



Logs and Reports

The Cisco Secure Access Control Server Release 4.0 Solution Engine, hereafter referred to as ACS, produces a variety of logs, and provides a way to view most of these logs in the ACS web interface as HTML reports.

This chapter contains the following topics:

- [Logging Format, page 11-1](#)
- [Special Logging Attributes, page 11-2](#)
- [Posture-Validation Attributes in Logs, page 11-3](#)
- [Update Packets in Accounting Logs, page 11-3](#)
- [About ACS Logs and Reports, page 11-4](#)
- [Working with CSV Logs, page 11-9](#)
- [Remote Logging, page 11-13](#)
- [Service Logs, page 11-19](#)

Logging Format

ACS logs a variety of user and system activities. Logs can be recorded in comma-separated value (CSV) files. The CSV format records data in columns separated by commas(.). This format is easily imported into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After data from a CSV file is imported into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, please see the documentation from the third-party vendor. You can access the CSV files on the ACS server hard drive or by downloading the CSV file from the web interface. For more information about downloading the CSV file from the web interface, see [Viewing a CSV Report, page 11-10](#).

For information about the formats that are available for a specific log, see [About ACS Logs and Reports, page 11-4](#).

Special Logging Attributes

Among the many attributes that ACS can record in its logs, a few are of special importance. The following list explains the special logging attributes that ACS provides.

- **User Attributes**—These logging attributes appear in the Attributes list for any log configuration page. ACS lists them by using their default names: Real Name, Description, User Field 3, User Field 4, and User Field 5. If you change the name of a user-defined attribute, the default name rather, than the new name, still appears in the Attributes list.

The values that you enter in the corresponding fields in the user account determine the content of these attributes. For more information about user attributes, see [User Data Configuration Options, page 3-4](#).

- **ExtDB Info**—If the user is authenticated with an external user database, this attribute contains a value that the database returns. In the case of a Windows user database, this attribute contains the name of the domain that authenticated the user.

In entries in the Failed Attempts log, this attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user-authentication attempt.

- **Access Device**—The name of the AAA client that is sending the logging data to ACS.
- **Network Device Group**—The network device group to which the access device (AAA client) belongs.
- **Filter Information**—The result of network access restrictions (NARs) applied to the user, if any. The message in this field indicates whether all applicable NARs permitted the user access, all applicable NARs denied the user access, or more specific information about which NAR denied the user access. If no NARs apply to the user, this logging attribute notes that no NARs were applied.

The Filter Information attribute is available for Passed Authentication and Failed Attempts logs.

- **Device Command Set**—The name of the device command set, if any, that was used to satisfy a command authorization request.

The Device Command Set attribute is available for Failed Attempts logs.

- **Remote Logging Result**—Whether a remote logging service successfully processes a forwarded accounting packet. This attribute is useful for determining which accounting packets, if any, a central logging service did not log. It is dependent upon the receipt of an acknowledgment message from the remote logging service. The acknowledgment message indicates that the remote logging service properly processed the accounting packet in the manner that the remote logging service is configured to do. A value of `Remote-logging-successful` indicates that the remote logging service successfully processed the accounting packet. A value of `Remote-logging-failed` indicates that the remote logging service did not process the accounting packet successfully.



Note

ACS cannot determine how a remote logging service is configured to process accounting packets that it is forwarded. For example, if a remote logging service is configured to discard accounting packets, it discards a forwarded accounting packet and responds to ACS with an acknowledgment message, causing ACS to write a value of `Remote-logging-successful` in the Remote Logging Result attribute in the local log that records the account packet.

- **Application-Posture-Token**—The application posture token (APT) returned by a particular policy during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs. For more information, see [Posture-Validation Attributes in Logs, page 11-3](#).

- **System-Posture-Token**—The system posture token (SPT) that is returned during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs. For more information, see [Posture-Validation Attributes in Logs, page 11-3](#).
- **Other Posture-Validation Attributes**—Attributes that a NAC client sends to ACS during a posture-validation request. The attributes are uniquely identified by the vendor name, application name, and attribute name. For example, the NAI:AV:DAT-Date attribute is an attribute containing information about the date of the DAT file on the NAC client for the anti-virus application by Network Associates, Inc. These attributes are available only in the Passed Authentications and Failed Attempts logs. For more information, see [Posture-Validation Attributes in Logs, page 11-3](#).

Posture-Validation Attributes in Logs

You can choose to log posture-validation attributes in the Passed Authentications and Failed Attempts logs. All inbound attributes are available for logging. The only two outbound attributes that you can record in logs are `Application-Posture-Assessment` and `System-Posture-Assessment`.

All posture-validation requests resulting in a system posture assessment/token (SPT) are logged in the Passed Authentications log. Posture-validation requests resulting in an SPT of anything other than `Healthy` are logged in the Failed Attempts log. For more information about posture tokens, see [Posture Tokens, page 14-3](#).

Reporting HCAP Errors

The `Authen-Failure-Code` entry in the *Failed-Attempts* report may display one of the following errors when Host Credentials Authentication Protocol (HCAP) fails:

- `Version failure - Could not communicate with external policy server - wrong HCAP version`
- `Connection failure - Could not open a connection to external policy server`
- `Authentication failure - Could not communicate with external policy server - authentication failure`
- `Timeout error - Could not connect to external policy server - timeout error`
- `Other - Posture Validation Failure on External Policy`

Update Packets in Accounting Logs

Whenever you configure ACS to record accounting data for user sessions, ACS records start and stop packets. If you want, you can configure ACS to record update packets, too. In addition to providing interim accounting information during a user session, update packets drive password-expiry messages via ACS Authentication Agent. In this use, the update packets are called watchdog packets.

**Note**

To record update packets in ACS accounting logs, you must configure your AAA clients to send the update packets. For more information about configuring your AAA client to send update packets, refer to the documentation for your AAA clients.

- **Logging Update Packets Locally**—To log update packets according to the local ACS logging configuration, enable the Log Update/Watchdog Packets from this Access Server option for each AAA client in Network Configuration.

For more information on setting this option for a AAA client, see [Adding AAA Clients, page 4-11](#).

- **Logging Update Packets Remotely**—To log update packets on a remote logging server, enable the Log Update/Watchdog Packets from this remote AAA Server option for the remote server AAA Server table entry on the local ACS.

For more information on setting this option for a AAA server, see [Adding AAA Servers, page 4-16](#).

About ACS Logs and Reports

ACS provides logs that can be divided into four types:

- Accounting logs
- Dynamic ACS administration reports
- ACS system logs
- Service logs

This section contains information about the items from the previous list. For information about service logs, see [Service Logs, page 11-19](#).

This section contains the following topics:

- [Accounting Logs, page 11-4](#)
- [Dynamic Administration Reports, page 11-6](#)
- [ACS System Logs, page 11-8](#)



Note

All reports open instantly when selected, except for the Logged-In Users report, which might take up to 20 seconds to open. Specific user information might take up to several minutes to appear.

Accounting Logs

Accounting logs contain information about the use of remote access services by users. By default, these logs are available in CSV format, with the exception of the Passed Authentications log. [Table 11-1](#) describes all accounting logs.

In the web interface, all accounting logs can be enabled, configured, and viewed. [Table 11-2](#) contains information about what you can do with the accounting logs.

Table 11-1 Accounting Log Descriptions

Log	Description
TACACS+ Accounting	Contains: <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification (CLID) • Session duration
TACACS+ Administration	Lists configuration commands entered on a AAA client by using TACACS+ (Cisco IOS). Particularly if you use ACS to perform command authorization, we recommend that you use this log. Note To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with ACS.
RADIUS Accounting	Contains: <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification information • Session duration You can configure ACS to include accounting for Voice-over-IP (VoIP) in the RADIUS Accounting log, in a separate VoIP accounting log, or in both places.
VoIP Accounting	Contains: <ul style="list-style-type: none"> • VoIP session stop and start times • AAA client messages with username • CLID information • VoIP session duration You can configure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places.
Failed Attempts	Lists authentication and authorization failures with an indication of the cause. For posture-validation requests, this log records the results of any posture validation that returns a posture token other than <code>Healthy</code> . Note In entries in the Failed Attempts log, the <code>ExtDB Info</code> attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user-authentication attempt.
Passed Authentications	Lists successful authentication requests. This log is not dependent upon accounting packets from your AAA clients, so it is available; even if your AAA clients do not support RADIUS accounting or if you have disabled accounting on your AAA clients. For posture-validation requests, this log records the results of all posture-validation requests resulting in an SPT.

Table 11-2 What You Can Do with Accounting Logs

What You Can Do	Description and Related Topics
Enable an accounting log	You can enable the log in CSV format. For instructions on how to enable an accounting log in CSV format, see Enabling or Disabling a CSV Log, page 11-10 . For information on Remote Logging, see Remote Logging, page 11-13 .
View an accounting report	For instructions on viewing an accounting report in the web interface, see Viewing a CSV Report, page 11-10 . For information on Remote Logging, see Remote Logging, page 11-13 .
Configure an accounting log	For instructions on configuring the CSV accounting log, see Configuring a CSV Log, page 11-12 .

Dynamic Administration Reports

These reports show the status of user accounts when you access them in the ACS web interface. They are available only in the web interface, are always enabled, and require no configuration.

[Table 11-3](#) contains descriptions of all dynamic administration reports and information about what you can do regarding dynamic administration reports.

Table 11-3 Dynamic Administration Report Descriptions and Related Topics

Report	Description and Related Topics
Logged-In Users	<p>Lists all users receiving services for a single AAA client or all AAA clients. Users accessing the network with Cisco Aironet equipment appear on the list for the access point that they are currently associated with, provided that the firmware image on the Cisco Aironet Access Point supports sending the RADIUS Service-Type attribute for rekey authentications.</p> <p>On a computer configured to perform machine authentication, machine authentication occurs when the computer starts. When a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section. Once user authentication begins, the computer no longer appears on the Logged-In Users List. For more information about machine authentication, see EAP and Windows Authentication, page 13-10.</p> <p>Note To use the logged-in user list feature, you must configure AAA clients to perform authentication and accounting by using the same protocol—TACACS+ or RADIUS.</p> <p>For instructions on viewing the Logged-in User report in the web interface, see Viewing the Logged-in Users Report, page 11-7.</p> <p>For instructions about deleting logged-in users from specific AAA clients or from all AAA clients, see Deleting Logged-in Users, page 11-7.</p>
Disabled Accounts	<p>Lists all user accounts that are disabled and the reason they were disabled.</p> <p>For instructions on viewing the Disabled Accounts report in the web interface, see Viewing the Disabled Accounts Report, page 11-8.</p>
Appliance Status Page	Lists information about resource utilization on the ACS Solution Engine. Also displays information about the IP configuration for the ACS Solution Engine and the MAC address of its network interface card. You cannot configure this log.

Viewing the Logged-in Users Report

To view the Logged-in Users report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users who are logged in through the AAA client. At the bottom of the table, the **All AAA Clients** entry shows the total number of users who are logged in.



Tip You can sort the table by any column's entries, in ascending or descending order. Click a column title once to sort the table by the entries in that column in ascending order. Click the column a second time to sort the table by the entries in that column in descending order.

Step 3 Do one of the following:

- To see a list of all users who are logged in, click **All AAA Clients**.
- To see a list of users who are logged in through a particular AAA client, click the name of the AAA client.

ACS displays a table of users who are logged in, including:

- Date and Time
- User
- Group
- Assigned IP
- Port
- Source AAA Client



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

Deleting Logged-in Users

From a Logged-in Users Report, you can instruct ACS to delete users who are logged into a specific AAA client. When a user session terminates without a AAA client sending an accounting stop packet to ACS, the Logged-in Users Report continues to show the user. Deleting logged-in users from a AAA client ends the accounting for those user sessions.



Note Deleting logged-in users only ends the ACS accounting record of users who are logged in to a particular AAA client. It does not terminate active user sessions, nor does it affect user records.

To delete logged-in users:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users who are logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users who are logged in.

Step 3 Click the name of the AAA client whose users you want to delete from the Logged-in Users report.

ACS displays a table of all users who are logged in through the AAA client. The Purge Logged in Users button appears below the table.

Step 4 Click **Purge Logged in Users**.

ACS displays a message, indicating the number of users who are purged from the report and the IP address of the AAA client.

Viewing the Disabled Accounts Report

To view the Disabled Accounts report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Disabled Accounts**.

The Select a user account to edit page displays disabled user accounts, the account status, and the group to which the user account is assigned.

Step 3 To edit a user account listed, in the User column, click the username.

ACS opens the user account for editing.

For more information about editing a user account, see [Basic User Setup Options, page 7-2](#).

ACS System Logs

System logs are logs about the ACS system and therefore record system-related events. These logs are useful for troubleshooting or audits. They are always enabled and are only available in CSV format. For information about each system log, including which system logs are configurable, see [Table 11-4](#).

For instructions on viewing a CSV report in the web interface, see [Viewing a CSV Report, page 11-10](#).

Table 11-4 System Log Descriptions

Log	Description
ACS Backup and Restore	Lists ACS backup and restore activity. You cannot configure this log.
RDBMS Synchronization	Lists RDBMS Synchronization activity. You cannot configure this log.
Database Replication	Lists database replication activity. You cannot configure this log.

Table 11-4 System Log Descriptions

Log	Description
Administration Audit	Lists actions taken by each system administrator, such as adding users, editing groups, configuring a AAA client, or viewing reports.
User Password Changes	Lists user password changes that users initiate, regardless of which password-change mechanism was used to change the password. Thus, this log contains records of password changes accomplished by the ACS Authentication Agent, by the User Changeable Password web interface, or by Telnet session on a network device using TACACS+. It does not list password changes that an administrator makes in the ACS web interface. For information about configuring the User Password-Changes log, see Configuring Local Password Management, page 8-5 .
ACS Service Monitoring	Lists when ACS services start and stop. For information about configuring the ACS Service Monitoring log, see ACS Active Service Management, page 8-13 .
Appliance Administration Audit	Lists administrator activity on the serial console, including logins, logouts, and commands executed. You cannot configure this log.

Working with CSV Logs

This section contains the following topics:

- [CSV Log File Names, page 11-9](#)
- [CSV Log Size and Retention, page 11-10](#)
- [Enabling or Disabling a CSV Log, page 11-10](#)
- [Viewing a CSV Report, page 11-10](#)
- [Log Filtering, page 11-11](#)
- [Configuring a CSV Log, page 11-12](#)

CSV Log File Names

When you access a report in Reports and Activity, ACS lists the CSV files in chronological order, with the current CSV file at the top of the list. The current file is named *log.csv*, where *log* is the name of the log.

Older files are named as:

logyyyy-mm-dd.csv

where

log is the name of the log.

yyyy is the year that the CSV file was started.

mm is the month that the CSV file was started, in numeric characters.

dd is the date that the CSV file was started.

For example, a Database Replication log file that was generated on October 13, 2002, would be named *Database Replication 2002-10-13.csv*.

CSV Log Size and Retention

For each CSV log, ACS writes a separate log file. When a log file reaches 10 MB in size, ACS starts a new log file. ACS retains the seven most recent log files for each CSV log.

Enabling or Disabling a CSV Log

This procedure describes how to enable or disable a CSV log. For instructions about configuring the content of a CSV log, see [Configuring a CSV Log, page 11-12](#).



Note

Some CSV logs are always enabled. For information about specific logs, including whether you can disable them, see [About ACS Logs and Reports, page 11-4](#).

To enable or disable a CSV log:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**.
 - Step 3** Click the name of the CSV log that you want to enable.
The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log that you selected.
 - Step 4** To enable the log, under Enable Logging, check the **Log to CSV log report** check box, where *log* is the name of the CSV log that you selected in Step 3.
 - Step 5** To disable the log, under Enable Logging, clear the **Log to CSV report log** check box, where *log* is the name of the CSV log that you selected in Step 3.
 - Step 6** Click **Submit**.

If you enabled the log, ACS begins logging information for the log that you selected. If you disabled the log, ACS stops logging information for the log that you selected.

Viewing a CSV Report

When you select Logged-in Users or Disabled Accounts, a list of logged-in users or disabled accounts appears in the display area, which is the pane on the right side of the web browser. For all other types of reports, a list of applicable reports appears. Files appear in chronological order, with the most recent file at the top of the list. The reports are named and listed by the date on which they were created; for example, a report ending with *2002-10-13.csv* was created on October 13, 2002.

Files in CSV format can be imported into spreadsheets by using most popular spreadsheet application software. Refer to your spreadsheet software documentation for instructions. You can also use a third-party reporting tool to manage report data. For example, *aaa-reports!* by Extraxi supports ACS.

You can download the CSV file for any CSV report that you view in ACS.

To view a CSV report:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click the name of the CSV report that you want to view.
- On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV report files.
- Step 3** Click the CSV report filename whose contents you want to view.
- If the CSV report file contains information, the information appears in the display area.



Tip

You can sort the table by entries in the column, in ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.



Tip

To check for newer information in the current CSV report, click **Refresh**.

- Step 4** If you want to download the CSV log file for the report that you are viewing:
- Click **Download**.
- Your browser displays a dialog box for accepting and saving the CSV file.
- Choose a location where you want to save the CSV file, and click **Save** to save the file.

Log Filtering

You can use ACS to filter CSV log reports. When you select a report type from the available reports types list, a report history (log) files list of the selected report type appears. After you select a specific CSV log file, and its contents appear, you can specify the filtering criteria. The filtering criteria is applied on the original log file, and only rows that match the criteria appear.

Filtering criteria includes a regular expression, a time range, or both.

Regular expression-based filtering checks that at least one of each column's value, per row, matches the provided regular expression. When you use regular expression filtering, ACS traverses each column and displays only the rows that match the filtering criteria.

You can use time-based filtering by specifying values for a Start Date & Time and an End Date & Time. Rows dated within the specified time range appear.

You can enter a regular expression for filtering, a time-based filter, or a combination of both. When you enter a regular expression and use time-based filtering as well, the report will include only the rows that match both criteria.



Note

The functionality of the **Refresh** and **Download** links remain unchanged (without filtering). See [Viewing a CSV Report, page 11-10](#).

To apply a log filter:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click the name of the CSV report type that you want to view.
On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV (log) report files.
- Step 3** Select a log file. The contents appear.
You can then specify filtering criteria and apply the filter to the log file's content.
- Step 4** In the **Regular Expression** text box enter a string value. The expression can be up to 100 characters long.
- Step 5** In the **Start Date & Time** and **End Date & Time** text boxes, enter string values. The date and time format is *dd/mm/yyyy, hh:mm:ss* or *mm/dd/yyyy, hh:mm:ss* as defined in the ACS system configuration for the date format.
- Step 6** In the **Rows per Page** box choose the number of rows to display per page. (The default is 50.)
- Step 7** Click **Apply Filter**. The ACS web server will apply the specified filtering criteria to the report file and display the filtered results in the report's table.
Click **Clear Filter** to reset filtering parameters to their default values. Use this option to display the entire report unfiltered.
- Step 8** Use the **Next** and **Previous** buttons to navigate forward and backward through the report pages.
-

Configuring a CSV Log

This procedure describes how to configure the content of a CSV log. For instructions on enabling or disabling a CSV log, see [Enabling or Disabling a CSV Log, page 11-10](#).

The logs to which this procedure applies are:

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Failed Attempts
- Passed Authentications

You can configure the log content of a CSV log. To configure CSV log content:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Logging**.
- Step 3** Click the name of the CSV log that you want to enable.
The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log that you selected.
The Select Columns To Log table contains two lists, Attributes and Logged Attributes. The attributes in the Logged Attributes list appear on the log that you selected.

Step 4 To add an attribute to the log, select the attribute in the Attributes list, and then click --> (right arrow button).

The attribute moves to the Logged Attributes list.



Tip Use the vertical scroll bar to find attributes that are not visible in the list box.

Step 5 To remove an attribute from the log, select the attribute in the Logged Attributes list, and then click <-- (left arrow button).

The attribute moves to the Attributes list.



Tip Use the vertical scroll bar to find attributes that are not visible in the list.

Step 6 To set the attributes in the Logged Attributes list back to the default selections, at the bottom of the browser window, click **Reset Columns**.

Step 7 Click **Submit**.

ACS implements the CSV log configuration that you specified.

Remote Logging

This section discusses remote logging capabilities of ACS Solution Engine.

This section contains the following topics:

- [About Remote Logging, page 11-13](#)
- [Implementing Centralized Remote Logging, page 11-14](#)
- [Local Configuration of Remote Logging, page 11-14](#)
- [Remote Agent Logging Configuration, page 11-17](#)

About Remote Logging

The Remote Logging feature enables ACS to send accounting data received from AAA clients to an ACS Remote Agent. The remote agent runs on a computer on your network. It writes the accounting data that ACS sends to it into CSV files. You can configure many ACS Solution Engines to point to a single remote agent, thus making the computer that runs the remote agent a central logging server. For more information about installing and configuring an ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents 4.0*.



Note

The Remote Logging feature does not affect the forwarding of accounting data for proxied authentication requests. ACS only applies Remote Logging settings to accounting data for sessions authenticated by proxy when accounting data for sessions authenticated by proxy is logged locally. For more information about proxied authentication requests and accounting data for sessions authenticated by proxy, see [Proxy Distribution Table Configuration, page 4-27](#).

The Remote Logging Setup page, available from the Logging Configuration page in the System Configuration section, is where you configure ACS to perform remote logging of accounting data. You can specify that account data is sent to a single remote agent or that it is sent to many remote agents. For more information about enabling remote logging, see [Local Configuration of Remote Logging, page 11-14](#).

Regardless of how many ACSes send their accounting data to the central logging server, the remote agent receives its configuration from a single ACS Solution Engine. That ACS is the configuration provider for the remote agent. In the HTML interface of the configuration provider ACS, you determine the remote agent configuration. By using the links under Remote Agent Logging Configuration on the Logging Configuration page, you determine:

- what logs the remote agent keeps
- what data is recorded for each log kept
- how the remote agent manages the log files

For more information about configuring remote agent logging, see [Remote Agent Logging Configuration, page 11-17](#).

Implementing Centralized Remote Logging

To implement centralized remote logging:

-
- Step 1** Install and configure an ACS Remote Agent on a computer that you want to use to store centralized logging data. For more information about installing and configuring an ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agent*.
 - Step 2** On each ACS Solution Engine, add the remote agent. For more information, see [Remote Agent Configuration, page 4-19](#).
 - Step 3** On each ACS Solution Engine, enable remote logging. For more information, see [Local Configuration of Remote Logging, page 11-14](#).
 - Step 4** On the ACS Solution Engine that the remote agent is configured to use as its configuration provider, configure remote agent logging. For more information, see [Remote Agent Logging Configuration, page 11-17](#).
 - Step 5** If you want to create another central logging server, for use as a secondary server or as a mirror server, perform Step 1 through Step 4 for the additional server.
-

Local Configuration of Remote Logging

Local configuration of remote logging entails enabling the ACS Solution Engine to send accounting data to remote agents and specifying to which remote agents the accounting data is to be sent.

Local configuration of remote logging is performed on the Remote Logging Setup page, accessed by the Remote Logging link, which is under Local Logging Configuration on the Logging Configuration page.

**Note**

Local configuration of remote logging does not affect the types of logs sent to remote agents or the configuration of the data included in logs sent to remote agents. For information about configuring which logs are sent to remote agents and the data the logs contain, see [Remote Agent Logging Configuration, page 11-17](#).

Remote Logging Options

ACS provides the following remote logging options, which appear on the Remote Logging Setup page:

- **Do not log Remotely**—When selected, this option limits ACS to writing accounting data for locally authenticated sessions only to the local logs that are enabled.
- **Log to all selected remote log services**—When selected, this option enables ACS to send accounting data for locally authenticated sessions to all remote agents in the Selected Log Services list.
- **Log to subsequent remote log services on failure**—When selected, this option enables ACS to send accounting data for locally authenticated sessions to the first remote agent in the Selected Log Services list that is available to provide logging services. You use this option to configure one or more backup central logging servers so that no accounting data is lost if the first central logging server fails or is otherwise unavailable to ACS.
- **Remote Log Services**—The remote agents configured in the Remote Agents table in Network Configuration to which ACS *does not* send accounting data for locally authenticated sessions.
- **Selected Log Services**—The remote agents configured in the Remote Agents table in Network Configuration to which ACS *does* send accounting data for locally authenticated sessions.

Enabling and Configuring Remote Logging

Before You Begin

Be certain that you have configured your central logging server. For more information, see [Implementing Centralized Remote Logging, page 11-14](#).

To enable and configure remote logging:

-
- Step 1** To enable remote logging:
- a. Click **Interface Configuration**.
 - b. Click **Advanced Options**.
 - c. Check the **Remote Logging** check box.
 - d. Click **Submit**.
- ACS displays the Remote Logging link on the Logging page in the System Configuration section.
- Step 2** Click **System Configuration**.
- Step 3** Click **Logging**.
- The Logging Configuration page appears.
- Step 4** Under Local Logging Configuration, click **Remote Logging**.

- Step 5** Select the applicable remote logging option:
- To send the accounting information for this ACS to more than one remote agent, select the **Log to all selected remote log services** option.
 - To send the accounting information for this ACS to a single remote agent, select the **Log to subsequent remote log services on failure** option.



Note Click the Log to subsequent remote log services on failure option when you want to configure ACS to send accounting data to a second remote agent if the first remote fails.

- Step 6** For each remote agent that you want the Selected Log Services list to display:
- In the Remote Log Services list, select the name of a remote agent to which you want to send accounting data for locally authenticated sessions.



Note The remote agents that appear in the Remote Log Services list are determined by the Remote Agents table in Network Configuration. For more information about the Remote Agents table, see [Remote Agent Configuration, page 4-19](#).

- Click --> (right arrow button) to move the selected remote agent to the Selected Log Services list.

- Step 7** To assign an order to the remote agents in the Selected Log Services list, click **Up** and **Down** to move selected remote agents until you have created the order you need.



Note If you click the Log to subsequent remote log services on failure option, ACS logs to the first accessible remote agent in the Selected Log Services list.

- Step 8** Click **Submit**.

ACS saves and implements the remote logging configuration that you specified.

Disabling Remote Logging

You can prevent ACS from sending its accounting information to remote agents by disabling the Remote Logging feature.

To disable remote logging:

- In the navigation bar, click **System Configuration**.
- Click **Logging**.
- Under Local Logging Configuration, click **Remote Logging**.
- Select the **Do not log Remotely** option.
- Click **Submit**.

ACS no longer sends its accounting information for locally authenticated sessions to remote agents.

Remote Agent Logging Configuration

Remote agent logging configuration entails enabling logs that you want a remote agent to keep and configuring which logging attributes are sent to remote agents. On the Logging Configuration page, the Remote Agent Logging Configuration table lists the CSV logs that you can configure ACS to send to a remote agent. You can configure each log separately.

For information about configuring which remote agents ACS sends log data to, see [Local Configuration of Remote Logging, page 11-14](#).

Remote Agent Logging Options

For each log that a remote agent can keep, you have the following configuration options:

- **Log to *log name* report**—Defines whether the remote log is enabled.
- **Attributes**—The available attributes whose data is *not* sent to the remote agent for logging.
- **Logged Attributes**—The attributes whose data *is* sent to the remote agent for logging.
- **Generate New File**—The frequency with which the remote agent starts a new CSV file for the log.

The options are:

- **Every day**—The remote agent starts a new CSV log file at 12 A.M. every day.
- **Every week**—The remote agent starts a new CSV log file at 12:00 A.M. every Sunday.
- **Every month**—The remote agent starts a new CSV log file at 12:00 A.M. on the first day of every month.
- **When size is greater than *X KB***—The remote agent starts a new CSV log file when the current log file grows to the number of kilobytes specified in the box.
- **Directory**—The directory where the remote agent writes the CSV log file. The directory must be specified by its full path on the server that runs the remote agent. If the server uses Microsoft Windows, the path must begin with the drive letter, such as *c:\acs-logs*. If the server uses Sun Solaris, the path must begin at the root directory, such as */usr/data/acs-logs*.
- **Manage Directory**—Defines whether the remote agent deletes older log files. Using the following options, you can specify how the remote agent determines which log files to delete:
 - **Keep only the last *X files***—The remote agent retains the most recent log files, up to the number of files specified. When the number of files specified is exceeded, the remote agent deletes the oldest files.
 - **Delete files older than *X days***—The remote agent deletes log files that are older than the number of days specified. When a log file grows older than the number of days specified, the remote agent deletes it.

Configuring Remote Agent Logs




This procedure describes how to configure the content of a remote agent CSV log. For instructions about enabling or disabling all remote agent logging, see [Local Configuration of Remote Logging, page 11-14](#).

This procedure applies to all logs recorded by a remote agent, that is, all logs listed in the Remote Agent Logging Configuration table on the Logging Configuration page.

Before You Begin

For information about the options available for remote agent log configuration, see [Remote Agent Logging Options, page 11-17](#).

To configure a CSV log for a remote agent:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Logging**.
- Step 3** Under Remote Agent Logging Configuration, click the name of the remote agent log that you want to configure.
- The CSV *log* File Configuration page appears, where *log* is the name of the remote agent log that you selected.
- Step 4** To enable the log, check the **Log to CSV *log* name report** check box.
-  **Note** If the Log to CSV *log* name report check box is not checked, ACS does not send data for this log to remote agents.
-
- Step 5** For each attribute that you want to include in the remote agent log, select the attribute in the Attributes list and click --> (right arrow button).
- The attribute moves to the Logged Attributes list.
-  **Tip** Use the vertical scroll bar to find attributes not visible in the list box.
-
- Step 6** If you need to remove an attribute from the remote agent log, select the attribute in the Logged Attributes list and click <-- (left arrow button).
- The attribute moves to the Attributes list.
-  **Tip** Use the vertical scroll bar to find attributes that are not visible in the list.
-
- Step 7** If you want to set the attributes in the Logged Attributes list back to the default selections, at the bottom of the browser window, click **Reset Columns**.
- Step 8** Under **Generate New File**, specify when the remote agent should begin a new log file.
- Step 9** If you want to manage which CSV files the remote agent keeps:
- Check the **Manage Directory** check box.
 - To limit the number of CSV files ACS retains, click the **Keep only the last X files** option and type the number of files that you want ACS to retain in the X box.
 - To limit the age of CSV files retained by ACS, select the **Delete files older than X days** option and type the number of days for which ACS should retain a CSV file before deleting it.
- Step 10** Click **Submit**.
- ACS implements the remote agent log configuration that you specified.
-

Service Logs

Service logs are considered diagnostic logs which you use for troubleshooting or debugging purposes only. These logs are not intended for general use by ACS administrators; instead, they are mainly sources of information for Cisco support personnel. Service logs contain a record of all ACS service actions and activities. When service logging is enabled, each service generates a log whenever the service is running, regardless of whether you are using the service. For example, RADIUS service logs are created even if you are not using the RADIUS protocol in your network.

This section covers:

- [Services Logged, page 11-19](#)
- [Configuring Service Logs, page 11-19](#)
- [Helping Customer Support Gather Data, page 11-20](#)

For more information about ACS services, see [Chapter 1, “Overview.”](#)

Services Logged

ACS generates logs for the following services:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRADIUS
- CSTacacs

The most recent debug log is named:

SERVICE.log

where *SERVICE* is the name of the applicable service.

Older debug logs are named with the year, month, and date on which they were created. For example, a file that was created on July 13, 1999, would be named:

SERVICE 1999-07-13.log

where *SERVICE* is the name of the applicable service.

If you selected the Day/Month/Year format, the file would be named:

SERVICE 13-07-1999.log

Configuring Service Logs

You can configure how ACS generates and manages the service log file. You can configure the following options for Level of Detail in the service log file:

- **None**—No log file is generated.
- **Low**—Only start and stop actions are logged. This is the default setting.

- **Full**—All services actions are logged.

To configure how ACS generates and manages the service log file:

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

Step 2 Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the computer that is running ACS.

Step 3 To disable the service log file, under Level of Detail, select the **None** option.

After you click **Restart**, ACS does not generate a new service log file.

Step 4 Click **Restart**.

ACS restarts its services and implements the service log settings that you specified.

Helping Customer Support Gather Data

So that customer support will have enough data to research potential issues, you must set your services log configuration correctly. Choose **System Configuration > Service Control**, and then choose **Full**. Ensure that you have sufficient disk space to handle your log entries.

The Support feature in the System Configuration section includes service logs in the *package.cab* file that it generates if you click Run Support Now. For information about this feature, see [Support Page, page 8-19](#).



Note

When creating a *package.cab* file that is larger than 2GB, additional *.cab* files are created due to the size limit of the packer. The sequence is: the first package name is *package.cab*, the second is *package1.cab*, and so on, until the N package, *packageN.cab*, where N is the number of packages minus one. The files are saved in the same location that is specified before the packing begins. These files are not standalone and all of them must be sent to package. Problems with the packed file (*package.cab*) may arise if there is not enough hard-disk space.
