



CHAPTER 29

Configuring System Message Logging

This chapter describes how to configure the system message logging on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

**Note**

For more information on the system messages, refer to the *Catalyst 6500 Series Switch System Message Guide*.

This chapter consists of these sections:

- [Understanding How the System Message Logging Works, page 29-1](#)
- [System Log Message Format, page 29-3](#)
- [Default System Message Logging Configuration, page 29-4](#)
- [Configuring the System Message Logging on the Switch, page 29-5](#)
- [Configuring CallHome, page 29-13](#)

Understanding How the System Message Logging Works

The system message logging software can save messages in a log file or direct the messages to other devices. The system message logging facility has these features:

- Provides you with logging information for monitoring and troubleshooting
- Allows you to select the types of logging information that is captured
- Allows you to select the destination of the captured logging information

By default, the switch logs normal but significant system messages to its internal buffer and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility (see [Table 29-1](#)) and the severity level (see [Table 29-2](#)). The messages are time-stamped to enhance real-time debugging and management.

You can access the logged system messages using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves the syslog messages in an internal buffer that can store up to 500 messages. You can monitor the system messages remotely by accessing the switch through Telnet or the console port, or by viewing the logs on a syslog server.

If a system failure occurs, the system `syslog-dump` allows you to write the system messages in the `syslog` buffer to a flash file, capturing the pertinent `syslog` information before the system fails. If the system core dump is enabled, the `syslog` is dumped before the core.

**Note**

The messages that are redirected to a `syslog` server are delayed up to 90 seconds.

Table 29-1 describes the facility types that are supported by the system message logs.

Table 29-1 System Message Log Facility Types

Facility Name	Definition
all	All facilities
acl	ACL facility
cdp	Cisco Discovery Protocol
cops	Common Open Policy Server
dtp	Dynamic Trunking Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
filesys	File System
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
ld	ASLB facility
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
protfilt	Protocol Filter
pruning	VTP pruning
privatevlan	Private VLAN facility
qos	Quality of Service
radius	Remote Access Dial-In User Service
rsvp	ReSerVation Protocol
security	Security
snmp	Simple Network Management Protocol
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol

Table 29-1 System Message Log Facility Types (continued)

Facility Name	Definition
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vmps	VLAN Membership Policy Server
vtp	VLAN Trunking Protocol

Table 29-2 describes the severity levels that are supported by the system message logs.

Table 29-2 Severity Level Definitions

Severity Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

System Log Message Format

The system log messages begin with a percent sign (%) and can contain up to 80 characters. The messages are displayed in this format:

mm/dd/yyyy:hh/mm/ss:facility-severity-MNEMONIC:description

Table 29-3 describes the elements of the syslog messages.

Table 29-3 System Log Message Elements

Element	Description
<i>mm/dd/yyyy:hh/mm/ss</i>	Date and time of the error or event. This information appears only if configured using the set logging timestamp enable command.
<i>facility</i>	Indicates the facility to which the message refers (for example, SNMP, SYS, etc.).
<i>severity</i>	Single-digit code from 0 to 7 that indicates the severity of the message.
<i>MNEMONIC</i>	Text string that uniquely describes the error message.
<i>description</i>	Text string containing the detailed information about the event being reported.

This example shows some typical switch system messages (at system startup):

```
1999 Apr 16 10:01:26 %MLS-5-MLSENABLED:IP Multilayer switching is enabled
1999 Apr 16 10:01:26 %MLS-5-NDEDISABLED:Netflow Data Export disabled
1999 Apr 16 10:01:26 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 10:01:47 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 10:01:42 %SYS-5-MOD_OK:Module 6 is online
1999 Apr 16 10:02:27 %PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1
1999 Apr 16 10:02:28 %PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/2
```

Default System Message Logging Configuration

Table 29-4 describes the default system message logging configuration.

Table 29-4 Default System Message Logging Configuration

Configuration Parameter	Default Setting
System message logging to the console	Enabled
System message logging to Telnet sessions	Enabled
Logging buffer size	500 (default and maximum setting)
Logging history size	1
Logging history severity	Warnings (4)
Timestamp option	Enabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings (4)
Facility/severity level for system messages	sys/5 dtp/5 pagp/5 mgmt/5 mls/5 cdp/4 udld/4 all other facilities/2
System syslog dump	Disabled
System syslog-dump device and filename specifications	flash device is slot0: Filename is sysloginfo

Configuring the System Message Logging on the Switch

These sections describe how to configure the system message logging on the switch:

- [Enabling and Disabling the Session Logging Settings, page 29-5](#)
- [Setting the System Message Logging Levels, page 29-6](#)
- [Enabling and Disabling the Logging Time-Stamp Enable State, page 29-7](#)
- [Setting the Logging Buffer Size, page 29-7](#)
- [Limiting the Number of syslog Messages, page 29-7](#)
- [Configuring the syslog Daemon on a UNIX syslog Server, page 29-8](#)
- [Configuring the syslog Servers, page 29-8](#)
- [Displaying the Logging Configuration, page 29-9](#)
- [Displaying the System Messages, page 29-11](#)
- [Enabling and Disabling the System syslog Dump, page 29-11](#)
- [Specifying the System syslog Dump Flash Device and Filename, page 29-12](#)

Enabling and Disabling the Session Logging Settings

By default, the system logging messages are sent to the console and Telnet sessions that are based on the default logging facility and severity values. If desired, you can disable logging to the console or logging to a given Telnet session.

When you disable or enable logging to the console sessions, the enable state is applied to all future console sessions. For example, if you disable logging to the console, disconnect from the console port, and later reconnect, logging is still disabled for the console.

When you disable or enable logging to a Telnet session, the enable state is applied only to that session. If you disable logging to a Telnet session, disconnect the session, and later reconnect, logging is enabled for the new session.



Note

If you enter the **set logging session** command while connected through the console port, the command has the same effect as entering the **set logging console** command. However, if you enter the **set logging console** command while you are connected through a Telnet session, the default console logging enable state is changed.

To enable or disable the logging state for the console sessions, perform this task in privileged mode:

	Task	Command
Step 1	Enable or disable the default logging state for the console sessions.	set logging console {enable disable}
Step 2	Verify the logging configuration.	show logging [noalias]

This example shows how to disable logging to the current and future console sessions:

```
Console> (enable) set logging console disable
System logging messages will not be sent to the console.
Console> (enable)
```

	Task	Command
Step 1		set logging session enable disable
Step 2		show logging noalias

```
Console> (enable) set logging session disable
System logging messages will not be sent to the current login session.
Console> (enable)
```

Setting the System Message Logging Levels

```
all
default
set logging level
default
```

	Task	Command
Step 1		set logging level all <i>facility severity</i> default
Step 2		show logging noalias

```
Console> (enable) set logging level all 5
All system logging facilities for this session set to severity 5(notifications)
Console> (enable)
```

cdp

```
Console> (enable) set logging level cdp 3 default
System logging facility <cdp> set to severity 3(errors)
Console> (enable)
```

Enabling and Disabling the Logging Time-Stamp Enable State

	Task	Command
Step 1		<code>set logging timestamp enable disable</code>
Step 2		<code>show logging noalias</code>

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable)
```

Setting the Logging Buffer Size

	Task	Command
Step 1		<code>set logging buffer <i>buffer_size</i></code>
Step 2		<code>show logging noalias</code>

```
Console> (enable) set logging buffer 200
System logging buffer size set to <200>
Console> (enable)
```

Limiting the Number of syslog Messages

	Task	Command
Step 1		<code>set logging history severity <i>severity_level</i></code>
Step 2		<code>show logging</code>

```
Console> (enable) set logging history severity 5
System logging history set to severity <5>
Console> (enable)
```

Configuring the syslog Daemon on a UNIX syslog Server

Step 1

```
user.debug /var/log/myfile.log
```



Note

```
user.debug /var/log/
```

```
user
```

```
debug
```

Step 2

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

Step 3

```
$ kill -HUP `cat /etc/syslog.pid`
```

Configuring the syslog Servers



Note

“Configuring the syslog Daemon on a UNIX syslog Server” section on page 29-8.

To configure the switch to log messages to a syslog server, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of one or more syslog servers ¹ .	set logging server <i>ip_addr</i>
Step 2	Set the facility and severity levels for syslog server messages.	set logging server facility <i>server_facility_parameter</i> set logging server severity <i>server_severity_level</i>
Step 3	Enable the system message logging to the configured syslog servers.	set logging server enable
Step 4	Verify the configuration.	show logging [noalias]

1. You can configure a maximum of three syslog servers.

This example shows how to specify a syslog server, set the facility and severity levels, and enable logging to the server:

```
Console> (enable) set logging server 10.10.10.100
10.10.10.100 added to System logging server table.
Console> (enable) set logging server facility local5
System logging server facility set to <local5>
Console> (enable) set logging server severity 5
System logging server severity set to <5>
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

To delete a syslog server from the syslog server table, perform this task in privileged mode:

Task	Command
Delete a syslog server from the syslog server table.	clear logging server <i>ip_addr</i>

This example shows how to delete a syslog server from the syslog server table:

```
Console> (enable) clear logging server 10.10.10.100
System logging server 10.10.10.100 removed from system logging server table.
Console> (enable)
```

To disable logging to the syslog server, perform this task in privileged mode:

Task	Command
Disable system message logging to the configured syslog servers.	set logging server disable

This example shows how to disable logging to the syslog servers:

```
Console> (enable) set logging server disable
System logging messages will not be sent to the configured syslog servers.
Console> (enable)
```

Displaying the Logging Configuration

Enter the **show logging** command to display the current system message logging configuration. Enter the **noalias** keyword to display the IP addresses instead of the host names of the configured syslog servers.

To display the current system message logging configuration, perform this task:

Task	Command
Display the current system message logging configuration.	show logging [noalias]

This example shows how to display the current system message logging configuration:

```
Console> (enable) show logging
Logging buffered size:      500
      timestamp option:    enabled
Logging history size:      1
      severity:            notifications(5)
Logging console:           enabled
Logging server:            disabled
      server facility:     LOCAL7
      server severity:     warnings(4)
Current Logging Session:   enabled
```

Facility	Default Severity	Current Session Sever
-----	-----	-----
acl	5	5
cdp	4	4
cops	3	3
dtp	5	5
dvlan	2	2
earl	2	2
fileSYS	2	2
gvrp	2	2
ip	2	2
kernel	2	2
ld	3	3
mcast	2	2
mgmt	5	5
mls	5	5
pagp	5	5
protfilt	2	2
pruning	2	2
privatevlan	3	3
qos	3	3
radius	2	2
rsvp	3	3
security	2	2
snmp	2	2
spantree	2	2
sys	5	5
tac	2	2
tcp	2	2
telnet	2	2
tftp	2	2
udld	4	4
vmps	2	2
vtp	2	2
0 (emergencies)	1 (alerts)	2 (critical)
3 (errors)	4 (warnings)	5 (notifications)
6 (information)	7 (debugging)	

```
Console> (enable)
```

Enter the **show logging buffer** command to display the messages in the switch logging buffer. If you do not specify *number_of_messages*, the default is to display the last 20 messages in the buffer (-20).

To display the messages in the switch logging buffer, perform one of these tasks:

Display the first <i>number_of_messages</i> messages in the buffer.	show logging buffer [<i>number_of_messages</i>]
Display the last <i>number_of_messages</i> messages in the buffer.	show logging buffer - [<i>number_of_messages</i>]

This example shows how to display the first five messages in the buffer:

```
Console> (enable) show logging buffer 5
1999 Apr 16 08:40:11 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 2 is online
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
```

This example shows how to display the last five messages in the buffer:

```
Console> (enable) show logging buffer -5
%PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%SPANTREE-5-PORTDEL_SUCCESS:3/2 deleted from vlan 1 (PAGP_Group_Rx)
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
Console> (enable)
```

If the system fails, a file containing the system messages in the syslog buffer (as displayed when entering the **show logging buffer** command) is produced.

To enable or disable the system syslog dump, perform this task in privileged mode (by default, the syslog dump is disabled):

Enable or disable the system syslog dump.	set system syslog-dump {enable disable}
Verify the status of the system syslog dump.	show system

This example shows how to enable the system syslog dump:

```
Console> (enable) set system syslog-dump enable
(1) In the event of a system crash, this feature will
cause a syslog file to be written out.
(2) Selected syslog file is slot0:sysloginfo
(3) Please make sure the above device has been installed,
and ready to use.
Syslog-dump enabled
Console> (enable)
```

This example shows how to disable the system syslog dump:

```
Console> (enable) set system syslog-dump disable
Syslog-dump disabled
Console> (enable)
```

This example shows how to display the status of the system syslog dump:

```
Console> (enable) show system
PS1-Status PS2-Status
-----
ok          none

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
-----
ok          off          ok          1,00:03:18  20 min
.
.
.
Core Dump          Core File
-----
disabled          slot0:crashinfo

Syslog Dump          Syslog File
-----
enabled            slot0:sysloginfo
Console> (enable)
```

Specifying the System syslog Dump Flash Device and Filename

	Task	Command
Step 1		set system syslog-file <i>device filename</i>
Step 2		show system

```
Console> (enable) set system syslog-file bootflash:
Default filename sysloginfo added to the device bootflash:
System syslog-file set.
Console> (enable)
```

```

Console> (enable) set system syslog-file bootflash:sysmsgsl
System syslog-file set.
Console> (enable)

```

```

Console> (enable) set system syslog-file
System syslog-file set to the default file.
Console> (enable)

```

Configuring CallHome

set logging callhome severity

set logging level

	Task	Command
Step 1		set logging callhome enable disable
Step 2		set logging callhome destination <i>Email or Epage Address</i> fragment <i>size in bytes</i>
Step 3		set logging callhome smtp-server <i>IP Address</i>
Step 4		set logging callhome severity <i>level</i>
	Note	

Task	Command
Step 5 (Optional) Set the “from” e-mail address in case the SMTP server cannot forward the syslog message. Note The SMTP server will send a message to the “from” address for the failed deliveries.	<i>Email Address</i>
Step 6 (Optional) Set the “reply to” e-mail address if you want the recipients to respond to a different address than the “from” address.	<i>Email address</i>
Step 7 Verify the configuration.	

```

Console> (enable) set logging callhome enable
Callhome functionality is enabled.
Callhome messages will be sent to the configured destination addresses.
Console> (enable)

```

- page adminjoe@epage.cisco.com using a fragment size of 128 bytes
- email adminboss@cisco.com, and adminjane@cisco.com

```

Console> (enable) set logging callhome destination adminjoe@epage.cisco fragment 128
Included adminjoe@epage.cisco in the table of callhome destination addresses.
Messages will be sent to this address in fragments of 128 bytes.
Console> (enable) set logging callhome destination adminjane@cisco.com
Included adminjane@cisco.com in the table of callhome destination addresses.
Messages will be sent to this address without fragmentation.
Console> (enable) set logging callhome destination adminboss@cisco.com
Included adminboss@cisco.com in the table of callhome destination addresses.
Messages will be sent to this address without fragmentation.
Console> (enable)

```

This example shows how to set the SMTP server with the IP address 172.16.8.19:

```

Console> (enable) set logging callhome smtp-server 172.20.8.16
Included 172.20.8.16 in the table of callhome SMTP servers.
Console> (enable)

```

This example shows how to set the severity to level 3 (critical and error messages):

```

Console> (enable) set logging callhome severity 3
Callhome severity level set to 3
Console> (enable)

```

This example shows how to set the From address to adminjoe@cisco.com:

```

Console> (enable) set logging callhome from adminjoe@cisco.com
From address of callhome messages is set to adminjoe@cisco.com
Console> (enable)

```

This example shows how to set the Reply to address to adminjane@cisco.com:

```

Console> (enable) set logging callhome reply-to adminjane@cisco.com
Reply-To address of callhome messages is set to adminjane@cisco.com
Console> (enable)

```

This example shows how to verify the configuration:

```

Console> (enable) show logging callhome
Callhome Functionality:      enabled
Callhome Severity:          LOG_ERR (3)

SMTP Server
-----
172.20.8.16

Destination Address          Message Size
-----
adminboss@cisco.com         No Fragmentation
adminjane@cisco.com         No Fragmentation
adminjoe@epage.cisco        128 bytes

From: adminjoe@cisco.com
Reply-To: adminjane@cisco.com
Console> (enable)

```

Disabling CallHome

When you disable CallHome, you do not clear any other of the CallHome parameters that are set. You need to clear each parameter individually.

To disable CallHome on your switch, perform this task in privileged mode:

Task	Command
Disable CallHome.	

This example shows how to disable CallHome:

```

Console> (enable) set logging callhome disable
Callhome functionality is disabled.
Callhome messages will not be sent to the configured destination addresses.
Console> (enable)

```

To clear an address from the list of addresses that receive CallHome messages, perform this task in privileged mode:

Task	Command
Clear a destination address from the list of addresses that receive CallHome messages.	<i>Email or Epage Address</i>

This example shows how to clear the destination address adminboss@cisco.com from the list of addresses that receive CallHome messages:

```

Console> (enable) clear logging callhome destination adminboss@cisco.com
Removed adminboss@cisco.com from the table of callhome destination addresses.
Console> (enable)

```

To clear the “from” address, perform this task in privileged mode:

Task	Command
Clear the “from” address.	

This example shows how to clear the “from” address:

```
Console> (enable) clear logging callhome from
Cleared the from address field of callhome messages.
Console> (enable)
```

To clear the “reply to” address, perform this task in privileged mode:

Task	Command
Clear the “reply to” address.	

This example shows how to clear the “reply to” address:

```
Console> (enable) clear logging callhome reply-to
Cleared the reply-to address field of callhome messages.
Console> (enable)
```

To clear an SMTP server from the list of CallHome SMTP servers, perform this task in privileged mode:

Task	Command
Clear an SMTP server.	<i>IP Address</i>

This example shows how to delete the SMTP server 172.20.8.16 from the list of CallHome servers:

```
Console> (enable) clear logging callhome smtp-server 172.20.8.16
Removed 172.20.8.16 from the table of callhome SMTP servers.
Console> (enable)
```

To clear the CallHome severity level, perform this task in privileged mode:

Task	Command
Clear the CallHome severity level.	

This example shows how to clear the CallHome severity level:

```
Console> (enable) clear logging callhome severity
Cleared callhome severity level to its default value of 2 (LOG_CRIT).
Console> (enable)
```