



CHAPTER 8

Syslog Logging Configuration Scenario

Overview

ACS provides a system logging (syslog) feature. With the addition of this feature, all AAA reports and audit report messages can be sent to up to two syslog servers.

Configuring Syslog Logging


To configure ACS to generate syslog messages:

-
- Step 1** In the navigation bar, click **System Configuration**.
The System Configuration page opens.
 - Step 2** Click **Logging**.
The Logging page opens, shown in [Figure 8-1](#).

Figure 8-1 Logging Configuration Page

Logging Configuration

[Critical Loggers Configuration](#)
[Remote Logging Servers Configuration](#)

ACS Reports 			
<input checked="" type="checkbox"/> Indicates Logging Enabled <input checked="" type="checkbox"/> Indicates Logging Disabled			
Report Name	CSV	ODBC	Syslog
Failed Attempts	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
Passed Authentication	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
RADIUS Accounting	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
TACACS+ Accounting	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
TACACS+ Administration	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
VoIP Accounting	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
Backup and Restore	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
Database Replication	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
Administration Audit	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
User Password Changes	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
ACS Service Monitoring	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure
RDBMS Synchronization	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure

158436

Step 3 To enable a syslog report, on the Logging Configuration page, click the **Configure** link in the syslog column, in the row for each report that you want to generate.

The Enable Login window for the specified report opens, as shown in [Figure 8-2](#).

Figure 8-2 Enable Logging Page
Syslog Failed Attempts File Configuration

Enable Logging ?

Log to Syslog Failed Attempts report

If the selected log is disabled, ACS will not implement critical logging for that report.

Select Columns To Log ?

Attributes	Logged Attributes
AAA Server	Message-Type
Priv-Ivl	User-Name
Proxy-IP-Address	NAS-IP-Address
ExtDB Info	Authen-Failure-Code
Source-NAS	Author-Failure-Code
Network Device Group	Caller-ID
Access Device	NAS-Port
Device Command S	Author-Data
PEAP/EAP-FAST-Cl	Group-Name
Global Message Id	Filter Information
Logged Remotely	
EAP Type	
EAP Type Name	
Network Access Profi	
Outbound Class	
Shared RAC	
Downloadable ACL	
System-Posture-Tok	
Application-Posture	

Up Down

Syslog Servers ?

	IP	Port	Max message length (Bytes)
Server 1:			
Server 2:			

Back to Help

Submit Reset Columns Cancel

158423

Step 4 Check the check box for logging the specified information to syslog.

For example, in [Figure 8-2](#), check the **Log to Syslog Failed Attempts Report** check box.

In the Select Columns to Log section, a list of the fields available for the specified syslog report appears.

Step 5 To move an attribute to the list of the attributes shown in the report, select the field in the Available column and then click the right arrow icon to move it to the Logged Attributes column.

In the Syslog Servers section, specify the following information for the syslog servers to which ACS will send logging information:

- **IP**—Enter the IP address of the syslog server.
- **Port**—Enter the syslog port number on the specified server.
- **Max message length (Bytes)**—Enter the maximum syslog message length that ACS will accept.

You can enter information for up to two syslog servers.

Step 6 Click **Submit**.

Step 7 Repeat the process for any additional reports for which you want to enable syslog reporting.

Format of Syslog Messages in ACS Reports

Syslog messages included in ACS reports have the following format:

```
<n> mmm dd hh:mm:ss XX:XX:XX:XX TAG msg_id total_seg seg# A1=V1
```

The elements of the message are:

- *n*—The Priority value of the message; it is a combination of facility and severity of the syslog message, which is calculated according to RFC 3164, by first multiplying the *facility* value by 8 and then adding the *severity* value.
- *mmm dd hh:mm:ss*—Date and time of the message.
- *XX:XX:XX:XX*—IP Address of the machine generating this syslog message.
- *TAG*—One of the following values, depending on the application name.
 - CisACS_01_PassedAuth—Cisco ACS passed authentications.
 - CisACS_02_FailedAuth—Cisco ACS failed attempts.
 - CisACS_03_RADIUSAcc—Cisco ACS RADIUS accounting.
 - CisACS_04_TACACSAcc—Cisco ACS TACACS+ accounting.
 - CisACS_05_TACACSAdmin—Cisco ACS TACACS+ administration.
 - CisACS_06_VoIPAcc—Cisco ACS VoIP accounting.
 - CisACS_11_BackRestore—ACS backup and restore log messages.
 - CisACS_12_Replication—ACS database replication log messages.
 - CisACS_13_AdminAudit—ACS administration audit log messages.
 - CisACS_14_PassChanges—ACS user password changes log messages.
 - CisACS_15_ServiceMon—ACS service monitoring log messages.
 - CisACS_16_ApplAdmin—ACS appliance administration audit log messages.
- *msg_id*—Unique message id. All segments of one message share the same message ID.
- *total_seg*—Total number of segments in this message.
- *seg#*—Segment sequence number within this message segmentation.
- *A1=V1*—Attribute-value pairs delimited by a comma (,) for Cisco ACS log messages and the message itself.

Facility Codes

ACS syslog messages use the following facility values:

- **4**—Security and authorization messages. This value is used for all AAA related messages (failed attempts, passed attempts, accounting, and so on).
- **13**—Log audit. This value is used for all other ACS report messages.

All ACS syslog messages use a severity value of 6 (informational).

For example, if the facility value is 13 and the severity value is 6, the Priority value is 110 ((8 x 13) + 6). The Priority value appears according to the syslog server setup, and might appear as

one of:

– **System3.Info**

– <110>



Note You cannot configure the format of the syslog facility and severity on ACS.

The following sample syslog message shows how the facility code and other information might look in an ACS-generated syslog message:

```
<110> Oct 16 08:58:07 64.103.114.149 CisACS_13_AdminAudit 18729fp11 1 0 AAA
Server=tfurman-w2k,admin-username=local_login,browser-ip=127.0.0.1,text-message=Administra
tion session finished,
```

In this example, <110 >represents the calculated value when the facility code is 13 (the log audit facility code).

Message Length Restrictions

When an ACS message exceeds the syslog standard length limitation or target length limitation, the message content is split into several segments:

- If all attribute-value elements fit into one segment then no segmentation is performed.
- If the message does not fit into one segment, the message is split between attribute-value pairs, keeping an attribute-value pair complete within the segment. That is, the first segment ends with a semicolon (;), while the next segment's content starts with the next attribute-value pair.
- In rare cases when one attribute-value pair is too long to fit in one segment all by itself, the value is segmented between sequenced segments of the message. Such segmentation might happen if attribute value contains several hundreds of characters. In general, ACS attribute values are designed to avoid such length.

All segments of one message have exactly the same header. The <msg_id> and <total_seg> values are shared between all segments. The <seg#> is set according to number of segments and the relative part of the content follows.

Use the following message length restrictions:

- For sending messages to a standard syslog server, the maximum message length should be 1024 bytes.
- For sending messages to Cisco Security Monitoring, Analysis and Response System (MARS), the maximum message length should be 500 bytes.
- Message segmentation should be used when the original message, including header and data, exceeds length limitations.

