CSRADIUS.	
Invalid CHAP Data received	The supplicant used invalid data for the CHAP protocol.	Check the supplicant configuration.
Invalid EAP Data received	The supplicant used invalid data for the ARAP protocol.	Check the supplicant configuration.
Invalid message authenticator in EAP request	Invalid authentication code in keywrap message.	Check the NAS or supplicant configuration.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
Invalid MS-CHAP Data received	The supplicant used invalid data for the MS-CHAP protocol.	Check the supplicant configuration.
Invalid Protocol Data	This error occurs when: <ul style="list-style-type: none"> ACS receives invalid data. CHAP challenge of less than 1 byte is received. An empty EAP message occurs in a conversation between NAS and ACS. 	Check the NAS configuration.
Invalid PDE Data received	The supplicant used invalid posture data.	Check the supplicant configuration.
Invalid RDBMS Sync Data received	Invalid data for RDBMS Sync.	Check the configuration.
Invalid TEAP Data received	The supplicant used invalid data for the TEAP protocol.	Check the supplicant configuration.
Invalid TLV Data received	The supplicant used invalid data for the TLV protocol.	Check the supplicant configuration.
Invalid VARSDB Data received	The supplicant used invalid data for the EAP protocol.	Check the supplicant configuration.
MAC auth bypass is not allowed	The Radius MAC authentication is not enabled. (Allow agentless request processing.)	Enable the Allow Agentless Request Processing option.
MAC-Authentication-Bypass group is disabled	This is a configuration issue.	Enable the respective group for MAC bypass.
Machine authentication is not permitted	This is a configuration issue.	In the windows external DB section, enable the Machine Authentication for the specific inner method.
Missing message authenticator in EAP request	This is a client related issue.	The client must send a message authenticator.
Number of audit round trips has exceeded limit	This is a configuration issue.	Increase the limit.
PEAP or EAP-FAST password change against Windows DB is disabled	This is a configuration issue.	Enable the Password Change option in the windows external DB.
Posture Validation failed because no profile matched	This is a configuration issue.	The profile must be configured.
Posture Validation Failure (general)	This is a general error.	Configure the posture server correctly.
Posture Validation Failure on External Policy	This is a general error.	Configure the posture server correctly.
Posture Validation Failure on Internal Policy	This is a general error.	Configure the posture server correctly.
TACACS+ enable password invalid	The password verification failed.	Use a valid password.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
TACACS+ enable privilege too low	This is a configuration issue.	Increase the Enable Privilege Level.
Token PIN changed	This is a configuration issue.	Use the changed PIN.
Unknown attributes were detected in the posture validation request	This is a client related issue.	The client must send valid attributes.
User requires a TACACS+ Enable Password	This is a configuration issue.	The client must use an enabled password.
User requires TACACS+ outbound password	This is a configuration issue.	The client must use an outbound password.
Users Access Filtered	This is a configuration issue.	Configure NAR correctly.
Users of this group are disabled	This is a configuration issue.	Enable the group.
Users Radius request rejected (by Radius extension DLL)	This is a general error.	The client must use valid credentials.
Users Usage Quota has been exhausted	This is a configuration issue.	The client must use valid accounting requests.
Windows dialin permission required	This is a configuration issue.	Enable Dialin Permissions.
Windows domain controller not found	This is a configuration issue.	Configure AD and DNS correctly.
Windows External DB user access was denied due to a Machine Access Restriction	This is a configuration issue.	Configure NAR correctly.
Windows login server unavailable	This is a configuration issue.	Configure AD and DNS correctly.
Windows login time restriction	This is a configuration issue.	Configure AD and DNS correctly.
Windows login type not granted	This is a configuration issue.	Configure AD correctly.
Windows password change failed	This is a configuration issue.	The client must use a valid password.
Windows user must change password	This is a configuration issue.	The client must change the password.
Windows workstation not allowed	This is a configuration issue.	Configure AD correctly.



INDEX

A

AAA client times out [6](#)
AAA servers
 troubleshooting [1](#)
accounting logs
 missing [28](#)
ACE SDI server [16](#)
ACS Backup [20](#)
ACS folder is locked [27](#)
ACS Restore [20](#)
ACS State Collector utility [6](#)
Active Directory
 configuration [18](#)
administrator
 database corruption [10](#)
 event notification [3](#)
 locked out [2, 12](#)
 remote (has no access) [4](#)
 remote (logon failed message) [4](#)
 remote access to browser [3](#)
 remote cannot browse [10](#)
 remote login [4](#)
antivirus software [13](#)
AppEventDump.txt file [10](#)
application-specific performance [15](#)
attributes
 missing [35](#)
audit server
 returns failure [25](#)
authentication
 cannot enable in TACACS+ [12](#)
 cannot enable on TACACS+ [12](#)

 diagnosing [5](#)
 failure with PAP [23](#)
 failures [2](#)
 for unknown NAS [7](#)
 logging halted [34](#)
 request not in external database [8](#)
 retry interval [6](#)
 TACACS+ fails [8](#)
 unknown users [15](#)
authorization
 policy [13](#)
 unexpected [7](#)
autorun.sh execution problems [29](#)

B

backup
 internal database [20](#)
 process [21](#)
browser
 access [3](#)
 cannot display web interface [9](#)
 crash on opening ACS [9](#)
 incomplete pages [9](#)
 lost connection [10](#)

C

callback not working [22](#)
cautions
 significance of [x](#)
Cisco IOS commands
 ACS does not deny [11](#)

CLI commands
 for troubleshooting 22
 conventions ix
 CSAdmin 15
 CSAgent.log 16
 CSAuth 15
 CSDBSync 15
 CSLog 15
 CSLogAgent.log 16
 CSMon 15
 CSRadius 15
 cssupport.exe 6, 8
 CSTacacs 15
 CSUtil 15
 CSWinAgent.log 16

D

databases

- ACS database files 13
- administrator database corruption 10
- external user database 15
- improper operation of external databases 17
- internal with bad MAC mapping 32
- LDAP with wrong MAC mapping 31
- RDBMS synchronization 14
- replication 14
- using LDP.exe with LDAP 13

devices

- check for problems 3
- missing in Logged in User report 34

device-type

- mismatch 25
- no attribute returned 25

dial-in users

- callback not working 22
- cannot connect 20
- dial-in not disabled 6

documentation

- conventions ix
- objectives ix
- related x

dump text file 21

E

EAP

- invalid signature 12
- logging 19

error codes 1

Error Message Decoder 6

Event Viewer files 10

external user database 15

F

Failed Attempts logs 2

Field Notices 5

G

GAME protocol

- audit server failure 25
- configuration 24
- policies and groups 24

generic host system state 15

group

- mapping problem 17
- move without inheriting new settings 6

I

installation

- related documentation x

interoperation does not work between builds 29

K

keys

match [7](#)

LLDP.exe utility [13](#)LEAP authentication failure [7](#)

logging

and authentication problems [34](#)failed attempts [2](#)interpreting logs [3](#)level [14](#)logging services [15](#)Passed Authentications [3](#)Remote Agent [16](#)removing log files [30](#)service logs [34](#)too many log files [30](#)two entries for one session [33](#)Windows services log files [14](#)

M

MAC address

with internal database [32](#)with LDAP [31](#)

MaxSessions

does not take effect [35](#)fluctuations [35](#)problems over VPDN [35](#)

monitoring

service [15](#)MSInfo.txt file [10](#)

NNAC Nonresponsive Endpoint limit [13](#)NRE limit [13](#)

NTLMv2

does not work [19](#)

OOutput Interpreter [6](#)

Ppackage.cab file [3,6](#)

policy

authorization [13](#)

posture

mismatches [11](#)Product Literature [5](#)

proxy requests

failures [29](#)

Rrad_mon.dll [26](#)

RADIUS

attributes missing [35](#)RADIUS extension DLL rejected user error [7](#)Radtest [4](#)RDBMS Synchronization [14](#)Registry File [10](#)rejected request [32](#)related documentation [x](#)

remote agent

log files [16](#)

replication

database [14](#)

reports

- blank [33](#)
- Logged in User reports lack devices [34](#)
- missing unknown user information [33](#)
- old format dates persist [33](#)
- request is rejected [32](#)
- resource.txt file [10](#)
- restart services [3](#)
- restore
 - internal database [20](#)
- restore process [21](#)
- retry interval [6](#)

S

- SecEventDump.txt file [10](#)
- Security Advisories, Responses and Notices [5](#)
- Security and Identity Management [5](#)
- Service Log Files [9](#)
- services
 - cannot restart [27](#)
 - restart [3](#)
 - starting [2](#)
- setup hangs [27](#)
- SPT
 - configuration [13](#)
- SysEventDump.txt file [10](#)
- System Posture Token
 - configuration [13](#)
- system resource consumption [15](#)

T

- tac_mon.dll [26](#)
- Tactest [4](#)
- token servers
 - no incoming requests [16](#)
 - RSA implementation [16](#)
- Troubleshoot and Alert [5](#)

- troubleshooting
 - AAA servers [1](#)
 - authentication [5](#)
 - authorization [5](#)
 - browser [8](#)
 - database [14](#)
 - dial-in connections [19](#)
 - EAP protocols [23](#)
 - GAME protocol [23](#)
 - installations [26](#)
 - interoperability problems [29](#)
 - logging [30](#)
 - MAC authentication bypass problems [31](#)
 - Network Admission Control [10](#)
 - Remote Agent [32](#)
 - reports [32](#)
 - upgrades [26](#)
 - user group management [34](#)
- Troubleshooting Guides [6](#)
- Troubleshooting TechNotes [5](#)

U

- unauthorized users [2](#)
- uninstall
 - cannot complete [28](#)
 - invalid file or data [28](#)
- unknown users [15](#)
 - information missing in reports [33](#)
- upgrade
 - cannot complete [28](#)
 - invalid file or data [28](#)
- upgrade command [29](#)
- user or group information
 - exporting [22](#)
- users
 - duplicate [15](#)

V

VPDN

MaxSessions not working [35](#)

W

warnings

significance of [x](#)

web interface

using with Solution Engine [24](#)

web pages

incomplete [9](#)

with Sybase [13](#)