



Troubleshooting

This appendix provides troubleshooting information for the Cisco Secure Access Control Server, Release 4.1, hereafter referred to as ACS.

This chapter contains the following topics:

- [Sources of Information, page A-2](#)
- [Common Problems, page A-14](#)
 - [Administration, page A-15](#)
 - [Authentication and Authorization, page A-18](#)
 - [Browser, page A-21](#)
 - [Cisco Network Admission Control \(NAC\), page A-23](#)
 - [Database, page A-26](#)
 - [Dial-In Connections, page A-31](#)
 - [EAP Protocols, page A-34](#)
 - [GAME Protocol, page A-35](#)
 - [Installations and Upgrades, page A-37](#)
 - [Interoperability, page A-40](#)
 - [Logging, page A-41](#)
 - [MAC Authentication Bypass Problems, page A-41](#)
 - [Remote Agent \(ACS Solution Engine\), page A-42](#)
 - [Reports, page A-42](#)
 - [User Group Management, page A-44](#)
- [Error Codes, page A-46](#)

Sources of Information

This section contains the following information:

- [Online Help](#), page A-2
- [Diagnostic Commands and Tools](#), page A-2
- [Collecting Diagnostic Information in package.cab](#), page A-3
- [Log Files](#), page A-5
- [Database Files](#), page A-8
- [Troubleshooting Using CSUtil.exe \(Windows Only\)](#), page A-8
- [Troubleshooting Using the CLI \(Solution Engine Only\)](#), page A-11
- [Services that Log and Monitor ACS](#), page A-13

Online Help

ACS provides the following online help:

- The Help pane on the right side of the web interface.
- The online help interface. Click the **Online Documentation** button 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.

Diagnostic Commands and Tools

ACS has extensive logging capabilities that allow an administrator to troubleshoot any issue pertaining to the ACS server itself (for example, replication) or an AAA request problem (for example, an authentication problem) from NAS.

Reports and Activity

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 CSV Failed Attempts log.
 - Step 2** On the **Configuration** page, move attributes from the **Attributes** column to the **Logged Attributes** column
 - Step 3** 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 Authentications report** checkbox in the **Enable Logging** pane.
-

**Note**

ACS provides additional reports in the System Configuration pane, such as CSV log files for Database Replication.

Radtest and Tactest

The Radtest and Tactest tools simulate the AAA requests that are sent 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 v4.1\bin. Go to <http://www.cisco.com> to find details on running these tools.

Collecting Diagnostic Information in *package.cab*

ACS services store information about their activities into various logging subdirectories. The ACS State Collector utility collects the log files needed for troubleshooting into a single file called *package.cab*. The utility also collects system information and user database information.

**Note**

ACS services stop while the utility collects information.

Creating and Testing *package.cab* on Windows

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 causes ACS to collect all debugging information.

To enable Full logging:

-
- Step 1** Choose **System Configuration > Service Control**.
 - Step 2** Choose **Full** for the **Level of Detail** in the **Service Log File Configuration** pane.
 - Step 3** Run a few tests that you are certain will fail.
 - Step 4** Run **cssupport.exe** from C:\Program Files\CiscoSecure ACS v4.1\bin\cssupport.exe. The default location for the *package.cab* file is \<ACS_install_dir>\Utils\Support.

When you return to normal operation, be sure to set the logging level to Low.

Creating *package.cab* from the Solution Engine

You use one of the following options to create the *package.cab* file from the Solution Engine:

- In the web interface, choose **System Configuration > Support > Run Support Now**.
- Run the **support** command from the CLI.

When the Solution Engine uses an external computer as a Remote Agent, running the **support** utility on the Solution Engine makes the Remote Agent collect its log files into one file. The filename is *<Pack_<computer name>_date_time>.cab* (for example, *Pack_ACS-SUS-A2_10-Sep-2006_15-50-48.cab*). To retrieve the support file, on the computer running the remote agent, open the CiscoSecure ACS Agent folder in the remote agent installation directory and download it to the administrator PC.

The Contents of *package.cab*

The *package.cab* file contains a large amount of information as described in this section, but the amount of information may be overwhelming. Use the guidelines in this section for interpreting *package.cab*.

The following files are available in *package.cab*:

- **Log Files**—Every service has a corresponding log file. These files contain extensive information about each service. For example, *auth.log* contains all the current log information of **CSAuth** service. ACS creates the log files every day, and the active log file is the file that does not have a date in its filename. For more information, see [Log Files, page A-5](#).
- **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.
- **User Database Files**—Three files go into making the ACS database: *user.dat*, *user.idx*, and *varsdb.mdb*. Unless Cisco requests these files, capturing these files is not necessary. Do not manipulate these files. For more information, see [Log Files, page A-5](#).
- **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.
- **Other Files**—*package.cab* also includes the following files:
 - *MSInfo.txt* contains the server and the operating system information.
 - The *resource.txt* file contains the ACS services resource usage information on the server.
 - *SecEventDump.txt*, *AppEventDump.txt*, and *SysEventDump.txt* contain an additional event dump on the server that you can use to troubleshoot any issues with the server itself.

Analyzing the Contents of *package.cab*

For every AAA request failure, you must first look at the Failed Attempts log and then search for the username in the *auth.log*. If an additional detail is needed, you must analyze the *TCS.log* or the *RDS.log*. Note that both **CSTacacs** and **CSRADIUS** form the communication bridge between the NAS and ACS, and **CSAuth** is the communication bridge between the **CSTacacs**, **CSRADIUS**, and any external user databases such as Active Directory and NDS.

The example in this section provides information on analyzing the contents of *package.cab*. In the example, a regular login authentication by the ACS server is failing. The NAS debug does not indicate the reason for the failure. You have the username.

To analyze the contents of *package.cab*:

-
- Step 1** Look at the Failed Attempts active.csv file to see why the user is failing. The information in this file can often give you the reason for failure so that you do not must further analyze the problem. However, for this example, the active.csv file does not provide the information.
- 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 could 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 log, the authentication request must be reaching ACS, and the first service that receives the packet is **CSTacacs**, as the communication protocol configured between the NAS and ACS is Terminal Access Controller Access Control System (TACACS+).
- Step 3** You therefore must 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. 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 *auth.log* because the packets are not being forwarded to the **CSAuth** service.

Log Files

This section contains the following troubleshooting information:

- [Log Files \(ACS for Windows Services\), page A-5](#)
- [Log Files \(Remote Agent\), page A-6](#)
- [General Procedure for Using Logs, page A-6](#)
- [Administration Report Log Examples, page A-6](#)
- [Administration Diagnostic Log Examples, page A-7](#)
- [CSAuth Log File Example, page A-7](#)
- [EAP Logging, page A-8](#)

Log Files (ACS for Windows Services)



Note

The service log files can get very large when running in Full debug mode.

The ACS for Windows services can generate the following log files:

Table A-1 ACS for Windows Log Files

Service	Location and File
CSAdmin	<ACS_install_dir>\CSAdmin\logs. Last file is ADMN.log
CSRADIUS	<ACS_install_dir>\CSRADIUS\logs. Last file is RDS.log
CSTacacs	<ACS_install_dir>\CSTacacs\logs. Last file is TCS.log

Table A-1 ACS for Windows Log Files (continued)

Service	Location and File
CSAuth	<ACS_install_dir>\CSAuth\logs. Last file is Auth.log
CSMon	<ACS_install_dir>\CSMon\logs. Last file is CSMon.log
CSDBSync	<ACS_install_dir>\CSDBSync\logs. Last file is CSDBSync.log
CSLog	<ACS_install_dir>\CSLog\logs. Last file is CSLog.log
CSUtil	<ACS_install_dir>\utils\logs. Last file is CSUtil.log

Log Files (Remote Agent)

The remote agent generates the following service log files:

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

These files should be correlated to the corresponding timestamp in *auth.log* on the appliance.

General Procedure for Using Logs

Follow this general procedure for using logs:

-
- Step 1** Ensure service log files are set to Full detail.
 - Step 2** Check the protocol traffic (**CSRADIUS/CSSTACACS**).
 - Step 3** Check *auth.log* for errors or hangs.
 - Step 4** Correlate the two timestamps.
 - Step 5** Check the Failed Attempts log and other logs.
-

Administration Report Log Examples

Choose **Reports and Activity > Administration Audit** to display the administration report log. The following examples 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 Examples

Choose `<ACS_install_dir>/CSAdmin/Logs/ADMIN.log` to open the administration diagnostic log. The following examples 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 Example

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

CSAuth log file example:

```
AUTH 08/05/2005 10:36:51 I 5081 3040 Start RQ1026, client 50 (127.0.0.1)
AUTH 08/05/2005 10:36:51 I 5081 3040 Done RQ1026, client 50, status -2046
AUTH 08/05/2005 10:36:52 I 5094 3040 Worker 2 processing message 299716.
AUTH 08/05/2005 10:36:52 I 5081 3040 Start RQ1027, client 50 (127.0.0.1)
```

Use the following information to interpret the log file entries:

- Single letter—I means Information, E means Error).
- Four digit number (such as 5081)—Source line number (possibly incorrect).

- Four digit number (such as 3040)—Thread ID. You can use this number to identify the work of individual worker threads. You can filter these logs in Excel to make identification easier.
- Worker request (RQ) numbers—The particular request number that the worker thread is processing. A conversation starts with `Start RQnnnn` and is not complete until `Done RQnnnn` by the same thread ID. There may be multiple events handled for the RQ number.
 - A `Start` request without a corresponding `Done` (after a long time), indicates a block.
 - `AllocateThread failed with -1` means that no workers could be scheduled.

EAP Logging

In ACS 4.1, EAP logging now displays messages in hexadecimal numbers (instead of ASCII characters). Use an external interpreter to get the detailed EAP message information.

Database Files

ACS 4.1 uses Sybase as database system. When you must send database files to the TAC, the database files are:

- `<ACS_install_dir>\CSDB\ACS.db`—Database.
- `ACS.log`—The last transactions (not yet committed).

Troubleshooting Using CSUtil.exe (Windows Only)

This section contains the following information:

- [Location and Syntax, page A-8](#)
- [Backing Up and Restoring the ACS Internal Database, page A-9](#)
- [Creating a Dump Text File, page A-10](#)
- [Compacting the User Database, page A-10](#)
- [Exporting User and Group Information, page A-11](#)

Location and Syntax

You can find the **CSUtil.exe** utility at the following location: `<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 following 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 [CSUtil Database Utility, page D-1](#).

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 backup or restore an external script, use **CSUtil.exe**. The command syntax for database backup using **CSUtil.exe** is:

```
C:\Program Files\CiscoSecure ACS v4.1\bin\CSUtil -b filename.
```

[Table A-2](#) describes the commands that support backup and restore:

Table A-2 Backup and Restore Options

Command	Description
-b	Back up system to a named file
-d	Dump user and group information to a text file (default: <i>dump.txt</i>)
-e	Decode error number to ASCII message
-g	Dump only group information to a text file (default: <i>group.txt</i>)
-i	Import user or NAS information (default: <i>import.txt</i>)
-l	Load internal data from a text file (created by the -d option)
-n	Create or initialize the ACS database
-q	Run CSUtil.exe in quiet mode
-r	Restore system from a named file (created by using the -b option)
-u	List users by group (default: <i>users.txt</i>)

For example:

```
C:\Program Files\CiscoSecure ACS v4.1\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 v4.1\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 uninstall 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 load 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 v4.1\bin\System Back
up\CRL Reg.RDF not received, skipping..
Done
```

The loading of a dump file replaces existing data.

Compacting the User Database

When you delete user records from the ACS database, ACS marks the records as deleted but does not remove the records. Therefore, you might want to compact the database to actually remove the deleted records from the database.

To compact a database:

-
- Step 1** Dump the data.
 - Step 2** Create a new database.
 - Step 3** Import all the data that was dumped earlier.
-

To compact a database, enter:

```
CSUtil.exe -q -d -n -1
```

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
```

Troubleshooting Using the CLI (Solution Engine Only)

This section contains the following information:

- [CLI Commands, page A-11](#)
- [Using the Web Interface with the Solution Engine, page A-12](#)

CLI Commands

ACS Solution Engine 4.1 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 A-3](#).

Table A-3 CLI Commands

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

Table A-3 CLI Commands (continued)

CLI Command	Description
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 appliance's hostname.
set ip	Set IP configuration.
set password	Set administrator's password.
set dbpassword	Set database encryption password.
set time	Set timezone, enable NTP synch 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	Shutdown appliance.

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 shutdown 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 following diagnostic logs:
 - 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.

Services that Log and Monitor ACS

The following services log and monitor ACS:

- **CSLog**—A logging service for audit-trailing, accounting of authentication, and authorization packets. **CSLog** collects data from the **CSTacacs** or **CSRADIUS** packet and **CSAuth**, and then scrubs the data so that the data can be stored into comma-separated value (CSV) files or forwarded to an Open DataBase Connectivity (ODBC)-compliant database.
- **CSMon**—Responsible for the monitoring, recording, and notification of ACS performance, including automatic response to some scenarios. For example, if the TACACS+ or the Remote Authentication Dial-In User Service (RADIUS) service stops functioning, ACS by default restarts all the services, unless otherwise configured.

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

- **Generic host system state**—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 log-on attempts, and compares these to predetermined thresholds for indications of atypical 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 dealing 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 cause 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.

Running Services from the Command Line

The main services can be run from the command line by specifying the `-z` option, for example, `csauth -z`. Pressing Return will cause the service to shut down.



Note

You may get a hang with some services at the end of shutdown right at the end. In this case, the process is stuck in a DLL unload (`ccmp.dll`) and you may need use **Control+C** to exit.

Some services offer more than the `-z` option. Use the `-h` flag to get help on available options for that service, for example, `csauth -h`.

Some examples of output from the `-h` option include:

```
Csradius -d -p -z
Cstacacs -e -z
```

Services have some memory mapped files and in general the services use NULL security attributes, which implies the process default. A service has a different default than the logged-in user, so if you run `csauth -z`, you usually find that `csadmin` will fail with a message about initializing IP Pools. In this case, both processes are trying to access the shared memory, but they are running as different effective users. The simplest solution is to run `csadmin -z` whenever you run `csauth -z`, or even not run `csadmin` at all if you do not need it.

Also note that `CSAuth` and `CSAdmin` load the external database DLLs (for example, `NTAuthenDLL`). If you are working with these DLLs, it is necessary to stop both `CSAuth` and `CSAdmin` each time you want to create the new binary in the program files folder.

If you are going to perform Windows authentications, then it is important to run from an account with sufficient permissions, for example, the same account configured for the ACS services. The Local Administrator on a member server might not work.

Common Problems

The following sections describe common problems and their resolutions:

- [Administration, page A-15](#)
- [Authentication and Authorization, page A-18](#)
- [Browser, page A-21](#)
- [Cisco Network Admission Control \(NAC\), page A-23](#)
- [Database, page A-26](#)
- [Dial-In Connections, page A-31](#)
- [EAP Protocols, page A-34](#)
- [GAME Protocol, page A-35](#)
- [Installations and Upgrades, page A-37](#)
- [Interoperability, page A-40](#)
- [Logging, page A-41](#)
- [MAC Authentication Bypass Problems, page A-41](#)
- [Remote Agent \(ACS Solution Engine\), page A-42](#)

- [Reports](#), page A-42
- [User Group Management](#), page A-44

Administration

This section contains the following troubleshooting information:

- [Unauthorized Users Logging In](#), page A-15
- [Restart Services Does Not Work](#), page A-16
- [Event Notification E-Mail Not Received](#), page A-16
- [Remote Administrator Cannot Access Browser](#), page A-16
- [Remote Administrators Cannot Log In](#), page A-17
- [Remote Administrator Receives Logon Failed... Message](#), page A-17
- [Remote Administrator Cannot Access ACS](#), page A-17



Note

For information on using the command line interface (CLI) to execute administrative commands, see the “Administering Cisco Secure ACS Solution Engine” chapter of *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1*.

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 GUI.
 - Option 2—Use:

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

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

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



Tip

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

Unauthorized Users Logging In

Condition

Unauthorized users can log in.

Action

List start and end IP addresses for the **Reject listed IP addresses** option. Choose **Administrator Control > Access Policy**, and 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 **CSAdmin > Stop > Start**.

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. Use the Windows **ping** command to confirm ACS connectivity.

To manually restart services, log in to the ACS console and enter the **restart** command, followed by a single 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

Ensure that the SMTP server name is correct. If the name is correct, ensure that the computer running ACS can ping the SMTP server or can send e-mail via a third-party e-mail software package.

Ensure that the e-mail address does not 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 *Release Notes for Cisco Secure ACS Release 4.1* for a list of supported browsers.
2. Ping ACS to confirm connectivity (ACS for Windows only).
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

List no start or end IP addresses for the **Allow only listed IP addresses to connect** option. Choose **Administrator Control > Access Policy**, and 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**.

If necessary, restart the server.

Action (ACS Solution Engine)

Restart the **CSAdmin** service. To restart the **CSAdmin** service, from the CLI enter the **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 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 the following troubleshooting information:

- [Windows Authentication Problems, page A-18](#)
- [Dial-in Not Disabled, page A-18](#)
- [Settings Not Inherited, page A-18](#)
- [Retry Interval Too Short, page A-19](#)
- [AAA Client Times Out, page A-19](#)
- [Unknown NAS Error, page A-19](#)
- [Key Mismatch Error, page A-19](#)
- [Unexpected Authorizations, page A-20](#)
- [RADIUS Extension DLL Rejected User Error, page A-20](#)
- [Request Does Not Appear in an External Database, page A-20](#)

Windows Authentication Problems

Condition

Problems diagnosing Windows authentications.

Action

Log in to the ACS server (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 Active Directory (AD) configuration issue.

If the login works, but ACS does not authenticate, this condition indicates permission problems. Check Auth.log for the username, and look for errors. Review the permission requirements and ensure 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 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 the following 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 ensure that the NAS is recognized:

-
- Step 1** Verify that the AAA client is configured under the Network Configuration section.
- Step 2** If you have RADIUS/TACACS source-interface command configured on the AAA client, ensure that the client on ACS is configured by using the IP address of the specified interface.
-

Key Mismatch Error

Condition

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

Action

To ensure 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. AV pairs used in one vendor protocol can be ignored by another vendor protocol. Ensure 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. Ensure that, at a minimum, the Network-EAP check box is selected.
- Step 2** If you are using an external user database for authentication, verify that ACS supports the database.
-

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 *auth.log* 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 there are unusual strings in place of the username, then check for configuration error in the TACACS+ client NAS, and correct the configuration of the device.

Browser

This section contains the following troubleshooting information:

- [Cannot Access the Web Interface, page A-21](#)
- [Pages Do Not Appear Properly, page A-21](#)
- [Browser crash when trying to open ACS., page A-22](#)
- [Session Connection Lost, page A-22](#)
- [Administrator Database Corruption \(Netscape\), page A-22](#)
- [Remote Administrator Cannot Browse, page A-22](#)

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 Cisco Secure ACS for Windows Release 4.1* and the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1* for a list of supported browsers, and the *Release Notes for Cisco Secure ACS Release 4.1* 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

Perform the following steps:

-
- Step 1** Check that JRE is installed on the client machine.
-

- Step 2** Check for using the right 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 JRE 1.5.0_00, upgrade to the current version of the JRE at the Java website.

Session Connection Lost

Condition

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

Action

Check the **Session idle timeout** value for remote administrators. Choose **Administration Control Session Policy Setup**, and 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 reauthenticate 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

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

Cisco Network Admission Control (NAC)

This section contains the following troubleshooting information:

- [Posture Problems, page A-23](#)
- [Cisco IOS Commands Not Denied, page A-24](#)
- [EAP Request Has Invalid Signature, page A-24](#)
- [Administrator Locked Out of Client, page A-24](#)
- [Cannot Enter Enable Mode, page A-25](#)
- [Nonresponsive Endpoint Limit Reached, page A-25](#)
- [NAC Posture Problem, page A-26](#)
- [NAC Posture Problem, page A-26](#)

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 “-----” instead of a posture.

Action

If you see “-----”, the AAA client is not receiving the posture-token attribute-value (AV) pair within a Cisco IOS/PIX RADIUS `cisco-av-pair` vendor-specific attribute (VSA). If the posture that appears does not correspond to the actual result of posture validation, the AAA client is receiving an incorrect value in the posture-token AV pair.

Check group mappings for Network Admission Control (NAC) databases to verify that the correct user groups are associated with each system posture token (SPT). In the user groups that are configured for use with NAC, ensure that the Cisco IOS/PIX `cisco-av-pair` VSA is correctly configured. For example, in a group configured to authorize NAC clients receiving a Healthy SPT, be sure the `[009\001]` `cisco-av-pair` check box is checked and that the following string appears in the `[009\001]` `cisco-av-pair` text box:
`posture-token=Healthy`



Caution

The posture-token AV pair is the only way that ACS notifies the AAA client of the SPT that the posture validation returns. Because you manually configure the posture-token AV pair, errors in configuring the posture-token can result in the incorrect SPT being sent to the AAA client; or, if the AV pair name is mistyped, the AAA client 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 [About the cisco-av-pair RADIUS Attribute, page C-5](#).

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 it is not already present, enter the following 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 for the following conditions:

- 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

Perform the following steps:

-
- Step 1** If you have a fallback method configured on your AAA client, disable connectivity to the AAA server and log in using local or line username and password.
 - 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, choose **Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features** and select that option to have the TACACS+ settings appear in the user settings. Then choose **Max privilege for any AAA Client** (this will typically be 15) and enter the **TACACS+ Enable Password** for the user.

Nonresponsive Endpoint Limit Reached

Condition

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

Action

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

When the system reaches the maximum limit of 100 unauthorized nonresponsive endpoints per Network Access Device (NAD), the following message appears on the router console:

```
*Jan 19 09:51:04.855: %AP-4-POSTURE_EXCEED_MAX_INIT: Exceeded maximum limit (100).
```

The router stops processing RADIUS requests for NAC. This mechanism will leave legitimate users, with or without 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 during any of the following situations. The:

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

Based on this behavior, 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 MAC or IP address wildcard with network access restrictions (NARs) in ACS.
- You should never have more than 100 unauthorized endpoints behind a single NAC-enabled router 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 token is automatically sent in the `cisco-av-pair` by the posture result.

Authorization Policy

When configuring an authorization policy and selecting **any** in the user group or the posture token, but the intention is **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).

Database

This section contains the following troubleshooting information:

- [RDBMS Synchronization Not Properly Operating, page A-26](#)
- [Database Replication Not Properly Operating, page A-26](#)
- [External User Database Not Available, page A-27](#)
- [Unknown Users Not Authenticated, page A-27](#)
- [User Problems, page A-27](#)
- [Cannot Implement the RSA Token Server, page A-28](#)
- [ACS Does Not See Incoming Request, page A-28](#)
- [External Databases Not Properly Operating \(ACS Solution Engine\), page A-29](#)
- [Group Mapping \(ACS Solution Engine\), page A-29](#)
- [Configuration of Active Directory \(ACS Solution Engine\), page A-30](#)
- [NTLMv2 Does Not Work, page A-31](#)

RDBMS Synchronization Not Properly Operating

Condition

RDBMS Synchronization is not properly operating.

Action

Ensure that the correct server appears in the Partners list.

Database Replication Not Properly Operating

Condition

Database Replication is not properly operating.

Action

- Ensure that you have correctly set the server as Send or Receive.
- On the sending server, ensure that the receiving server is in the Replication list.

- On the receiving server, ensure that the sending server is selected in the Accept Replication from list. Also, ensure that the sending server is not in the replication partner list.
- Ensure 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. Ensure 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 Password Authentication Protocol (PAP).

To authenticate unknown users:

- Step 1** Choose **External User Databases > Unknown User Policy**.
- Step 2** Select the **Check the following external user databases** option.
- Step 3** From the External Databases list, select the database(s) against which to authenticate unknown users.
- Step 4** Click **—>** (right arrow button) 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

Clean up the database by entering the following command from the command line:

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

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

**Tip**

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

For more information on using the `CSUtil.exe` command, see [Appendix D, “CSUtil Database Utility.”](#)

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 running ACS. (Ensure that your login account has administrative privileges.)
 - Step 2** Ensure 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 `sdconf.rec` in the `%SystemRoot%\system32` directory.
 - Step 6** Ensure that you can **ping** the machine that is running the ACE server by hostname. (You might need to add the machine in the `lmhosts` file.)
 - Step 7** Verify that support for RSA is enabled in **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, install the token server.
-

ACS Does Not See Incoming Request

Condition

On the ACE 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, ensure that you are using PAP and not MS-CHAP or 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

Make sure that a two-way trust (for dial-in check) is established between the ACS domain and the other domains. Check CSAuth.log 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 the following message in a pop up 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 Microsoft.com.
- NetBIOS over TCP is not enabled.
- DNS is not correctly working. You can try reregistering by using **ipconfig /flushdns** and then **ipconfig /registerdns** from a DOS prompt. Otherwise, go to Microsoft.com for more information.
- RPC is not correctly working (for example, after Blaster Update). Go to Microsoft.com to find the following MS hot fixes:
 - kb822831
 - kb823980
 - kb824105
 - kb824146
- The domain controllers are not synchronized. To synchronize, use the following 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 (ACS Solution Engine)



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 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 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 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 then the **Browse** button.
 - 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.

Dial-In Connections

This section contains the following troubleshooting information:

- [Cannot Connect to AAA Client \(No Report\)](#), page A-31
- [Cannot Connect to the AAA Client \(Windows External Database\)](#), page A-32
- [Cannot Connect to AAA Client \(ACS Internal Database\)](#), page A-33
- [Cannot Connect to AAA Client \(Telnet Connection Authenticated\)](#), page A-33
- [Cannot Connect to AAA Client \(Telnet Connection Not Authenticated\)](#), page A-34
- [Callback Not Working](#), page A-34
- [Authentication Fails When Using PAP](#), page A-34

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, choose **Reports and Activity**, then choose **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 a AAA client/modem configuration, not ACS.
- LAN connections for the AAA client and the computer running ACS are physically connected.
- IP address of the AAA client in the ACS configuration is correct.
- IP address of ACS in AAA client configuration is correct.
- TACACS+ or RADIUS 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.

A record of a failed attempt appears 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 that the user information 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 have Account Disabled chosen.
- User Properties for the dial-in window does not have Grant dial-in permission to user disabled, 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 configuration is selected in the Password Authentication list on the User Setup page for the user.

- 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/PPP, IPX/PPP or Exec/Telnet). Click **Submit + Restart** if you make a change.
- The user expiration information in the Windows user database has not caused a failed authentication. For troubleshooting purposes, disable password expiry for the user in the Windows user database.

Then:

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

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

From within ACS confirm that the:

- Username is entered into ACS.
- ACS internal database is selected from the Password Authentication list and a password has been entered in User Setup for the user.
- ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Click **Submit + Restart** if you made a change.
- Expiration information has not caused 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

The problem can be isolated to one of three areas:

- Line or modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured.
- The user is not assigned to a group that has the correct authorization rights. 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

Ensure 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, go to the Interface Configuration section and check the **Per-User Advanced TACACS+ Features** check box. Then, choose the **TACACS+ Outbound Password** section of the **Advanced TACACS+ Settings** table on the **User Setup** page, then 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 AUTH.log. |
| Step 2 | Enable DEBUG logging on the NAD and examine 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. |
-

GAME Protocol

This section contains the following troubleshooting information:

- [GAME Configuration Problem, page A-35](#)
- [GAME Troubleshooting Setup, page A-36](#)
- [Expected Device-Type is Not Matched, page A-36](#)
- [Device-type Attribute is Not Returned by the Audit Server, page A-36](#)
- [Failure Returned by the Audit Server, page A-37](#)

GAME Configuration Problem

Condition

The GAME configuration is incorrect.

Action

Use the following checklist to check the configuration:

- Choose **Network Access Profiles > Protocols** to be sure that you have checked **Allow Agentless Request Processing**.
- Choose **Network Access Profiles > Posture Validation > Select Audit** to ensure that you checked an Audit Server to set up the appropriate device-type rules.
- Choose **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 added to 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 the following policies and groups:

- Ensure that the host to audit is configured or that Audit All Hosts is selected.
- Select Audit All Groups.
- Configure the following unique groups:
 - Configure a group for Assign this Group if Audit Server Do not Return a Device Type.
 - Configure a Match-all rule and assign a group for all device-type strings returned by the audit server.
 - Choose **Network Access Profiles > Authentication** and configure a group for If Agentless Request was not Assigned.

Configure the following logging:

- 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 the following configuration items:

- Configure the Game Troubleshooting Setup. See [GAME Troubleshooting Setup, page A-36](#).
- 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 debug 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.

Auth.log indicates 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 the following configuration items and logging:

- Configure the GAME Troubleshooting setup. See [GAME Troubleshooting Setup, page A-36](#).
- Audit Device-Type column is . . . (empty) in Pass Authen Report.
- After audit, the Group configured for Assign this Group if AuditServer Do not Return a Device is assigned.
- Check for a device type for a known device.

Failure Returned by the Audit Server

Condition

The audit server returns a failure.

AUTH.log indicates Audit Server return zero length device type or 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 the following configuration items:

- GAME Troubleshooting setup. See [GAME Troubleshooting Setup, page A-36](#).
- 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 audit.
- Audit Server is accessible and functional (that is, posture audit works with the same server).

Installations and Upgrades

This section contains the following troubleshooting information:

- [rad_mon.dll and tac_mon.dll In Use Condition, page A-38](#)
- [During Upgrade the ACS Folder is Locked, page A-38](#)
- [During Uninstall the ACS Folder is Locked, page A-38](#)
- [After Restart ACS Cannot Start Services, page A-38](#)
- [Upgrade or Uninstall Cannot Complete, page A-39](#)
- [Invalid File or Data, page A-39](#)
- [Accounting Logs Missing, page A-39](#)
- [Upgrade Command Does Not Work \(ACS Solution Engine\), page A-40](#)
- [On Solaris, autorun.sh Does Not Execute \(ACS Solution Engine\), page A-40](#)

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 .dlls, such as **AgentSrv.exe**. You can use third-party tools to find the processes that are using the .dlls.

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

Remove excess log files. ACS stores log files in \CiscoSecure ACS v.4.1\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**. In the Services Log File Configuration, check **Manage Directory**, and choose **Keep only the last <n> files**. Set <n> to 3.

If PNLogAgent is running, stop that service to release any locks that it might have on the folder.

During Uninstall the ACS Folder is Locked

Condition

When uninstalling, the ACS folder is locked.

Action

Check for the following conditions:

- A **CSUtil.exe** process from an aborted restore is still in a created but not started state. Solution: Restart.
- Another application such as **Notepad** has an file open. Solution: Close the application.
- An explorer has a subfolder of ACS install open. Solution: 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 the following 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 the on the service and select Properties.
 - Step 3** Change the Startup Type to Disabled.
-

Upgrade or Uninstall Cannot Complete

Condition

Upgrade or uninstall cannot complete.

Action

Close:

- Step 1** All ACS files.
 - Step 2** All log files, for example, *auth.log*.
 - Step 3** All programs,
 - Step 4** Programs such as Radtest, and close any binaries that are running.
 - Step 5** MMC tools like Performance Monitor.
-

Invalid File or Data

Condition

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

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 using a Solaris distribution server, **autorun.sh** cannot be executed.

Action

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

Interoperability

This section contains the following troubleshooting information:

- [Interoperation Between Builds, page A-40](#)
- [Proxy Requests Fail, page A-40](#)

Interoperation Between Builds

Condition

Interoperation between different builds of ACS does not work.

Action

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

Proxy Requests Fail

Condition

Proxy requests to another server fail.

Action

Ensure 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. Choose **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 (**CS Tacacs**, **CS Radius**, or **CS Auth**) are down.
- The secret key is misconfigured.
- Inbound or Outbound messaging is misconfigured.

Logging

This section describes troubleshooting procedures for log files.

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 rerunning uninstall, 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.4.1\Logs. If a log file folder becomes too large, and you cannot upgrade, you must first delete all but a small number of files from the folder (for example 3). When ACS starts up, choose **System Configuration > Service Control**. In the Services Log File Configuration, check Manage Directory, and choose Keep only the last <n> files. Set <n> to a small number (for example, 3).

MAC Authentication Bypass Problems

This section contains the following information:

- [The MAC Address Exists in LDAP but Always Maps to the Default User Group, page A-41](#)
- [The MAC Exists in the Internal Database but is Mapped to the Wrong User Group, page A-42](#)
- [Request is Rejected, page A-42](#)

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

- Check the LDAP configuration.
- Check the LDAP Group Mapping settings.
- Verify that the MAC address format stored in the LDAP server is one of the supported formats.

- 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

- Ensure 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)

The following sections describe 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 the following information:

- [Blank Reports, page A-42](#)
- [Unknown User Information Missing, page A-43](#)
- [Two Entries Logged for One User Session, page A-43](#)
- [Old Format Dates Persist, page A-43](#)
- [Logging Halted, page A-43](#)
- [Logged in Users Report Works Only with Certain Devices, page A-44](#)

Blank Reports

Condition

A report is blank.

Action

Ensure that you have selected **Log to <reportname> Report** under **System Configuration > Logging > Log Target <reportname>**. You must also set **Network Configuration <servername> Access Server Type** to **ACS for Windows NT**.

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

Make sure that the remote logging function is not configured to send accounting packets to the same location as the Send Accounting Information fields in the Proxy Distribution Table.

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 made, you must restart the **CSAdmin** services and log on again.

Logging Halted

Condition

Effect of logging unavailability on 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 little 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 the following troubleshooting information:

- [MaxSessions Not Working Over VPDN, page A-44](#)
- [MaxSessions Fluctuates, page A-45](#)
- [MaxSessions Does Not Take Effect, page A-45](#)
- [TACACS+ and RADIUS ATTRIBUTES Missing, page A-45](#)

MaxSessions Not Working Over VPDN

Condition

MaxSessions over 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

Ensure 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

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

**Note**

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

Error Codes

Table A-4 provides an alphabetized list of the ACS error codes.

Table A-4 ACS 4.1 Error Codes

A valid EAP-FAST master key does not exist; make sure EAP-FAST replication is operational
Access denied because no profile matched
Access denied to Voice-over-IP group
Access denied: fast-reconnect was successful, but user was not found in cache
Access rejected due to authorization policy in the network access profiles
ACS account disabled
ACS ARAP password invalid
ACS CHAP password invalid
ACS login time restriction
ACS MSCHAP password is invalid
ACS password invalid
ACS UNIX password invalid
ACS User Account Expired
ACS User exceeded max sessions
ACS user unknown
ACS user's password has expired
Audit Server returned an error
Authentication protocol is not allowed for this network access profile
Authentication session invalidated
Authentication type not supported by External DB
Badly formed Downloadable ACL request from device
Cached token rejected/expired
Certificate name or binary comparison failed
CLI user unknown
Could not access password aging state in ACS internal DB
Could not check password aging state in ACS internal DB
Could not communicate with external policy server - authentication failure
Could not communicate with external policy server - wrong HCAP version
Could not communicate with the Audit Server
Could not connect to external policy server - timeout error
Could not open a connection to external policy server
Could not open a connection to external policy server - Could not validate server certificate
DB object lock not granted
EAP type not configured
EAP-FAST anonymous in-band provisioning is disabled
EAP-FAST authenticated in-band provisioning is not disabled
EAP-FAST user ID does not match to initiators ID presented inside the PAC

Table A-4 ACS 4.1 Error Codes (continued)

EAP-FAST user was provisioned with a new PAC
EAP-FAST users PAC is invalid
EAP-TLS or PEAP authentication failed during SSL handshake
Enabling Tacacs+ is not allowed for this Access Server
Error assigning RADIUS Authorization Components to a user
Error communicating with the audit server, or invalid response was returned
Error parsing Audit Server Response
External DB account disabled
External DB account expired
External DB account locked out
External DB account restriction
External DB ARAP password is invalid
External DB CHAP password is invalid
External DB did not return MPPE key material
External DB EAP authentication failed
External DB is not configured
External DB is not configured
External DB is not configured for this network access profile
External DB is not operational
External DB MSCHAP password is invalid
External DB password expired
External DB password invalid
External DB reports about an error condition
External DB user invalid or bad password
External DB user unknown
External user not found
Failed to allocate IP address for a user
Internal error
Internal error assigning RADIUS Authorization Components attributes
Internal error during Downloadable ACL exchange
Internal error while assigning Downloadable ACL to a user
Invalid characters in username
Invalid MAC Address format=dword:00000066
Invalid message authenticator in EAP request
Invalid Protocol Data
Key Mismatch
MAC auth bypass is not allowed
MAC-Authentication-Bypass group is disabled
Machine authentication is not permitted
Missing message authenticator in EAP request
Number of audit round trips has exceeded limit
PEAP or EAP-FAST password change against Windows DB is disabled

Table A-4 ACS 4.1 Error Codes (continued)

Posture Validation failed because no profile matched
Posture Validation Failure (general)
Posture Validation Failure on External Policy
Posture Validation Failure on Internal Policy
Tacacs+ enable password invalid
Tacacs+ enable privilege too low
Token PIN changed
Unknown attributes were detected in the posture validation request
User requires a Tacacs+ Enable Password
User requires Tacacs+ outbound password
Users Access Filtered
Users of this group are disabled
Users Radius request rejected (by Radius extension DLL)
Users Usage Quota has been exhausted
Windows dialin permission required
Windows domain controller not found
Windows External DB user access was denied due to a Machine Access Restriction
Windows login server unavailable
Windows login time restriction
Windows login type not granted
Windows password change failed
Windows user must change password
Windows workstation not allowed