



Logs and Reports

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

This chapter contains the following topics:

- [Logging Formats, page 11-1](#)
- [Special Logging Attributes, page 11-2](#)
- [Posture-Validation Attributes in Logs, page 11-3](#)
- [Update Packets in Accounting Logs, page 11-3](#)
- [About ACS Logs and Reports, page 11-4](#)
- [Working with CSV Logs, page 11-10](#)
- [Working with ODBC Logs, page 11-16](#)
- [Remote Logging, page 11-19](#)
- [Service Logs, page 11-23](#)

Logging Formats

ACS logs a variety of user and system activities. Depending on the log and how you have configured 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 from the third-party vendor. You can access the CSV files on the ACS server hard drive or by downloading the CSV file from the web interface. For more information about downloading the CSV file from the web interface, see [Viewing a CSV Report, page 11-12](#).
- **ODBC-compliant database tables**—You can use Open DataBase Connectivity (ODBC) logging to configure 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 from the relational database vendor.

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

Special Logging Attributes

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

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

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

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

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

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

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

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

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

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



Note

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

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

Posture-Validation Attributes in Logs

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

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

Reporting HCAP Errors

The `Authen-Failure-Code` entry in the Failed-Attempts report may display one of the following errors when HCAP fails:

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

Update Packets in Accounting Logs

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

**Note**

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

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

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

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

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

About ACS Logs and Reports

ACS provides logs that can be divided into four types:

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

This section contains information about the items from the previous list. For information about service logs, see [Service Logs, page 11-23](#).

This section contains the following topics:

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

**Note**

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

Accounting Logs

Accounting logs contain information about the use of remote access services by users. By default, these logs are available in CSV format, with the exception of the Passed Authentications log. You can also configure 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 web interface, all accounting logs can be enabled, configured, and viewed. [Table 11-2](#) contains information about what you can do with the accounting logs.

Table 11-1 Accounting Log Descriptions

Log	Description
TACACS+ Accounting	<p>Contains:</p> <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification (CLID) • Session duration
TACACS+ Administration	<p>Lists configuration commands entered on a AAA client by using TACACS+ (Cisco IOS). Particularly if you use ACS to perform command authorization, we recommend that you use this log.</p> <p>Note To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with ACS.</p>
RADIUS Accounting	<p>Contains:</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 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:</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 ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places.</p>
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 <code>Healthy</code>.</p> <p>Note In entries in the Failed Attempts log, the <code>ExtDB Info</code> attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user-authentication attempt.</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 all posture-validation requests resulting in an SPT.</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 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 11-11. • ODBC—For instructions on how to enable an account log in ODBC format, see Configuring an ODBC Log, page 11-17.
View an accounting report	For instructions on viewing an accounting report in the web interface, see Viewing a CSV Report, page 11-12 .
Configure an accounting log	<p>The steps for configuring an accounting log vary depending upon which format you use. For more information about log formats, see Logging Formats, page 11-1.</p> <ul style="list-style-type: none"> • CSV—For instructions on configuring the CSV accounting log, see Configuring a CSV Log, page 11-14. • ODBC—For instructions on configuring ODBC accounting log, see Configuring an ODBC Log, page 11-17.

Dynamic Administration Reports

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

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

Table 11-3 Dynamic Administration Report Descriptions and Related Topics

Report	Description and Related Topics
Logged-In Users	<p>Lists all users receiving services for a single AAA client or all AAA clients. Users accessing the network with Cisco Aironet equipment appear on the list for the access point that they are currently associated with, provided that the firmware image on the Cisco Aironet Access Point supports sending the RADIUS Service-Type attribute for rekey authentications.</p> <p>On a computer configured to perform machine authentication, machine authentication occurs when the computer starts. When a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section. Once user authentication begins, the computer no longer appears on the Logged-In Users List. For more information about machine authentication, see EAP and Windows Authentication, page 13-10.</p> <p>Note To use the logged-in user list feature, you must configure AAA clients to perform authentication and accounting by using the same protocol—TACACS+ or RADIUS.</p> <p>For instructions on viewing the Logged-in User report in the web interface, see Viewing the Logged-in Users Report, page 11-7.</p> <p>For instructions about deleting logged-in users from specific AAA clients or from all AAA clients, see Deleting Logged-in Users, page 11-7.</p>
Disabled Accounts	<p>Lists all user accounts that are disabled and the reason they were disabled.</p> <p>For instructions on viewing the Disabled Accounts report in the web interface, see Viewing the Disabled Accounts Report, page 11-8.</p>

Viewing the Logged-in Users Report

To view the Logged-in Users report:

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

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

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



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

Step 3 Do one of the following:

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

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

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



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

Deleting Logged-in Users

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



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

To delete logged-in users:

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

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

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

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

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

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

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

Viewing the Disabled Accounts Report

To view the Disabled Accounts report:

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

Step 2 Click **Disabled Accounts**.

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

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

ACS opens the user account for editing.

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

ACS System Logs

System logs are logs about the ACS system and therefore record system-related events. These logs are useful for troubleshooting or audits. They are always enabled and are only available in CSV format. 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 web interface, see [Viewing a CSV Report, page 11-12](#).

Table 11-4 Accounting Log Descriptions and Related Topics

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

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

Log	Description and Related Topics
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 11-9 .
User Password Changes	Lists user password changes that users initiate, regardless of which password-change mechanism was used to change the password. Thus, this log contains records of password changes accomplished by the ACS Authentication Agent, by the User Changeable Password web interface, or by Telnet session on a network device using TACACS+. It does not list password changes that an administrator makes in the ACS web interface. For information about configuring the User Password-Changes log, see Configuring Local Password Management, page 8-6 .
ACS Service Monitoring	Lists when ACS services start and stop. For information about configuring the ACS Service Monitoring log, see ACS Active Service Management, page 8-13 .

Configuring the Administration Audit Log

You use this procedure to configure how often, or at what size limit, 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:

-
- 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 a frequency:
- **Every day**— ACS generates a new Administrative Audit CSV file at the start of each day.
 - **Every week**— ACS generates a new Administrative Audit CSV file at the start of each week.
 - **Every month**— 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 ACS keeps:
- a. Check the **Manage Directory** check box.
 - b. To limit the number of Administrative Audit CSV files that ACS retains, select the **Keep only the last X files** option and type in the *X* box the number of files that you want ACS to retain.
 - c. To limit the age of Administrative Audit CSV files that ACS retains, select the **Delete files older than X days** option and type the number of days for which ACS should retain a Administrative Audit CSV file before deleting it.

Step 6 Click **Submit**.

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 11-10](#)
- [CSV Log File Locations, page 11-10](#)
- [Enabling or Disabling a CSV Log, page 11-11](#)
- [Viewing a CSV Report, page 11-12](#)
- [Log Filtering, page 11-13](#)
- [Configuring a CSV Log, page 11-14](#)

**Tip**

Using a CSV file may not work well in different countries; for example, when imported into programs such as Word or Excel. You may need to replace the commas (,) with semicolons (;), if necessary.

CSV Log File Names

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

Older files are named as:

logyyyy-mm-dd.csv

where

log is the name of the log.

yyyy is the year that the CSV file was started.

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

dd is the date that the CSV file was started.

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

CSV Log File Locations

By default, ACS keeps log files in directories that are unique to the log. You can use the web interface 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
ACS Backup and Restore	Logs\Backup and Restore	No
RDBMS Synchronization	Logs\DbSync	No
RDBMS Synchronization	Logs\DBReplicate	No
Administration Audit	Logs\AdminAudit	No
User Password Changes	CSAuth>PasswordLogs	No
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 11-14](#).



Note

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

To enable or disable a CSV log:

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

Viewing a CSV Report

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

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

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

To view a CSV report:

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

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

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



Tip You can configure how ACS handles old CSV report files. For more information, see [Configuring a CSV Log, page 11-14](#).

Step 3 Click the CSV report filename whose contents that 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 ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.



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

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

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 click **Save** to save the file.

Log Filtering

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

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

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

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

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



Note

The functionality of the **Refresh** and **Download** links remain unchanged (without filtering). See [Viewing a CSV Report, page 11-12](#).

To apply a log filter:

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

Regular Expression Basic Syntax Reference

Table 11-6 lists the Regular Expression characters and their syntax definitions.

Table 11-6 Regular Expression Syntax Definitions

Character	Regular Expression Use
^	A caret (^) matches to the beginning of the string. Referred to as “begins with.” For example, ^A will match ABc , A123 , but not 1A234 . See the last table entry for another caret usage.
\$	The dollar sign (\$) matches the end of the string. Referred to as “ends with.” For example, yz\$ will match strings ending with xyz , 0123yz , but not 12yzA .
\	The backslash (\) matches a given string at any location. Referred to as “contains.” A backslash is also used for expressing 'special characters' in a given regular expression (For example, \+ will match against the plus sign (+), to differentiate from the plus sign (+) usage in regular expressions.
.	The dot (.) matches any character.
*	The asterisk (*) indicates that the character to the left of the asterisk in the expression should match for any number of instances (that is, 0 or more times).
+	The plus sign (+) is similar to the asterisk (*) but at least one match of the character should appear to the left of the plus sign (+) in the expression.
?	The question mark (?) matches the expression or character to its left 0 or 1 times.
	The pipe () allows the expression on either side of it to match the target string. For example, A a matches against A as well as a .
-	The hyphen (-) indicates a range of values. For example, a-z .
()	The parentheses are used for grouping of expressions and affects the order of pattern evaluation
[]	Brackets ([]) and () enclosing a set of characters indicate that any of the enclosed characters may match the target character. Values in brackets can be one or more characters, or ranges. For example, [02468] , [0-9] .
[^	When a caret (^) is positioned to immediately follow a left bracket ([), it excludes the remaining characters within brackets from matching the target string. For example, [^0-9] indicates that the target character is alpha rather than numeric.

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 11-11](#).

The logs to which this procedure applies are:

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

**Note**

You cannot configure the ACS Backup and Restore, RDBMS synchronization, and Database Replication CSV logs.

You can configure several aspects of a CSV log, including:

- **Log content**—Select which data attributes are included in the log.
- **Log generation frequency**—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**—Specify where on the local hard drive ACS writes the CSV file.
- **CSV file retention**—Specify how many old CSV files ACS maintains or set a maximum number of files to retain.

To configure a CSV log:

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

Step 2 Click **Logging**.

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

The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log that you selected.

The Select Columns To Log table contains two lists, Attributes and Logged Attributes. The attributes in the Logged Attributes list appear on the log that you selected.

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

The attribute moves to the Logged Attributes list.

**Tip**

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

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

The attribute moves to the Attributes list.

**Tip**

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

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

Step 7 To generate a new CSV file at a regular interval, select a frequency:

- **Every day**— ACS generates a new CSV file at the start of each day.
- **Every week**— ACS generates a new CSV file at the start of each week.
- **Every month**— 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 ACS keeps:

- Select the **Manage Directory** check box.

- b. To limit the number of CSV files that ACS retains, select the **Keep only the last X files** option and type the number of files you want ACS to retain in the X box.
- c. To limit the age of the CSV files that ACS can retain, select the **Delete files older than X days** option and type the number of days for which ACS should retain a CSV file before deleting it.

Step 10 Click **Submit**.

ACS implements the CSV log configuration that you specified.

Working with ODBC Logs

This section contains the following topics:

- [Preparing for ODBC Logging, page 11-16](#)
- [Configuring a System Data Source Name for ODBC Logging, page 11-17](#)
- [Configuring an ODBC Log, page 11-17](#)

Preparing for ODBC Logging

The following procedure explains how to prepare for ODBC logging. After you have prepared for ODBC logging, you can configure individual ODBC logs.

To prepare for ODBC logging:

- 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 that is running ACS. For instructions, see [Configuring a System Data Source Name for an ODBC External User Database, page 13-43](#).
- Step 3** Enable ODBC logging in the ACS web interface:
 - a. In the navigation bar, click **Interface Configuration**.
 - b. Click **Advanced Options**.
 - c. Select the **ODBC Logging** check box.
 - d. Click **Submit**.

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

You can now configure individual ODBC logs. For instructions, see [Configuring an ODBC Log, page 11-17](#).

Configuring a System Data Source Name for ODBC Logging

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

To create a system DSN for use with ODBC logging:

-
- 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 to use with your new DSN, and then click **Finish**.
- A dialog box displays fields requiring information that is specific to the ODBC driver that 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 ACS for communicating with the relational database is created on the computer running 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:

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



Note

Before you can configure an ODBC log, you must prepare for ODBC logging. For more information, see [Preparing for ODBC Logging, page 11-16](#).

To configure an ODBC log:

- 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. ACS includes in the log only those attributes that are in the Logged Attributes list.

Step 4 Specify the attributes that you want 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 that are 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 ACS to communicate with the ODBC database:

- a. From the Data Source list, select the system DSN that you created to allow 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**.

ACS saves the log configuration.

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

The ODBC log configuration page reappears.

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 that is specified in the **Table Name** box. The column names are the attributes that are 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 exactly match the names in the generated SQL.

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

- a. In the navigation bar, click **System Configuration**.
- b. Click **Logging**.
- c. Click the name of the ODBC log that you are configuring.

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

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

Step 12 Click **Submit**.

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

Remote Logging

This section discusses the remote logging capabilities of ACS.

This section contains the following topics:

- [About Remote Logging, page 11-19](#)
- [Implementing Centralized Remote Logging, page 11-20](#)
- [Remote Logging Options, page 11-21](#)
- [Enabling and Configuring Remote Logging, page 11-21](#)
- [Disabling Remote Logging, page 11-22](#)

About Remote Logging

You can use the Remote Logging feature to centralize accounting logs that multiple ACSs generate. You can configure each ACS to point to one ACS to use as a central logging server. The central logging ACS still performs AAA functions, but it also is the repository for accounting logs that it receives. For more information about ACS accounting logs, see [Accounting Logs, page 11-4](#).

The Remote Logging feature enables 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 that it is configured to use—CSV and ODBC—regardless of the local logging configuration on the ACSs that are sending the data to the central logging server.

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. ACS only applies Remote Logging settings to accounting data for sessions that the proxy authenticates when accounting data for sessions that the proxy authenticates is logged locally. For more information about proxied authentication requests and accounting data for sessions that the proxy authenticates, see [Proxy Distribution Table Configuration, page 4-23](#).

Implementing Centralized Remote Logging

Before You Begin

Ensure that gateway devices between remote ACSs and the central logging ACS permit the central logging ACS to receive data on TCP port 2001.

To implement centralized remote logging:

Step 1 On a computer on which you will to store centralized logging data, install ACS. For information about installing ACS, see the *Installation Guide for Cisco Secure ACS for Windows*.

Step 2 In the ACS that is running on the central logging server:

- a. Configure the accounting logs as needed. All accounting data that is sent to the central logging server will be recorded in the way that you configure accounting logs on this ACS. For information about accounting logs, see [Accounting Logs, page 11-4](#).

Accounting logs can be recorded in CSV or ODBC format. For information about configuring CSV logs, see [Working with CSV Logs, page 11-10](#). For information about configuring ODBC logs, see [Configuring an ODBC Log, page 11-17](#).

- b. Add to the AAA Servers table each ACS that the central logging server is to receive accounting data from. For more information, see [AAA Server Configuration, page 4-15](#).

**Note**

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

Step 3 For each ACS that will send its accounting data to the central logging server:

- a. Add the central logging server to the AAA Servers table in Network Configuration. For more information, see [AAA Server Configuration, page 4-15](#).
- b. Enable remote logging. For more information, see [Enabling and Configuring Remote Logging, page 11-21](#).

Step 4 If you want to create other central logging servers for use as secondary servers or as mirrored logging servers, perform Step 1 through Step 3 for each additional server.

Remote Logging Options

ACS provides the following remote logging options. These options appear on the Remote Logging Setup page.

- **Do not log Remotely**— ACS writes accounting data for locally authenticated sessions only to the local logs that are enabled.
- **Log to all selected remote log services**— ACS sends accounting data for locally authenticated sessions to all ACSs in the Selected Log Services list.
- **Log to subsequent remote log services on failure**— ACS sends accounting data for locally authenticated sessions to the first ACS that is operational in the Selected Log Services list. You can, therefore, configure one or more backup central logging servers so that no accounting data is lost if the first central logging server fails or is otherwise unavailable to ACS.
- **Remote Log Services**—This list represents the ACSs that are configured in the Remote Agents table in Network Configuration to which ACS *does not* send accounting data for locally authenticated sessions.
- **Selected Log Services**—This list represents the ACSs that are configured in the Remote Agents table in Network Configuration to which ACS *does* send accounting data for locally authenticated sessions.

Enabling and Configuring Remote Logging

**Note**

Before configuring the Remote Logging feature on ACS, ensure that you have configured your central logging ACS. For more information, see [Implementing Centralized Remote Logging, page 11-20](#).

To enable and configure remote logging:

Step 1 To enable the Remote Logging feature in the web interface:

- a. Click **Interface Configuration**.
- b. Click **Advanced Options**.
- c. Select the **Remote Logging** check box.
- d. Click **Submit**.

ACS displays the Remote Logging link on the Logging page in the System Configuration section.

Step 2 Click **System Configuration**.

Step 3 Click **Logging**.

The Logging Configuration page appears.

Step 4 Click **Remote Logging**.

Step 5 Select the applicable remote logging option:

- a. To send the accounting information for this ACS to more than one ACS, select the **Log to all selected remote log services** option.
- b. To send the accounting information for this ACS to one 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 ACS to send accounting data to a second remote ACS if the first ACS fails.

Step 6 For each remote ACS that you want to include in the Selected Log Services list:

- a. In the Remote Log Services list, select the name of a ACS to which you want to send accounting data for locally authenticated sessions.



Note The ACSs that are 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 4-15](#).

- b. Click --> (right arrow button) to move the selected 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 ACSs until the order is what you need.



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

Step 8 Click **Submit**.

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

Disabling Remote Logging

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

To disable remote logging:

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**.

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

Service Logs

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

This section covers:

- [Services Logged, page 11-23](#)
- [Configuring Service Logs, page 11-24](#)
- [Helping Customer Support Gather Data, page 11-25](#)

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

Services Logged

ACS generates logs for the following services:

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

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

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

The most recent debug log is named:

```
SERVICE.log
```

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

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

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

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

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

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

Configuring Service Logs

You can configure how ACS generates and manages the service log file. The options for configuring the service log file are:

- **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**— ACS generates a new log file at 12:01 A.M. local time every day.
 - **Every Week**— ACS generates a new log file at 12:01 A.M. local time every Sunday.
 - **Every Month**— 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**— 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**— ACS retains up to the number of files specified by x .
 - **Delete files older than x days**— ACS retains only those service logs that are not older than the number of days specified by x .

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

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

Step 2 Click **Service Control**.

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

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

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

Step 4 To configure how often 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 determine which service log files ACS keeps:

- a. Select the **Manage Directory** check box.
- b. To limit the number of service log files that ACS retains, select the **Keep only the last x files** option and in the x box type the number of files that you want ACS to retain.
- c. To limit the age of service log files that ACS retains, select the **Delete files older than x days** option and in the x box type the number of days for which ACS should retain a service log file before deleting it.

Step 6 Click **Restart**.

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

Helping Customer Support Gather Data

Before You Begin

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

If a problem exists on your ACS, customer support will ask you to create a *package.cab* file. The *package.cab* file contains various files including:

- **Certificate files**—The ACS server certificate, as well as the certificate's CA.
- **Admin.txt**—Contains information regarding ACS administrators.
- **Host.txt and HostServices.txt**—Contain information regarding hosts and hosts configuration.
- **NDG.txt**—Contains configured network device groups.
- **DictionaryKey.txt and DictionaryValue.txt**—Contains ACS dictionary files.

To create a *package.cab* file:

-
- Step 1** At the command prompt, type **drwtsn32**.
- Check the Dr. Watson settings to be sure the **Dump all Symbol Table** and **Dump All Thread Contents** options are selected in addition to the default options.
- Step 2** Go to the directory in which ACS was installed.
- Step 3** Type **CSSupport.exe**.
- Run the executable with all default options. The program will collect all the necessary information including Dr. Watson logs and place them in a file called *package.cab*. The location of the file appears when the executable is finished.
-



Note

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