



Logs and Reports

Cisco Secure ACS for Windows Server produces a variety of logs and provides a way to view most of these logs in the Cisco Secure ACS HTML interface as HTML reports.

This chapter contains the following topics:

- [Logging Formats, page 11-2](#)
- [Special Logging Attributes, page 11-2](#)
- [NAC Attributes in Logs, page 11-4](#)
- [Update Packets in Accounting Logs, page 11-5](#)
- [About Cisco Secure ACS Logs and Reports, page 11-6](#)
- [Working with CSV Logs, page 11-15](#)
- [Working with ODBC Logs, page 11-21](#)
- [Remote Logging, page 11-26](#)
- [Service Logs, page 11-31](#)

Logging Formats

Cisco Secure ACS logs a variety of user and system activities. Depending on the log, and how you have configured Cisco Secure ACS, logs can be recorded in one of two formats:

- **Comma-separated value (CSV) files**—The CSV format records data in columns separated by commas. This format is easily imported into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After data from a CSV file is imported into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, please see the documentation supplied by the third-party vendor. You can access the CSV files either on the Cisco Secure ACS server hard drive or by downloading the CSV file from the HTML interface. For more information about downloading the CSV file from the HTML interface, see [Viewing a CSV Report, page 11-18](#).
- **ODBC-compliant database tables**—ODBC logging enables you to configure Cisco Secure ACS to log directly in an ODBC-compliant relational database, where it is stored in tables, one table per log. After the data is exported to the relational database, you can use the data however you need. For more information about querying the data in your relational database, refer to the documentation supplied by the relational database vendor.

For information about the formats available for a specific log, see [About Cisco Secure ACS Logs and Reports, page 11-6](#).

Special Logging Attributes

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

- **User Attributes**—These logging attributes appear in the Attributes list for any log configuration page. Cisco Secure ACS lists them 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 content of these attributes is determined by the values entered in the corresponding fields in the user account. For more information about user attributes, see [User Data Configuration Options, page 3-3](#).

- **ExtDB Info**—If the user is authenticated with an external user database, this attribute contains a value returned by the database. 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 sending the logging data to Cisco Secure 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 forwarded accounting packet is successfully processed by a remote logging service. This attribute is useful for determining which accounting packets, if any, may not have been logged by a central logging service. 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**

Cisco Secure 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 Cisco Secure ACS with an acknowledgment message, causing Cisco Secure 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 [NAC Attributes in Logs, page 11-4](#).
- **System-Posture-Token**—The system posture token (SPT) returned by a Network Admission Control (NAC) database during a posture validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs. For more information, see [NAC Attributes in Logs, page 11-4](#).
- **Other posture validation attributes**—Attributes sent to Cisco Secure ACS by a NAC client in a posture validation request, identified by the vendor name, application name, and attribute name that uniquely identify the attribute. 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 a Network Associates, Inc., anti-virus application. These attributes are available only in the Passed Authentications and Failed Attempts logs. For more information, see [NAC Attributes in Logs, page 11-4](#).

NAC Attributes in Logs

Posture validation attributes, used by NAC, can be used 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-Token and System-Posture-Token.

Posture validation requests resulting in an system posture token (SPT) of Healthy 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 14-4](#).

Update Packets in Accounting Logs

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



Note

To record update packets in Cisco Secure 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 local Cisco Secure 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 a AAA Client, page 4-16](#).

- **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 Cisco Secure ACS.

For more information on setting this option for a AAA server, see [Adding a AAA Server, page 4-24](#).

About Cisco Secure ACS Logs and Reports

The logs that Cisco Secure ACS provides can be divided into four types:

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

This section contains information about the first three types of logs. For information about service logs, see [Service Logs, page 11-31](#).

This section contains the following topics:

- [Accounting Logs, page 11-6](#)
- [Dynamic Administration Reports, page 11-9](#)
- [Cisco Secure ACS System Logs, page 11-13](#)

Accounting Logs

Accounting logs contain information about the use of remote access services by users. By default, these logs are available in CSV format. With the exception of the Passed Authentications log, you can also configure Cisco Secure ACS to export the data for these logs to an ODBC-compliant relational database that you configure to store the log data. [Table 11-1](#) describes all accounting logs.

In the HTML interface, all accounting logs can be enabled, configured, and viewed. [Table 11-2](#) contains information about what you can do in the Cisco Secure ACS HTML interface regarding accounting logs.

Table 11-1 Accounting Log Descriptions

Log	Description
TACACS+ Accounting	<p>Contains the following information:</p> <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification (CLID) information • Session duration
TACACS+ Administration	<p>Lists configuration commands entered on a AAA client using TACACS+ (Cisco IOS). Particularly if you use Cisco Secure ACS to perform command authorization, we recommend that you use this log.</p> <p>Note To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with Cisco Secure ACS.</p>
RADIUS Accounting	<p>Contains the following information:</p> <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification information • Session duration <p>You can configure Cisco Secure ACS to include accounting for Voice-over-IP (VoIP) in the RADIUS Accounting log, in a separate VoIP accounting log, or in both places.</p>
VoIP Accounting	<p>Contains the following information:</p> <ul style="list-style-type: none"> • VoIP session stop and start times • AAA client messages with username • CLID information • VoIP session duration <p>You can configure Cisco Secure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places.</p>

Table 11-1 Accounting Log Descriptions (continued)

Log	Description
Failed Attempts	<p>Lists authentication and authorization failures with an indication of the cause. For posture validation requests, this log records the results of any posture validation that returns a posture token other than Healthy.</p> <p>Note In entries in the Failed Attempts log, the ExtDB Info attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user authentication attempt.</p>
Passed Authentications	<p>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 any posture validation that returns a posture token of Healthy.</p> <p>Note The Passed Authentications log cannot be configured using an ODBC format.</p>

Table 11-2 What You Can Do with Accounting Logs

What You Can Do	Description and Related Topics
Enable an accounting log	<p>You can enable the log in either CSV or ODBC format.</p> <ul style="list-style-type: none"> • CSV—For instructions on how to enable an accounting log in CSV format, see Enabling or Disabling a CSV Log, page 11-17. • ODBC—For instructions on how to enable an account log in ODBC format, see Configuring an ODBC Log, page 11-23.

Table 11-2 *What You Can Do with Accounting Logs (continued)*

What You Can Do	Description and Related Topics
View an accounting report	For instructions on viewing an accounting report in the HTML interface, see Viewing a CSV Report, page 11-18 .
Configure an accounting log	<p>The steps for configuring an accounting log vary depending upon which format you want to use. For more information about log formats, see Logging Formats, page 11-2.</p> <ul style="list-style-type: none"> • CSV—For instructions on configuring the CSV accounting log, see Configuring a CSV Log, page 11-19. • ODBC—For instructions on configuring ODBC accounting log, see Configuring an ODBC Log, page 11-23.

Dynamic Administration Reports

These reports show the status of user accounts at the moment you access them in the Cisco Secure ACS HTML interface. They are available only in the HTML 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 data-bbox="354 310 1220 464">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 data-bbox="354 483 1231 699">On a computer configured to perform machine authentication, machine authentication occurs when the computer started. 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 13-15.</p> <p data-bbox="354 719 1231 808">Note To use the logged-in user list feature, you must configure AAA clients to perform authentication and accounting using the same protocol—either TACACS+ or RADIUS.</p> <p data-bbox="354 841 1231 898">For instructions on viewing the Logged-in User report in the HTML interface, see Viewing the Logged-in Users Report, page 11-10.</p> <p data-bbox="354 917 1213 974">For instructions about deleting logged-in users from specific AAA clients or from all AAA clients, see Deleting Logged-in Users, page 11-11.</p>
Disabled Accounts	<p data-bbox="354 995 1186 1019">Lists all user accounts that are disabled and the reason they were disabled.</p> <p data-bbox="354 1039 1153 1096">For instructions on viewing the Disabled Accounts report in the HTML interface, see Viewing the Disabled Accounts Report, page 11-12.</p>

Viewing the Logged-in Users Report

To view the Logged-in Users report, follow these steps:

-
- 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 logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users logged in.

**Tip**

You can sort the table by any column's entries, in either 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 logged in, click **All AAA Clients**.
- To see a list of users logged in through a particular AAA client, click the name of the AAA client.

Cisco Secure ACS displays a table of users logged in, including the following information:

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

**Tip**

You can sort the table by the entries in any column, in either 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 Cisco Secure ACS to delete users logged into a specific AAA client. When a user session terminates without a AAA client sending an accounting stop packet to Cisco Secure 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 Cisco Secure ACS accounting record of users 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, follow these steps:

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 logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users logged in.

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

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

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

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

Viewing the Disabled Accounts Report

To view the Disabled Accounts report, follow these steps:

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.

Cisco Secure ACS opens the user account for editing.

For more information about editing a user account, see [Basic User Setup Options, page 7-3](#).

Cisco Secure ACS System Logs

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

For instructions on viewing a CSV report in the HTML interface, see [Viewing a CSV Report, page 11-18](#).

Table 11-4 Accounting Log Descriptions and Related Topics

Log	Description and Related Topics
ACS Backup and Restore	Lists Cisco Secure ACS backup and restore activity. This log cannot be configured.
RDBMS Synchronization	Lists RDBMS Synchronization activity. This log cannot be configured.
Database Replication	Lists database replication activity. This log cannot be configured.
Administration Audit	Lists actions taken by each system administrator, such as adding users, editing groups, configuring a AAA client, or viewing reports. For instructions on configuring the Administration Audit log, see Configuring the Administration Audit Log, page 11-14 .

Table 11-4 Accounting Log Descriptions and Related Topics (continued)

Log	Description and Related Topics
User Password Changes	<p>Lists user password changes initiated by users, regardless of which password change mechanism was used to change the password. Thus, this log contains records of password changes accomplished by the CiscoSecure Authentication Agent, by the User Changeable Password HTML interface, or by Telnet session on a network device using TACACS+. It does not list password changes made by an administrator in the Cisco Secure ACS HTML interface.</p> <p>For information about configuring the User Password Changes log, see Configuring Local Password Management, page 8-7.</p>
ACS Service Monitoring	<p>Lists when Cisco Secure ACS services start and stop.</p> <p>For information about configuring the ACS Service Monitoring log, see Cisco Secure ACS Active Service Management, page 8-17.</p>

Configuring the Administration Audit Log

You use this procedure to configure how often, or at what size limit, Cisco Secure ACS generates a new Administration Audit Log file. You can also use this procedure to configure the Administration Audit Log file storage limits with regard to number or age.

To configure the Administrative Audit log, follow these steps:

-
- Step 1** In the navigation bar, click **Administration Control**.
- Step 2** Click **Audit Policy**.
The Audit Policy Setup page appears.
- Step 3** To generate a new Administrative Audit CSV file at a regular interval, select one of the following options:
- **Every day**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each day.
 - **Every week**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each week.
 - **Every month**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each month.

- Step 4** To generate a new Administrative Audit CSV file when the current file reaches a specific size, select the **When size is greater than X KB** option and type the file size threshold in kilobytes in the *X* box.
- Step 5** To manage which Administrative Audit CSV files Cisco Secure ACS keeps, follow these steps:
- Select the **Manage Directory** check box.
 - To limit the number of Administrative Audit CSV files Cisco Secure ACS retains, select the **Keep only the last X files** option and type in the *X* box the number of files you want Cisco Secure ACS to retain.
 - To limit how old Administrative Audit CSV files retained by Cisco Secure ACS can be, select the **Delete files older than X days** option and type the number of days for which Cisco Secure ACS should retain a Administrative Audit CSV file before deleting it.
- Step 6** Click **Submit**.
- Cisco Secure ACS saves and implements the Administrative Audit log settings you specified.
-

Working with CSV Logs

This section contains the following topics:

- [CSV Log File Names, page 11-15](#)
- [CSV Log File Locations, page 11-16](#)
- [Enabling or Disabling a CSV Log, page 11-17](#)
- [Viewing a CSV Report, page 11-18](#)
- [Configuring a CSV Log, page 11-19](#)

CSV Log File Names

When you access a report in Reports and Activity, Cisco Secure 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 in the following format:

logyyyy-mm-dd.csv

where

log is the name of the log.

yyyy is the year the CSV file was started.

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

dd is the date the CSV file was started.

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

CSV Log File Locations

By default, Cisco Secure ACS keeps log files in directories unique to the log. The HTML interface enables you to configure the log file location for some logs while the location for other log files is not configurable. The default directories for all logs are within *sysdrive*:\Program Files\CiscoSecure ACS v.x.x. For the subdirectory of this location for a specific log, see [Table 11-5](#).

Table 11-5 Default CSV Log File Locations

Log	Default Location	Configurable?
TACACS+ Accounting	Logs\TACACS+Accounting	Yes
CSV TACACS+ Administration	Logs\TACACS+Administration	Yes
CSV RADIUS Accounting	Logs\RADIUS Accounting	Yes
CSV VoIP Accounting	Logs\VoIP Accounting	Yes
CSV Failed Attempts	Logs\Failed Attempts	Yes
Passed Authentications	Logs\Passed Authentications	Yes
Cisco Secure ACS Backup and Restore	Logs\Backup and Restore	No
RDBMS Synchronization	Logs\DbSync	No
RDBMS Synchronization	Logs\DBReplicate	No
Administration Audit	Logs\AdminAudit	No

Table 11-5 Default CSV Log File Locations (continued)

Log	Default Location	Configurable?
User Password Changes	CSAuth\PasswordLogs	No
Cisco Secure ACS Active Service Monitoring	Logs\ServiceMonitoring	No

Enabling or Disabling a CSV Log

This procedure describes how to enable or disable a CSV log. For instructions about configuring the content of a CSV log, see [Configuring a CSV Log](#), page 11-19.



Note

Some CSV logs are always enabled. For information about specific logs, including whether you can disable them, see [About Cisco Secure ACS Logs and Reports](#), page 11-6.

To enable or disable a CSV log, follow these steps:

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

If you enabled the log, Cisco Secure ACS begins logging information for the log selected. If you disabled the log, Cisco Secure ACS stops logging information for the log 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 frame on the right side of the web browser. For all other types of reports, a list of applicable reports appears. Files are listed 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 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 Cisco Secure ACS (<http://www.extraxi.com>).

You can download the CSV file for any CSV report you view in Cisco Secure ACS. The procedure below includes steps for doing so.

To view a CSV report, follow these steps:

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

Step 2 Click the name of the CSV report you want to view.

On the right side of the browser, Cisco Secure ACS lists the current CSV report filename and the filenames of any old CSV report files.



Tip You can configure how Cisco Secure ACS handles old CSV report files. For more information, see [Configuring a CSV Log, page 11-19](#).

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 any entries in the column, in either 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 the entries in that column in descending order.



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

Step 4 If you want to download the CSV log file for the report you are viewing, follow these steps:

a. Click **Download**.

Your browser displays a dialog box for accepting and saving the CSV file.

b. Choose a location to save the CSV file and save the file.

Configuring a CSV Log

This procedure describes how to configure the content of a CSV log. For instructions to enable or disable a CSV log, see [Enabling or Disabling a CSV Log, page 11-17](#).

The logs to which this procedure applies are as follows:

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



Note

The ACS Backup and Restore, RDBMS Synchronization, and Database Replication CSV logs cannot be configured.

You can configure several aspects of a CSV log:

- **Log content**—You can select which data attributes are included in the log.
- **Log generation frequency**—You can determine whether a new log is started after a specific length of time or when the current CSV file reaches a particular size.

- **CSV file location**—You can specify where on the local hard drive Cisco Secure ACS writes the CSV file.
- **CSV file retention**—You can specify how many old CSV files Cisco Secure ACS maintains or set a maximum number of files it is to retain.

To configure a CSV log, follow these steps:

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

Step 2 Click **Logging**.

Step 3 Click the name of the CSV log you want to enable.

The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log 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 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 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 not visible in the list.

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

- Step 7** To generate a new CSV file at a regular interval, select one of the following options:
- **Every day**—Cisco Secure ACS generates a new CSV file at the start of each day.
 - **Every week**—Cisco Secure ACS generates a new CSV file at the start of each week.
 - **Every month**—Cisco Secure ACS generates a new CSV file at the start of each month.
- Step 8** To generate a new CSV file when the current file reaches a specific size, select the **When size is greater than X KB** option and type the file size threshold, in kilobytes, in the *X* box.
- Step 9** To manage which CSV files Cisco Secure ACS keeps, follow these steps:
- a. Select the **Manage Directory** check box.
 - b. To limit the number of CSV files Cisco Secure ACS retains, select the **Keep only the last X files** option and type the number of files you want Cisco Secure ACS to retain in the *X* box.
 - c. To limit how old CSV files retained by Cisco Secure ACS can be, select the **Delete files older than X days** option and type the number of days for which Cisco Secure ACS should retain a CSV file before deleting it.
- Step 10** Click **Submit**.
- Cisco Secure ACS implements the CSV log configuration that you specified.
-

Working with ODBC Logs

This section contains the following topics:

- [Preparing for ODBC Logging, page 11-22](#)
- [Configuring a System Data Source Name for ODBC Logging, page 11-22](#)
- [Configuring an ODBC Log, page 11-23](#)

Preparing for ODBC Logging

To prepare for ODBC logging, there are several steps you must complete. After you have prepared for ODBC logging, you can configure individual ODBC logs.

To prepare for ODBC logging, follow these steps:

-
- Step 1** Set up the relational database to which you want to export logging data. For more information, refer to your relational database documentation.
 - Step 2** Set up a system data source name (DSN) on the computer running Cisco Secure ACS. For instructions, see [Configuring a System Data Source Name for an ODBC External User Database](#), page 13-70.
 - Step 3** Enable ODBC logging in the Cisco Secure ACS HTML interface:
 - a. In the navigation bar, click **Interface Configuration**.
 - b. Click **Advanced Options**.
 - c. Select the **ODBC Logging** check box.
 - d. Click **Submit**.

Cisco Secure ACS enables the ODBC logging feature. On the Logging page, in the System Configuration section, Cisco Secure ACS displays links for configuring ODBC logs.

You can now configure individual ODBC logs. For instructions, see [Configuring an ODBC Log](#), page 11-23.

Configuring a System Data Source Name for ODBC Logging

On the computer running Cisco Secure ACS, you must create a system DSN for Cisco Secure ACS to communicate with the relational database that is to store your logging data.

To create a system DSN for use with ODBC logging, follow these steps:

-
- Step 1** In Windows Control Panel, double-click **ODBC Data Sources**.
 - Step 2** In the ODBC Data Source Administrator page, click the **System DSN** tab.

- Step 3** Click **Add**.
- Step 4** Select the driver you need to use with your new DSN, and then click **Finish**.
A dialog box displays fields requiring information specific to the ODBC driver you selected.
- Step 5** Type a descriptive name for the DSN in the Data Source Name box.
- Step 6** Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant relational database runs.
- Step 7** Click **OK**.
- Step 8** Close the ODBC window and Windows Control Panel.
The System DSN to be used by Cisco Secure ACS for communicating with the relational database is created on the computer running Cisco Secure ACS. The name you assigned to the DSN appears in the Data Source list on each ODBC log configuration page.
-

Configuring an ODBC Log

The logs to which this procedure applies are as follows:

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



Note

Before you can configure an ODBC log, you must prepare for ODBC logging. For more information, see [Preparing for ODBC Logging, page 11-22](#).

To configure an ODBC log, follow these steps:

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

Step 2 Click **Logging**.

Step 3 Click the name of the ODBC log you want to enable.

The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.

The Select Columns To Log table contains two lists: Attributes and Logged Attributes. When you first access the ODBC configuration page for a log, the Logged Attributes list contains the default set of attributes. Cisco Secure ACS includes in the log only those attributes that are in the Logged Attributes list.

Step 4 Specify the attributes that you want Cisco Secure ACS to send to the relational database:

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

The attribute moves to the Logged Attributes list.



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

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

The attribute moves to the Attributes list.



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

- c. To set the attributes in the Logged Attributes list back to the default selections, click **Reset Columns**.

Step 5 In the ODBC Connection Settings table, configure Cisco Secure ACS to communicate with the ODBC database. To do so, follow these steps:

- a. From the Data Source list, select the system DSN you created to allow Cisco Secure ACS to send ODBC logging data to your relational database.
- b. In the Username box, type the username of a user account in your relational database (up to 80 characters).



Note The user must have sufficient privileges in the relational database to write the ODBC logging data to the appropriate table.

- c. In the Password box, type the password (up to 80 characters) for the relational database user account you specified in Step b.
- d. In the Table Name box, type the name (up to 80 characters) of the table to which you want ODBC logging data appended.

Step 6 Click **Submit**.

Cisco Secure ACS saves the log configuration.

Step 7 Click the name of the ODBC log you are configuring.

Cisco Secure ACS displays the ODBC log configuration page again.

Step 8 Click **Show Create Table**.

The right side of the browser displays an SQL create table statement for Microsoft SQL Server. The table name is the name specified in the Table Name box. The column names are the attributes specified in the Logged Attributes list.



Note The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.

Step 9 Using the information provided in the generated SQL, create a table in your relational database for this ODBC log.



Note For ODBC logging to work, the table name and the column names must match exactly the names in the generated SQL.

Step 10 Continuing in Cisco Secure ACS, access the configuration page for the ODBC log you are configuring:

- a. In the navigation bar, click **System Configuration**.
- b. Click **Logging**.

- c. Click the name of the ODBC log you are configuring.

The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.

Step 11 Select the **Log to ODBC *log* report** check box, where *log* is the name of the ODBC log you selected.

Step 12 Click **Submit**.

Cisco Secure ACS begins sending logging data to the relational database table specified, using the system DSN you configured.

Remote Logging

This section discusses remote logging capabilities of Cisco Secure ACS.

This section contains the following topics:

- [About Remote Logging, page 11-26](#)
- [Implementing Centralized Remote Logging, page 11-27](#)
- [Remote Logging Options, page 11-28](#)
- [Enabling and Configuring Remote Logging, page 11-29](#)
- [Disabling Remote Logging, page 11-31](#)

About Remote Logging

The Remote Logging feature enables you to centralize accounting logs generated by multiple Cisco Secure ACSes. You can configure each Cisco Secure ACS to point to one Cisco Secure ACS that is to be used as a central logging server. The central logging Cisco Secure ACS still performs AAA functions, but it also is the repository for accounting logs it receives. For more information about Cisco Secure ACS accounting logs, see [Accounting Logs, page 11-6](#).

The Remote Logging feature enables Cisco Secure ACS to send accounting data received from AAA clients directly to the CSLog service on the remote logging server, where the accounting data is written to the logs. The logging server

generates the accounting logs in the formats it is configured to use—CSV and ODBC—regardless of the local logging configuration on the Cisco Secure ACSes sending the data to the central logging server.

Cisco Secure ACS listens on TCP port 2001 for remote logging communication. Remote logging data is encrypted by a 128-bit proprietary algorithm.

**Note**

The Remote Logging feature does not affect the forwarding of accounting data for proxied authentication requests. Cisco Secure 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 4-34](#).

Implementing Centralized Remote Logging

Before You Begin

Make sure that gateway devices between remote Cisco Secure ACSes and the central logging Cisco Secure ACS permit the central logging Cisco Secure ACS to receive data on TCP port 2001.

To implement centralized remote logging, follow these steps:

-
- Step 1** On a computer that you want to use to store centralized logging data, install Cisco Secure ACS for Windows Server. For information about installing Cisco Secure ACS, see the *Installation Guide for Cisco Secure ACS for Windows Server*.
- Step 2** In the Cisco Secure ACS running on the central logging server, follow these steps:
- Configure the accounting logs as needed. All accounting data sent to the central logging server will be recorded in the way you configure accounting logs on this Cisco Secure ACS. For information about accounting logs, see [Accounting Logs, page 11-6](#).

Accounting logs can be recorded in either CSV or ODBC format. For information about configuring CSV logs, see [Working with CSV Logs, page 11-15](#). For information about configuring ODBC logs, see [Configuring an ODBC Log, page 11-23](#).

- b. Add to the AAA Servers table each Cisco Secure ACS that the central logging server is to receive accounting data from. For more information, see [AAA Server Configuration, page 4-21](#).

**Note**

If the central logging server is to log watchdog and update packets for a Cisco Secure ACS, be sure that the Log Update/Watchdog Packets from this remote AAA Server check box is selected for that Cisco Secure ACS in the AAA Servers table.

- Step 3** For each Cisco Secure ACS that is to send its accounting data to the central logging server, follow these steps:
- a. Add the central logging server to the AAA Servers table in Network Configuration. For more information, see [AAA Server Configuration, page 4-21](#).
 - b. Enable remote logging. For more information, see [Enabling and Configuring Remote Logging, page 11-29](#).
- Step 4** If you want to create other central logging servers, for use either as secondary servers or as mirrored logging servers, perform Step 1 through Step 3 for each additional server.
-

Remote Logging Options

Cisco Secure ACS provides the remote logging options listed below. These options appear on the Remote Logging Setup page.

- **Do not log Remotely**—Cisco Secure ACS writes accounting data for locally authenticated sessions only to the local logs that are enabled.
- **Log to all selected remote log services**—Cisco Secure ACS sends accounting data for locally authenticated sessions to all Cisco Secure ACSes in the Selected Log Services list.
- **Log to subsequent remote log services on failure**—Cisco Secure ACS sends accounting data for locally authenticated sessions to the first Cisco Secure ACS that is operational in the Selected Log Services list. This

behavior enables you 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 Cisco Secure ACS.

- **Remote Log Services**—This list represents the Cisco Secure ACSes configured in the Remote Agents table in Network Configuration to which Cisco Secure ACS *does not* send accounting data for locally authenticated sessions.
- **Selected Log Services**—This list represents the Cisco Secure ACSes configured in the Remote Agents table in Network Configuration to which Cisco Secure ACS *does* send accounting data for locally authenticated sessions.

Enabling and Configuring Remote Logging



Note

Before configuring the Remote Logging feature on a Cisco Secure ACS, make sure that you have configured your central logging Cisco Secure ACS. For more information, see [Implementing Centralized Remote Logging, page 11-27](#).

To enable and configure remote logging, follow these steps:

-
- Step 1** To enable the Remote Logging feature in the HTML interface, follow these steps:
- a. Click **Interface Configuration**.
 - b. Click **Advanced Options**.
 - c. Select the **Remote Logging** check box.
 - d. Click **Submit**.
- Cisco Secure ACS displays the Remote Logging link on the Logging page in the System Configuration section.
- Step 2** Click **System Configuration**.
- Step 3** Click **Logging**.
- The Logging Configuration page appears.
- Step 4** Click **Remote Logging**.

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



Note Use the “Log to subsequent remote log services on failure” option when you want to configure Cisco Secure ACS to send accounting data to a second remote Cisco Secure ACS if the first Cisco Secure ACS fails.

- Step 6** For each remote Cisco Secure ACS you want to have in the Selected Log Services list, follow these steps:
- a. In the Remote Log Services list, select the name of a Cisco Secure ACS to which you want to send accounting data for locally authenticated sessions.



Note The Cisco Secure ACSes available in the Remote Log Services list is determined by the AAA Servers table in Network Configuration. For more information about the AAA Servers table, see [AAA Server Configuration, page 4-21](#).

- b. Click --> (right arrow button) to move the selected Cisco Secure ACS to the Selected Log Services list.

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



Note If the “Log to subsequent remote log services on failure” option is selected, Cisco Secure ACS logs to the first accessible Cisco Secure ACS in the Selected Log Services list.

Step 8 Click **Submit**.

Cisco Secure ACS saves and implements the remote logging configuration you specified.

Disabling Remote Logging

By disabling the Remote Logging feature, you prevent Cisco Secure ACS from sending its accounting information to a central logging Cisco Secure ACS.

To disable remote logging, follow these steps:

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

Step 2 Click **Logging**.

Step 3 Click **Remote Logging**.

Step 4 Select the **Do not log Remotely** option.

Step 5 Click **Submit**.

Cisco Secure ACS no longer sends its accounting information for locally authenticated sessions to remote logging servers.

Service Logs

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

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

Services Logged

Cisco Secure ACS generates logs for the following services:

- CSAdmin
- CSAAuth
- CSDBSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

These files are located in the `\Logs` subdirectory of the applicable service directory. For example, the following is the default directory for the CiscoSecure authentication service:

```
c:\Program Files\CiscoSecure ACS vX.X\CSAuth\Logs
```

The most recent debug log is named as follows:

```
SERVICE.log
```

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

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

```
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 as follows:

```
SERVICE 13-07-1999.log
```

Configuring Service Logs

You can configure how Cisco Secure ACS generates and manages the service log file. The options for configuring the service log file are listed below.

- **Level of detail**—You can set the service log file to contain one of three levels of detail:
 - **None**—No log file is generated.
 - **Low**—Only start and stop actions are logged. This is the default setting.
 - **Full**—All services actions are logged.
- **Generate new file**—You can control how often a new service log file is created:
 - **Every Day**—Cisco Secure ACS generates a new log file at 12:01 A.M. local time every day.
 - **Every Week**—Cisco Secure ACS generates a new log file at 12:01 A.M. local time every Sunday.
 - **Every Month**—Cisco Secure ACS generates a new log file at 12:01 A.M. on the first day of every month.
 - **When Size is Greater than x KB**—Cisco Secure ACS generates a new log file after the current service log file reaches the size specified, in kilobytes, by x .
- **Manage Directory**—You can control how long service log files are kept:
 - **Keep only the last x files**—Cisco Secure ACS retains up to the number of files specified by x .
 - **Delete files older than x days**—Cisco Secure ACS retains only those service logs that are not older than the number of days specified by x .

To configure how Cisco Secure ACS generates and manages the service log file, follow these steps:

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

Step 2 Click **Service Control**.

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

- Step 3** To disable the service log file, under Level of detail, select the **None** option. After you click Restart, Cisco Secure ACS does not generate new service logs file.
- Step 4** To configure how often Cisco Secure ACS creates a service log file, select one of the options under Generate New File.



Note Settings under Generate New File have no effect if you selected None under Level of detail.

- Step 5** To manage which service log files Cisco Secure ACS keeps, follow these steps:
- Select the **Manage Directory** check box.
 - To limit the number of service log files Cisco Secure ACS retains, select the **Keep only the last X files** option and in the X box type the number of files you want Cisco Secure ACS to retain.
 - To limit how old service log files retained by Cisco Secure ACS can be, select the **Delete files older than X days** option and in the X box type the number of days for which Cisco Secure ACS should retain a service log file before deleting it.
- Step 6** Click **Restart**.
- Cisco Secure ACS restarts its services and implements the service log settings you specified.
-