



Logs and Reports

Cisco Secure ACS Solution Engine 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 11-1](#)
- [Special Logging Attributes, page 11-2](#)
- [NAC Attributes in Logs, page 11-4](#)
- [Update Packets in Accounting Logs, page 11-4](#)
- [About Cisco Secure ACS Logs and Reports, page 11-5](#)
- [Working with CSV Logs, page 11-13](#)
- [Remote Logging, page 11-17](#)
- [Service Logs, page 11-25](#)

Logging Formats

Cisco Secure ACS logs a variety of user and system activities. Regardless of the content, a Cisco Secure ACS Solution Engine writes all logs in comma-separated (CSV) files. The CSV format records data in columns separated by commas.

Files in a CSV format are 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 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 11-14](#).

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 a 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 4-17](#).

- **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 4-25](#).

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 11-25](#).

This section contains the following topics:

- [Accounting Logs, page 11-6](#)
- [Dynamic Administration Reports, page 11-7](#)
- [Cisco Secure ACS System Logs, page 11-12](#)

Accounting Logs

Accounting logs contain information about the use of remote access services by users. They are available in CSV format. [Table 11-1](#) contains descriptions of 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 • CLID 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>

Table 11-1 Accounting Log Descriptions (Continued)

Log	Description
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>
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 Healthy.
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 any posture validation that returns a posture token of Healthy.

Table 11-2 What You Can Do with Accounting Logs

What You Can Do	Description and Related Topics
Enable an accounting log	For instructions, see Enabling or Disabling a CSV Log, page 11-13 .
View an accounting report	For instructions, see Viewing a CSV Report, page 11-14 .
Configure an accounting log	For instructions, see Configuring a CSV Log, page 11-15 .

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>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 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 13-14.</p> <p>Note To use the logged-in user list feature, you must configure AAA client to perform authentication and accounting using the same protocol—either TACACS+ or RADIUS.</p> <p>For instructions on viewing the Logged-in User report in the HTML interface, see Viewing the Logged-in Users Report, page 11-9.</p> <p>For instructions about deleting logged-in users from specific AAA clients or from all AAA clients, see Deleting Logged-in Users, page 11-10.</p>
Disabled Accounts	<p>Lists all user accounts that are currently disabled and the reason they were disabled.</p> <p>For instructions on viewing the Disabled Accounts report in the HTML interface, see Viewing the Disabled Accounts Report, page 11-11.</p>
Appliance Status	<p>Lists statistics about resource utilization on the Cisco Secure ACS Solution Engine and provides details about IP configuration, including the MAC address for the network interface card.</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 7-2](#).

Viewing the Appliance Status Report

Use this procedure to view the Appliance Status report.

To view the Appliance Status report, follow these steps:

Step 1 In the navigation bar, click **Reports and Activity**.**Step 2** Click **Appliance Status**.

Cisco Secure ACS displays information about resource utilization on the Cisco Secure ACS Solution Engine. Also displayed is information about the IP configuration for the Cisco Secure ACS Solution Engine and the MAC address of its network interface card.

**Tip**

Click Refresh to update the information displayed on the Appliance Status report page.

Cisco Secure ACS System Logs

The 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 available in CSV format. For information about each system log, see [Table 11-4](#).

For instructions on viewing a CSV report in the HTML interface, see [Viewing a CSV Report, page 11-14](#).

Table 11-4 System 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.
User Password Changes	Lists user password changes initiated by users, regardless of which password change mechanism 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.
ACS Service Monitoring	Lists when Cisco Secure ACS services start and stop.
Appliance Administration Audit	Lists administrator activity on the serial console, including logins, logouts, and commands executed.

Working with CSV Logs

This section contains the following topics:

- [CSV Log Size and Retention, page 11-13](#)
- [Enabling or Disabling a CSV Log, page 11-13](#)
- [Viewing a CSV Report, page 11-14](#)
- [Configuring a CSV Log, page 11-15](#)

CSV Log Size and Retention

For each CSV log, Cisco Secure ACS writes a separate log file. When a log file reaches 10 MB in size, Cisco Secure ACS starts a new log file. Cisco Secure ACS retains the most recent 7 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 11-15](#).



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 11-5](#).

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 11-15](#).

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 data attributes that make up the content of a CSV log. For instructions about enabling or disabling a CSV log, see [Enabling or Disabling a CSV Log, page 11-13](#).

The logs to which this procedure applies are:

- 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.

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, 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 Click **Submit**.

Cisco Secure ACS implements the CSV log configuration that you specified.

Remote Logging

This section discusses remote logging capabilities of Cisco Secure ACS.

This section contains the following topics:

- [About Remote Logging, page 11-17](#)
- [Implementing Centralized Remote Logging, page 11-18](#)
- [Local Configuration of Remote Logging, page 11-19](#)
- [Remote Agent Logging Configuration, page 11-22](#)

About Remote Logging

The Remote Logging feature enables Cisco Secure ACS to send accounting data received from AAA clients to a Cisco Secure ACS Remote Agent. The remote agent runs on a computer on your network. It writes the accounting data sent to it by Cisco Secure ACS into CSV files. You can configure many Cisco Secure 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 Cisco Secure ACS accounting logs, see [Accounting Logs, page 11-6](#). For more information about installing and configuring a Cisco Secure ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agent*.



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 4-41](#).

The Remote Logging Setup page, available from the Logging Configuration page in the System Configuration section, is where you configure Cisco Secure 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 11-19](#).

Regardless of how many Cisco Secure ACSes send their accounting data to the central logging server, the remote agent receives its configuration from a single Cisco Secure ACS Solution Engine. That Cisco Secure ACS is the configuration provider for the remote agent. In the HTML interface of the configuration provider Cisco Secure ACS, you determine the remote agent configuration. By using the links found 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, and how the remote agent manages the log files. For more information about configuring remote agent logging, see [Remote Agent Logging Configuration, page 11-22](#).

Implementing Centralized Remote Logging

To implement centralized remote logging, follow these steps:

-
- Step 1** Install and configure a Cisco Secure ACS Remote Agent on a computer that you want to use to store centralized logging data. For more information about installing and configuring a Cisco Secure ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agent*.
 - Step 2** On each Cisco Secure ACS Solution Engine, add the remote agent. For more information, see [Remote Agent Configuration, page 4-29](#).
 - Step 3** On each Cisco Secure ACS Solution Engine, enable remote logging. For more information, see [Local Configuration of Remote Logging, page 11-19](#).
 - Step 4** On the Cisco Secure 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 11-22](#).
 - Step 5** If you want to create another central logging server, for use either 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 consists of enabling the Cisco Secure ACS Solution Engine to send accounting data to remote agents and specifying which remote agents the accounting data is to be sent to.

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 11-22](#).

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**—When selected, this option limits Cisco Secure 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 Cisco Secure 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 Cisco Secure 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. This 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**—The remote agents 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**—The remote agents 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

Before You Begin

Make sure that you have configured your central logging server. For more information, see [Implementing Centralized Remote Logging, page 11-18](#).

To enable and configure remote logging, follow these steps:

-
- Step 1** To enable remote logging, follow these steps:
- Click **Interface Configuration**.
 - Click **Advanced Options**.
 - Select the **Remote Logging** check box.
 - 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** Under Local Logging Configuration, click **Remote Logging**.
- Step 5** Select the applicable remote logging option:
- To send the accounting information for this Cisco Secure ACS to more than one remote agent, select the **Log to all selected remote log services** option.
 - To send the accounting information for this Cisco Secure ACS to a single remote agent, 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 agent if the first remote fails.

- Step 6** For each remote agent 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 remote agent to which you want to send accounting data for locally authenticated sessions.



Note The remote agents available in the Remote Log Services list is determined by the Remote Agents table in Network Configuration. For more information about the Remote Agents table, see [Remote Agent Configuration, page 4-29](#).

- b. 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 the “Log to subsequent remote log services on failure” option is selected, Cisco Secure ACS logs to the first accessible remote agent 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

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

To disable remote logging, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**.
 - Step 3** Under Local Logging Configuration, 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 agents.

Remote Agent Logging Configuration

Remote agent logging configuration consists of 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 Cisco Secure ACS to send to a remote agent. You can configure each log separately.

For information about configuring which remote agents Cisco Secure ACS sends log data to, see [Local Configuration of Remote Logging, page 11-19](#).

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. You have the following options:
 - **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 11-19](#).

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 11-22](#).

To configure a CSV log for a remote agent, follow these steps:

-
- 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 you want to configure.

The CSV *log* File Configuration page appears, where *log* is the name of the remote agent log you selected.

Step 4 To enable the log, select the **Log to CSV *log name* report** check box.



Note If the Log to CSV *log name* report check box is not selected, Cisco Secure 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 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, 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 remote agent log configuration that you specified.

Service Logs

The service logs may be 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, Cisco Secure ACS generates RADIUS service logs even if you are not using RADIUS to communicate with AAA clients or other AAA servers.

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 more information about this feature, see [Support, page 8-25](#).

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

Services Logged

Cisco Secure ACS generates logs for the following services:

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

These files can be retrieved from the appliance using the Support feature in the System Configuration section or using the **support** command at the serial console.

For each service, Cisco Secure ACS writes separate log files. When a log file reaches 10 MB in size, Cisco Secure ACS starts a new log file. Cisco Secure ACS retains the most recent 30 log files for each service.

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, 2003, would be named as follows:

SERVICE 2003-07-13.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 13-07-2003.log

Configuring Service Log Detail

You can configure the level of detail with which Cisco Secure ACS generates service log files. 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.

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 Cisco Secure ACS appliance.

- Step 3** If you want 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** If you want to enable service logging, under Level of detail, select the **Low** or **Full** option, as applicable.
After you click Restart, Cisco Secure ACS generates service logs with the level of detail you specified.
- Step 5** Click **Restart**.
Cisco Secure ACS restarts its services and implements the service log settings you specified.
-

