



CHAPTER 1

Troubleshooting Procedures and Tools

Revised: November 13, 2009, 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 1-13](#)
- [Command Line Utilities, page 1-18](#)

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 cannot 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 2-25](#). 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 1-18](#). 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 1-14](#).

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 Authentications 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 2-4](#).

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 cannot determine whether the problem is on a device or on ACS, see [Additional Testing for User Authentication, page 1-4](#).
- If you cannot 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 v4.1\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

Always run **Radtest** and **Tactest** off line. In the **Radtest** and **Tactest** examples, the username is **abcde**.

Testing RADIUS with Radtest.exe

Starting from the command line:

```
>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 CA 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:

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

- When did the problem occur?
- What were the network conditions?
- Have there been any recent changes on the network?
- Is additional software running on the ACS server? Cisco does not recommend running additional software on the ACS server.

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.

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 causes ACS to collect all debugging information.

**Note**

The Full logging level can cause 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.
-

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 v4.1\bin\cssupport.exe. The default location for the package.cab file is \<ACS_install_dir>\Utils\Support. See [Examples of Logs, page 1-15](#).

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:

-
- Step 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.
 - Step 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.
 - Step 3** Download the file from your FTP server.
 - Step 4** Use [Examples of Logs](#), page 1-15.
 - Step 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>.cab` (for example, `Pack_ACS-SUS-A2_10-Sep-2006_15-50-48.cab`). 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, `Auth.log` 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 1-13](#).
- **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**—`package.cab` 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`

Follow this general procedure for analyzing `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 Auth.log; also, check for errors or hangs.
- Step 5** Correlate the two timestamps.
- 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 Active Directory and LDAP.
-

Examples of Analyzing Package.cab

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 authentications 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	Caller-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 **CSRradius**. You examine RDS.log and discover that the authentication message was delivered to the **CSAuth** service.
- Step 3** You examine Auth.log, 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 Auth.log 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 Auth.log 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 4.1 uses Sybase as 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 | Run the Command prompt. |
| Step 4 | Change directory to <ACS_install_dir>\bin. |
| Step 5 | Run <code>CSUpdate -upgrade <patch-filename></code> . |
| 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 1-13](#)
- [Services that Generate Log Files, page 1-14](#)
- [Services that Log and Monitor ACS, page 1-14](#)
- [Service Log Files on the Remote Agent, page 1-15](#)
- [Examples of Logs, page 1-15](#)

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 comma-separated value (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 Cisco Secure Access Control Server Troubleshooting Guide.

- **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 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 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 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.

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 Auth.log 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 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)
```

To interpret the log file entries:

- **Single letter**—**I** means Information, **E** means Error). You can use the command **CSUtil.exe -e** to get a description of the error.
- **Four digit number (such as 5081)**—Source line number (for internal reference only).
- **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. Multiple events might be handled by the RQ number.
 - A **Start** request without a corresponding **Done** (after a long time), indicates a block.
 - **AllocateThread** failed with **-1** means that the system is using the maximum worker threads. Ensure that your external databases are not causing excessive delays.

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.



Note

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

Detailed logging of the EAP process in **Auth.log** 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 1-18](#)
- [The Remote Agent CLI \(Solution Engine Only\), page 1-21](#)

CSUtil.exe (Windows Only)

ACS provides the **CSUtil.exe** utility, which you can use for troubleshooting as well as 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 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 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.
-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 v4.1\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.

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 4.1 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 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.
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 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.

Table 1-5 CLI Commands (continued)

CLI Command	Description
reboot	Soft reboot appliance.
restart	Restart ACS services.
shutdown	Shutdown appliance.

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 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:
 - 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.

