



## Configuring System Message Logs

---

- [Restrictions for Configuring System Message Logs, on page 1](#)
- [Information About Configuring System Message Logs, on page 1](#)
- [How to Configure System Message Logs, on page 4](#)
- [Monitoring and Maintaining System Message Logs, on page 12](#)
- [Configuration Examples for System Message Logs, on page 12](#)

### Restrictions for Configuring System Message Logs

When the **logging discriminator** command is configured, the device may experience memory leak or crash. This usually happens during heavy syslog or debug output. The rate of the memory leak is dependent on the number of logs being produced. In extreme cases, the device may also crash. As a workaround, use the **no logging discriminator** command to disable the logging discriminator.

### Information About Configuring System Message Logs

#### System Message Logging

By default, a switch sends the output from system messages and **debug** privileged EXEC commands to a logging process. Stack members can trigger system messages. A stack member that generates a system message appends its hostname in the form of hostname-n, where n is a switch range from 1 to 8, and redirects the output to the logging process on the active switchstack's active switch. Though the active switchstack's active switch is a stack member, it does not append its hostname to system messages. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the active consoles after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, see the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on a standalone switch, and in the case of a switch stack, on the active switchstack's active switch. If a standalone switch or the stack master fails, the log is lost unless you had saved it to flash memory.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet, through the console port, or through the Ethernet management port. In a switch stack, all stack member consoles provide the same console output.



**Note** The syslog format is compatible with 4.3 BSD UNIX.

## System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Depending on the switch, messages appear in one of these formats:

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

The part of the message preceding the percent sign depends on the setting of these global configuration commands:

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime [localtime] [msec] [show-timezone]**
- **service timestamps log uptime**

**Table 1: System Log Message Elements**

Element	Description
<i>seq no:</i>	Stamps log messages with a sequence number only if the <b>service sequence-numbers</b> global configuration command is configured.
<i>timestamp</i> formats: <i>mm/dd h h:mm:ss</i> or <i>hh:mm:ss</i> (short uptime) or <i>d h</i> (long uptime)	Date and time of the message or event. This information appears only if the <b>service timestamps log [datetime   log]</b> global configuration command is configured.
<i>facility</i>	The facility to which the message refers (for example, SNMP, SYS, and so forth).

Element	Description
<i>severity</i>	Single-digit code from 0 to 7 that is the severity of the message.
<i>MNEMONIC</i>	Text string that uniquely describes the message.
<i>description</i>	Text string containing detailed information about the event being reported.
<i>hostname-n</i>	Hostname of a stack member and its switch number in the stack. Though the active switchstack's active switch is a stack member, it does <i>not</i> append its hostname to system messages.

## Default System Message Logging Settings

Table 2: Default System Message Logging Settings

Feature	Default Setting
System message logging to the console	Enabled.
Console severity	Debugging.
Logging file configuration	No filename specified.
Logging buffer size	4096 bytes.
Logging history size	1 message.
Time stamps	Disabled.
Synchronous logging	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Server facility	Local7
Server severity	Informational.

## Enabling Syslog Trap Messages

You can enable Syslog traps using the **snmp-server enable traps syslog** command.

After enabling Syslog traps, you have to specify the trap message severity. Use the **logging snmp-trap** command to specify the trap level. By default, the command enables severity 0 to 4. To enable all the severity level, configure the **logging snmp-trap 0 7** command.

To enable individual trap levels, configure the following commands:

- **logging snmp-trap emergencies**: Enables only severity 0 traps.

- **logging snmp-trap alert** Enables only severity 1 traps.

Note that, along with the Syslog traps, the Syslog history should also be applied. Without this configuration, Syslog traps are not sent.

Use the **logging history informational** command to enable the Syslog history.

## How to Configure System Message Logs

### Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

This task is optional.

#### SUMMARY STEPS

1. **configure terminal**
2. **logging buffered** *[size]*
3. **logging** *host*
4. **logging file flash:** *filename* *[max-file-size* *[min-file-size]]* *[severity-level-number | type]*
5. **end**
6. **terminal monitor**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging buffered</b> <i>[size]</i> <b>Example:</b> Switch(config)# <b>logging buffered 8192</b>	<p>Logs messages to an internal buffer on the switch or on a standalone switch or, in the case of a switch stack, on the active switch. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes.</p> <p>If a standalone switch or the active switch fails, the log file is lost unless you previously saved it to flash memory. See Step 4.</p> <p><b>Note</b> Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the <b>show memory</b> privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should <i>not</i> be set to this amount.</p>

	Command or Action	Purpose
Step 3	<p><b>logging</b> <i>host</i></p> <p><b>Example:</b></p> <pre>Switch(config)# logging 125.1.1.100</pre>	<p>Logs messages to a UNIX syslog server host.</p> <p><i>host</i> specifies the name or IP address of the host to be used as the syslog server.</p> <p>To build a list of syslog servers that receive logging messages, enter this command more than once.</p>
Step 4	<p><b>logging file flash:</b> <i>filename</i> [<i>max-file-size</i> [<i>min-file-size</i>]] [<i>severity-level-number</i>   <i>type</i>]</p> <p><b>Example:</b></p> <pre>Switch(config)# logging file flash:log_msg.txt 40960 4096 3</pre>	<p>Stores log messages in a file in flash memory on a standalone switch or, in the case of a switch stack, on the active switch.</p> <ul style="list-style-type: none"> <li>• <i>filename</i>—Enters the log message filename.</li> <li>• (Optional) <b>max-file-size</b> —Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes.</li> <li>• (Optional) <i>min-file-size</i>—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes.</li> <li>• (Optional) <i>severity-level-number</i>   <i>type</i>—Specifies either the logging severity level or the logging type. The severity range is 0 to 7.</li> </ul>
Step 5	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>
Step 6	<p><b>terminal monitor</b></p> <p><b>Example:</b></p> <pre>Switch# terminal monitor</pre>	<p>Logs messages to a nonconsole terminal during the current session.</p> <p>Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.</p>

## Synchronizing Log Messages

You can synchronize unsolicited messages and **debug** privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or is printed. Unsolicited messages and **debug** command output appears on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.

This task is optional.

## SUMMARY STEPS

1. **configure terminal**
2. **line** [**console** | **vty**] *line-number* [*ending-line-number*]
3. **logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]
4. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>line</b> [ <b>console</b>   <b>vty</b> ] <i>line-number</i> [ <i>ending-line-number</i> ] <b>Example:</b> <pre>Switch(config)# line console</pre>	<p>Specifies the line to be configured for synchronous logging of messages.</p> <ul style="list-style-type: none"> <li>• <b>console</b>—Specifies configurations that occur through the switch console port or the Ethernet management port.</li> <li>• <b>line vty</b> <i>line-number</i>—Specifies which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15.</li> </ul> <p>You can change the setting of all 16 vty lines at once by entering:</p> <pre>line vty 0 15</pre> <p>You can also change the setting of the single vty line being used for your current connection. For example, to change the setting for vty line 2, enter:</p> <pre>line vty 2</pre> <p>When you enter this command, the mode changes to line configuration.</p>
<b>Step 3</b>	<b>logging synchronous</b> [ <b>level</b> [ <i>severity-level</i>   <b>all</b> ]   <b>limit</b> <i>number-of-buffers</i> ] <b>Example:</b> <pre>Switch(config)# logging synchronous level 3 limit 1000</pre>	<p>Enables synchronous logging of messages.</p> <ul style="list-style-type: none"> <li>• (Optional) <b>level</b> <i>severity-level</i>—Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• (Optional) <b>level all</b>—Specifies that all messages are printed asynchronously regardless of the severity level.</li> <li>• (Optional) <b>limit number-of-buffers</b>—Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The range is 0 to 2147483647. The default is 20.</li> </ul>
<b>Step 4</b>	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.

## Disabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press **Return**.

To reenable message logging after it has been disabled, use the **logging on** global configuration command.

This task is optional.

### SUMMARY STEPS

1. **configure terminal**
2. **no logging console**
3. **end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>no logging console</b> <b>Example:</b>	Disables message logging.

	Command or Action	Purpose
	Switch(config)# <code>no logging console</code>	
<b>Step 3</b>	<b>end</b> <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode.

## Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time-stamped.

This task is optional.

### SUMMARY STEPS

- 1. configure terminal**
- Use one of these commands:
  - `service timestamps log uptime`
  - `service timestamps log datetime[msec | localtime | show-timezone]`
- 3. end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	Use one of these commands: <ul style="list-style-type: none"> <li>• <code>service timestamps log uptime</code></li> <li>• <code>service timestamps log datetime[msec   localtime   show-timezone]</code></li> </ul> <b>Example:</b> Switch(config)# <code>service timestamps log uptime</code> or Switch(config)# <code>service timestamps log datetime</code>	Enables log time stamps. <ul style="list-style-type: none"> <li>• <b>log uptime</b>—Enables time stamps on log messages, showing the time since the system was rebooted.</li> <li>• <b>log datetime</b>—Enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.</li> </ul>
<b>Step 3</b>	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.



	Command or Action	Purpose
	<code>Switch(config)# end</code>	

## Enabling and Disabling Sequence Numbers in Log Messages

If there is more than one log message with the same time stamp, you can display messages with sequence numbers to view these messages. By default, sequence numbers in log messages are not displayed.

This task is optional.

### SUMMARY STEPS

1. `configure terminal`
2. `service sequence-numbers`
3. `end`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <code>Switch# configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>service sequence-numbers</b> <b>Example:</b> <code>Switch(config)# service sequence-numbers</code>	Enables sequence numbers.
<b>Step 3</b>	<b>end</b> <b>Example:</b> <code>Switch(config)# end</code>	Returns to privileged EXEC mode.

## Defining the Message Severity Level

Limit messages displayed to the selected device by specifying the severity level of the message.

This task is optional.

### SUMMARY STEPS

1. `configure terminal`
2. `logging console level`

3. **logging monitor** *level*
4. **logging trap** *level*
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>logging console</b> <i>level</i> <b>Example:</b> Switch(config)# <b>logging console 3</b>	Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.
<b>Step 3</b>	<b>logging monitor</b> <i>level</i> <b>Example:</b> Switch(config)# <b>logging monitor 3</b>	Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.
<b>Step 4</b>	<b>logging trap</b> <i>level</i> <b>Example:</b> Switch(config)# <b>logging trap 3</b>	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.

## Limiting Syslog Messages Sent to the History Table and to SNMP

This task explains how to limit syslog messages that are sent to the history table and to SNMP.

This task is optional.

### SUMMARY STEPS

1. **configure terminal**
2. **logging history** *level*
3. **logging history size** *number*
4. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 2	<b>logging history level</b> <b>Example:</b> <pre>Switch(config)# logging history 3</pre>	Changes the default level of syslog messages stored in the history file and sent to the SNMP server.  By default, <b>warnings</b> , <b>errors</b> , <b>critical</b> , <b>alerts</b> , and <b>emergencies</b> messages are sent.
Step 3	<b>logging history size number</b> <b>Example:</b> <pre>Switch(config)# logging history size 200</pre>	Specifies the number of syslog messages that can be stored in the history table.  The default is to store one message. The range is 0 to 500 messages.
Step 4	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.

## Logging Messages to a UNIX Syslog Daemon

This task is optional.



**Note** Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

### Before you begin

- Log in as root.
- Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server.

### SUMMARY STEPS

1. Add a line to the file `/etc/syslog.conf`.
2. Enter these commands at the UNIX shell prompt.
3. Make sure the syslog daemon reads the new changes.

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	Add a line to the file /etc/syslog.conf. <b>Example:</b>  <code>local7.debug /usr/adm/logs/cisco.log</code>	<ul style="list-style-type: none"> <li>• <b>local7</b>—Specifies the logging facility.</li> <li>• <b>debug</b>—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it.</li> </ul>
<b>Step 2</b>	Enter these commands at the UNIX shell prompt. <b>Example:</b>  <code>\$ touch /var/log/cisco.log</code> <code>\$ chmod 666 /var/log/cisco.log</code>	Creates the log file. The syslog daemon sends messages at this level or at a more severe level to this file.
<b>Step 3</b>	Make sure the syslog daemon reads the new changes. <b>Example:</b>  <code>\$ kill -HUP `cat /etc/syslog.pid`</code>	For more information, see the <b>man syslog.conf</b> and <b>man syslogd</b> commands on your UNIX system.

## Monitoring and Maintaining System Message Logs

### Monitoring Configuration Archive Logs

Command	Purpose
<code>show archive log config {all   number [end-number]   user username [session number] number [end-number]   statistics} [provisioning]</code>	Displays the entire configuration log or the log for specified parameters.

## Configuration Examples for System Message Logs

### Example: Switch System Message

This example shows a partial switch system message on a switch:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down 2
```

```
*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

