CHAPTER 19

Understanding Logging

This chapter describes logging functionality in ACS 5.3. Administrators and users use the various management interfaces of ACS to perform different tasks. Using the administrative access control feature, you can assign permissions to administrators and users to perform different tasks.

Apart from this, you also need an option to track the various actions performed by the administrators and users. ACS offers you several logs that you can use to track these actions and events.

This chapter contains the following sections:

About Logging

You can gather the following logs in ACS:

- Customer Logs—For auditing and troubleshooting your ACS, including logs that record daily operations, such as accounting, auditing, and system-level diagnostics.
- Debug logs—Low-level text messages that you can export to Cisco technical support for evaluation and troubleshooting. You configure ACS debug logs, using the command line interface. Specifically, you enable and configure severity levels of the ACS debug logs using the command line interface. See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.3* for more information.
- Platform logs—Log files generated by the ACS appliance operating system.

Debug and platform logs are stored locally on each ACS server. Customer logs can be viewed centrally for all servers in a deployment.

You can use the following ACS interfaces for logging:

- Web interface—This is the primary logging interface. You can configure which messages to log and to where you want the messages logged.
- Command line interface (CLI)—Allows you to display and download logs, debug logs, and debug backup logs to the local target. The CLI also allows you to display and download platform logs. See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.3* for more information.

Using Log Targets

You can specify to send customer log information to multiple consumers or *Log Targets* and specify whether the log messages are stored locally in text format or forwarded to syslog servers. By default, a single predefined local Log Target called *Local Store* stores data in text format on an ACS server and contains log messages from the local ACS server only. You can view records stored in the Local Store from the CLI.

In addition, you can specify that logs be forwarded to a syslog server. ACS uses syslog transport to forward logs to the Monitoring and Reports component. You can also define additional syslog servers to receive ACS log messages. For each additional syslog server you specify, you must define a remote log target.

In a distributed deployment, you should designate one of the secondary ACS servers as the Monitoring and Reports server, and specify that it receive the logs from all servers in the deployment. By default, a Log Target called the *LogCollector* identifies the Monitoring and Reports server.

In cases where a distributed deployment is used, the Log Collector option on the web interface designates which server collects the log information. It is recommended that you designate a secondary server within the deployment to act as the Monitoring and Reports server.

This section contains the following topics:

Logging Categories

Each log is associated with a message code that is bundled with the logging categories according to the log message content. Logging categories help describe the content of the messages that they contain.

A logging category is a bundle of message codes which describe a function of ACS, a flow, or a use case. The categories are arranged in a hierarchical structure and used for logging configuration. Each category has:

- Name—A descriptive name
- Type—Audit, Accounting, or Diagnostics
- Attribute list—A list of attributes that may be logged with messages associated with a category, if applicable

ACS provides these preconfigured global ACS logging categories, to which you can assign log targets (see Local Store Target, page 19-5):

- Administrative and Operational audit, which can include:
  - ACS configuration changes—Logs all configuration changes made to ACS. When an in item is added or edited, the configuration change events also include details of the attributes that were changed and their new values. If an edit request resulted in no attributes having new values, no configuration audit record is created.

Note For complex configuration items or attributes, such as policy or DACL contents, the new attribute value is reported as "New/Updated" and the audit does not contain the actual attribute value or values.

  - ACS administrator access—Logs all events that occur when an administrators accesses the system until the administrator logs out. It logs whether the administrator exits ACS with an explicit request or if the session has timed out. This log also includes login attempts that fail due to account inactivity. Login failures along with failure reasons are logged.
  - ACS operational changes—Logs all operations requested by administrators, including promoting an ACS from your deployment as the primary, requesting a full replication, performing software downloads, doing a backup or restore, generating and restoring PACs, and so on.
  - Internal user password change—Logs all changes made to internal user passwords across all management interfaces.

  In addition, the administrative and operational audit messages must be logged to the local store. You can optionally log these messages to remote logging targets (see Local Store Target, page 19-5).

- AAA audit, which can include RADIUS and TACACS+ successful or failed authentications, command-access passed or failed authentications, password changes, and RADIUS request responses.
- AAA diagnostics, which can include authentication, authorization, and accounting information for RADIUS and TACACS+ diagnostic requests and RADIUS attributes requests, and identity store and authentication flow information. Logging these messages is optional.
- System diagnostic, which can include system startup and system shutdown, and logging-related diagnostic messages:
  - Administration diagnostic messages related to the CLI and web interface
  - External server-related messages
  - Local database messages
  - Local services messages
  - Certificate related messages

  Logging these messages is optional.
- System statistics, which contains information on system performance and resource utilization. It includes data such as CPU and memory usage and process health and latency for handling requests.
- Accounting, which can contain TACACS+ network access session start, stop, and update messages, as well as messages that are related to command accounting. In addition, you can log these messages to the local store. Logging these messages is optional.

The log messages can be contained in the logging categories as described in this topic, or they can be contained in the logging subcategories. You can configure each logging subcategory separately, and its configuration does not affect the parent category.

In the ACS web interface, choose **System Administration > Configuration > Logging Categories > Global** to view the hierarchical structure of the logging categories and subcategories. In the web interface, choose **Monitoring and Reports > Catalog** to run reports based on your configured logging categories.

Each log message contains the following information:

- Event code—A unique message code.
- Logging category—Identifies the category to which a log message belongs.
- Severity level—Identifies the level of severity for diagnostics. See Log Message Severity Levels, page 19-4 for more information.
- Message class—Identifies groups of messages of similar context, for example, RADIUS, policy, or EAP-related context.
- Message text—Brief English language explanatory text.
- Description—English language text that describes log message reasons, troubleshooting information (if applicable), and external links for more information.
- Failure reason (optional)—Indicates whether a log message is associated with a failure reason.

Passwords are not logged, encrypted or not.

Global and Per-Instance Logging Categories

By default, a single log category configuration applies to all servers in a deployment. For each log category, the threshold severity of messages to be logged, whether messages are to be logged to the local target, and the remote syslog targets to which the messages are to be sent to, are defined.

The log categories are organized in a hierarchical structure so that any configuration changes you make to a parent category are applied to all the child categories. However, the administrator can apply different configurations to the individual servers in a deployment.

For example, you can apply more intensive diagnostic logging on one server in the deployment. The per-instance logging category configuration displays all servers in a deployment and indicates whether they are configured to utilize the global logging configuration or have their own *custom* configuration.

To define a custom configuration for a server, you must first select the *Override* option, and then configure the specific log category definitions for that server.

You can use the Log Message Catalog to display all possible log messages that can be generated, each with its corresponding category and severity. This information can be useful when configuring the logging category definitions.

Log Message Severity Levels

You can configure logs of a certain severity level, and higher, to be logged for a specific logging category and add this as a configuration element to further limit or expand the number of messages that you want to save, view, and export.

For example, if you configure logs of severity level WARNING to be logged for a specific logging category, log messages for that logging category of severity level WARNING and those of a higher priority levels (ERROR and FATAL) are sent to any configured locations. Table 19-1 describes the severity levels and their associated priority levels.

Table 19-1 Log Message Severity Levels

ACS Severity Level	Description	Syslog Severity Level
FATAL	Emergency. ACS is not usable and you must take action immediately.	1 (highest)
ERROR	Critical or error conditions.	3
WARN	Normal, but significant condition.	4
NOTICE	Audit and accounting messages. Messages of severity NOTICE are always sent to the configured log targets and are not filtered, regardless of the specified severity threshold.	5
INFO	Diagnostic informational message.	6
DEBUG	Diagnostic message.	7

Local Store Target

Log messages in the local store are text files that are sent to one log file, located at */opt/CSCOacs/logs/localStore/*, regardless of which logging category they belong to. The local store can only contain log messages from the local ACS node; the local store cannot accept log messages from other ACS nodes.

You can configure which logs are sent to the local store, but you cannot configure which attributes are sent with the log messages; *all* attributes are sent with sent log messages.

Administrative and operational audit log messages are always sent to the local store, and you can also send them to remote syslog server and Monitoring and Reports server targets.

Log messages are sent to the local store with this syslog message format:

time stamp sequence_num msg_code msg_sev msg_class msg_text attr=value

Table 19-2 describes the content of the local store syslog message format.

Table 19-2 Local Store and Syslog Message Format

Field	Description
timestamp	Date of the message generation, according to the local clock of the originating ACS, in the format *YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm*. Possible values are: • *YYYY* = Numeric representation of the year. • *MM* = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number. • *DD* = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number. • *hh* = The hour of the day—00 to 23. • *mm* = The minute of the hour—00 to 59. • *ss* = The second of the minute—00 to 59. • *xxx* = The millisecond of the second—000 to 999. • *+/-zz:zz* = The time zone offset from the ACS server's time zone, where zh is the number of offset hours and zm is the number of minutes of the offset hour, all of which is preceded by a minus or plus sign to indicate the direction of the offset. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on an ACS node that is two hours ahead of the ACS server's time zone.
sequence_num	Global counter of each message. If one message is sent to the local store and the next to the syslog server target, the counter increments by 2. Possible values are 0000000001 to 999999999.
msg_code	Message code as defined in the logging categories.
msg_sev	Message severity level of a log message (see Table 19-1).
msg_class	Message class, which identifies groups of messages with the same context.
text_msg	English language descriptive text message.
attr=value	Set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair. Attribute names are as defined in the ACS dictionaries. Values of the Response direction AttributesSet are bundled to one attribute called Response and are enclosed in curly brackets {}. In addition, the attribute-value pairs within the Response are separated by semicolons. For example: Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00; }

You can use the web interface to configure the number of days to retain local store log files; however, the default setting is to purge data when it exceeds 5 MB or each day, whichever limit is first attained.

If you do configure more than one day to retain local store files and the data size of the combined files reaches 95000Mb, a FATAL message is sent to the system diagnostic log, and all logging to the local store is stopped until data is purged. Use the web interface to purge local store log files. Purging actions are logged to the current, active log file. See Deleting Local Log Data, page 18-23.

The current log file is named *acsLocalStore.log*. Older log files are named in the format *acsLocalStore.log.YYYY-MM-DD-hh-mm-ss-xxx*, where:

- acsLocalStore.log = The prefix of a non-active local store log file, appended with the time stamp.

Note The time stamp is added when the file is first created, and should match the time stamp of the first log message in the file.

  - *YYYY* = Numeric representation of the year.
  - *MM* = Numeric representation of the month. For single-digit months (1 to 9), a zero precedes the number.
  - *DD* = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number.
  - *hh* = Hour of the day—00 to 23.
  - *mm* = Minute of the hour—00 to 59.
  - *ss* = Second of the minute—00 to 59.
  - *xxx* = Millisecond of the second—000 to 999.

You can configure the local store to be a critical log target. See Viewing Log Messages, page 19-10 for more information on critical log targets.

You can send log messages to the local log target (local store) or to up to eight remote log targets (on a remote syslog server):

- Select **System Administration > Configuration > Log Configuration > Remote Log Targets** to configure remote log targets.
- Select **System Administration > Configuration > Log Configuration > Logging Categories** to configure which log messages you want to send to which targets.

Critical Log Target

The local store target can function as a critical log target—the primary, or mandatory, log target for a logging category.

For example, administrative and operational audit messages are always logged to the local store, but you can also configure them to be logged to a remote syslog server or the Monitoring and Reports server log target. However, administrative and operational audit messages configured to be additionally logged to a remote log target are only logged to that remote log target if they are first logged successfully to the local log target.

When you configure a critical log target, and a message is sent to that critical log target, the message is also sent to the configured noncritical log target on a best-effort basis.

- When you configure a critical log target, and a message does not log to that critical log target, the message is also not sent to the configured noncritical log.
- When you do not configure a critical log target, a message is sent to a configured noncritical log target on a best-effort basis.

Select **System Administration > Configuration > Log Configuration > Logging Categories > Global > *log_category***, where *log_category*, is a specific logging category to configure the critical log target for the logging categories.

Note Critical logging is applicable for accounting and AAA audit (passed authentications) categories only. You cannot configure critical logging for the following categories: AAA diagnostics, system diagnostics, and system statistics.

Remote Syslog Server Target

You can use the web interface to configure logging category messages so that they are sent to remote syslog server targets. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP.

Log messages are sent to the remote syslog server with this syslog message header format, which precedes the local store syslog message format (see Table 19-2):

pri_num YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

Table 19-3 describes the content of the remote syslog message header format.

Table 19-3 Remote Syslog Message Header Format

Field	Description
pri_num	Priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value* 8) + severity value. The facility code valid options are: • LOCAL0 (Code = 16) • LOCAL1 (Code = 17) • LOCAL2 (Code = 18) • LOCAL3 (Code = 19) • LOCAL4 (Code = 20) • LOCAL5 (Code = 21) • LOCAL6 (Code = 22; default) • LOCAL7 (Code = 23) Severity value—See Table 19-1 for severity values.
time	Date of the message generation, according to the local clock of the originating ACS, in the format *YYYY Mmm DD hh:mm:ss*. Possible values are: • *YYYY* = Numeric representation of the year. • *Mmm* = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • *DD* = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number. • *hh* = The hour of the day—00 to 23. • *mm* = The minute of the hour—00 to 59. • *ss* = The second of the minute—00 to 59. Some device send messages that specify a time zone in the format -/+hhmm, where - and + identifies the directional offset from the ACS server's time zone, hh is the number of offset hours, and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on an ACS node that is two hours ahead of the ACS server's time zone.
xx:xx:xx:xx/host_name	IP address of the originating ACS, or the hostname.
cat_name	Logging category name preceded by the `CSCOacs` string.
msg_id	Unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.
total_seg	Total number of segments in a log message. Long messages are divided into more than one segment.
seg_num	Segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

The syslog message data or payload is the same as the Local Store Message Format, which is described in Table 19-2.

The remote syslog server targets are identified by the facility code names *LOCAL0* to *LOCAL7* (*LOCAL6* is the default logging location.) Log messages that you assign to the remote syslog server are sent to the default location for Linux syslog (*/var/log/messages*), however; you can configure a different location on the server.

The remote syslog server cannot function as a critical log target. See Critical Log Target, page 19-7 for more information on critical log targets.

Monitoring and Reports Server Target

You can use the web interface to configure logging category messages so that they are sent to the Monitoring and Reports server target. Log messages are sent to the Monitoring and Reports server target in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP protocol.

Log messages are sent to the Monitoring and Reports server with the syslog message header format described in Table 19-3, which precedes the local store syslog message format (see Table 19-2).

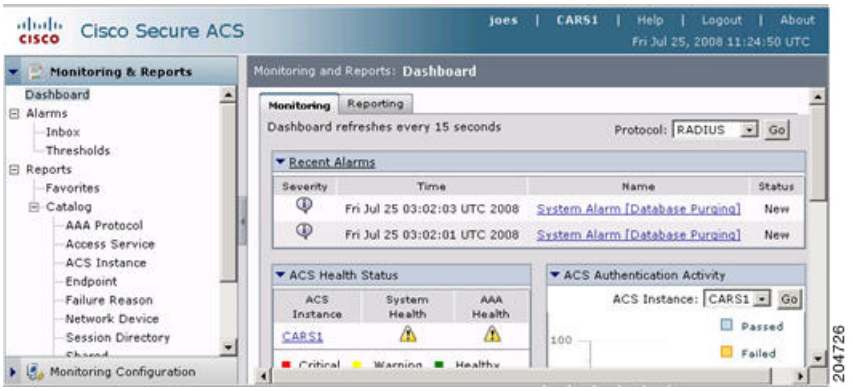
The Monitoring and Reports server cannot function as a critical log target. See Critical Log Target, page 19-7 for more information on critical log targets.

Viewing Log Messages

You can use the web interface and the CLI to view locally stored log messages. You cannot view log messages that are sent to remote syslog servers via the web interface or the CLI.

In the web interface, choose **Monitoring and Reports > Launch Monitoring & Report Viewer** to open the Monitoring and Reports Viewer in a secondary window (see Figure 19-1). See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.3* for more information about viewing log messages via the CLI.

Figure 19-1 Monitoring and Reports Viewer



The Monitoring & Report Viewer has two drawer options:

- Monitoring and Reports—Use this drawer to view and configure alarms, view log reports, and perform troubleshooting tasks.
- Monitoring Configuration—Use this drawer to view and configure logging operations and system settings.

In addition to the information that is captured in the log messages described in Logging Categories, page 19-2, the Viewer reports list successful and failed AAA authentication attempts with Step attributes. Step attributes provide information about other events that occurred within the same session. This information allows you to see the sequence of steps that resulted in an authentication success or failure.

You can use the Viewer to:

- Manage alarms, reports, and troubleshooting information.
- Manage system operations, including purging data, collecting logs, scheduling jobs, and monitoring status
- Manage system configuration, including editing failure reasons, and configuring e-mail, session directory, and alarm settings

See Monitoring and Reporting in ACS, page 11-1 for more information

Debug Logs

You can use the web interface and the CLI to send logs, including debug logs, to Cisco technical support personnel if you need troubleshooting assistance. In the web interface, choose **Monitoring and Reports > Launch Monitoring & Report Viewer > Monitoring and Reports > Troubleshooting > ACS Support Bundle**.

You can also use the CLI to view and export the hardware server in the Application Deployment Engine-OS 1.2 environment logs. These messages are sent to */var/log/boot.log* only and are unrelated to the way in which the CLI views or exports ACS debug log messages. See the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.3* for information.

ACS 4.x Versus ACS 5.3 Logging

If you are familiar with the logging functionality in ACS 4.x, ensure that you familiarize yourself with the logging functionality of ACS 5.3, which is considerably different. Table 19-4 describes the differences between the logging functionality of ACS 4.x and ACS 5.3.

Table 19-4 ACS 4.x vs. ACS 5.3 Logging Functionality

This logging function...	is handled this way in ACS 4.x...	and this way in ACS 5.3
Log Types	• AAA-related logs contain information about the use of remote access services by users. • Audit logs contain information about the ACS system and activities and, therefore, record system-related events. These logs are useful for troubleshooting or audits. CSV audit logs are always enabled, and you can enable or disable audit logs to other loggers. You cannot configure the audit log content. Audit logs can display the actual changes administrators have made for each user. ACS audit logs list all the attributes that were changed for a given user.	See Logging Categories, page 19-2.
Available Log Targets	• CSV Logger • Syslog Logger • ODBC Logger • Remote Logging	See Remote Syslog Server Target, page 19-8 and Local Store Target, page 19-5.
Log File Locations	• CSV Logger: *sysdrive*`:\Program Files\CiscoSecure ACS v`*x.x*.	• Local store target logs: */opt/CSCOacs/logs/localStore/*. • Remote syslog server target logs: */var/log/messages*.
Report Types	• CSV • Dynamic Administration • Entitlement	See Monitoring and Reporting in ACS, page 11-1.
Error Codes and Message Text	For ACS 4.2, CSAuth diagnostic logs display a description of client requests and responses. Previous versions of ACS used a numeric code for client requests and responses.	All messages, see Viewing Log Messages, page 19-10.

Table 19-4 ACS 4.x vs. ACS 5.3 Logging Functionality (continued)

This logging function…	is handled this way in ACS 4.x…	and this way in ACS 5.3
Configuration	Use the **System Configuration > Logging** page to define: • Loggers and individual logs • Critical loggers • Remote logging • CSV log file • Syslog log • ODBC log	See Configuring Logs, page 18-21 and the *CLI Reference Guide for the Cisco Secure Access Control System 5.3*.
Viewing and Downloading Log Messages	Use the **Reports and Activity** pages.	See Viewing Log Messages, page 19-10.
Troubleshooting with Log Messages	Service log files reside in the *Logs* subdirectory of the applicable service directory.	See Debug Logs, page 19-11.