



# Configuring System Message Logs

---

This module contains the following topics:

- [Finding Feature Information, page 1](#)
- [Information About Configuring System Message Logs, page 2](#)
- [How to Configure System Message Logs, page 4](#)
- [Monitoring and Maintaining System Message Logs, page 12](#)
- [Configuration Examples for System Message Logs, page 13](#)
- [Additional References for System Message Logs, page 13](#)
- [Additional References for System Message Logs, page 15](#)
- [Feature History and Information For System Message Logs, page 16](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Related Topics

[Feature History and Information for Troubleshooting Software Configuration](#)

# Information About Configuring System Message Logs

## 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 the **service sequence-numbers**, **service timestamps log datetime**, **service timestamps log datetime [localtime] [msec] [show-timezone]**, or **service timestamps log uptime** global configuration command.

**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).
<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 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.

## Syslog Message Limits

If you enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels are stored in the history table even if syslog traps are not enabled.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

The history table lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, *emergencies* equal 1, not 0, and *critical* equals 3, not 2.

# 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</b> <b>8192</b>	Logs messages to an internal buffer on the switch or on a standalone switch or, in the case of a switch stack, on the . The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes.  If a standalone switch or the fails, the log file is lost unless you previously saved it to flash memory. See Step 4.  <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.
Step 3	<b>logging</b> <i>host</i>  <b>Example:</b> Switch(config)# <b>logging</b> <b>125.1.1.100</b>	Logs messages to a UNIX syslog server host.  <i>host</i> specifies the name or IP address of the host to be used as the syslog server.  To build a list of syslog servers that receive logging messages, enter this command more than once.

	Command or Action	Purpose
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 .</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
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>line [console   vty] line-number [ending-line-number]</b>  <b>Example:</b> Switch(config)# <b>line console</b>	Specifies the line to be configured for synchronous logging of messages. <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 line-number</b>—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:  line vty 0 15</p> <p>Or you can 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:  line vty 2</p> <p>When you enter this command, the mode changes to line configuration.</p>
Step 3	<b>logging synchronous [level [severity-level   all]   limit number-of-buffers]</b>  <b>Example:</b> Switch(config)# <b>logging synchronous level 3 limit 1000</b>	Enables synchronous logging of messages. <ul style="list-style-type: none"> <li>• (Optional) <b>level severity-level</b>—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> <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>
Step 4	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	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 re-enable 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
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>no logging console</b>  <b>Example:</b> Switch(config)# <b>no logging console</b>	Disables message logging.
Step 3	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	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**
2. 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# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Use one of these commands: <ul style="list-style-type: none"> <li>• <b>service timestamps log uptime</b></li> <li>• <b>service timestamps log datetime[msec   localtime   show-timezone]</b></li> </ul> <b>Example:</b> Switch(config)# <b>service timestamps log uptime</b> or Switch(config)# <b>service timestamps log datetime</b>	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> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.

## 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> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>service sequence-numbers</b>  <b>Example:</b> Switch(config)# <b>service sequence-numbers</b>	Enables sequence numbers.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	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 level</b>  <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 level</b>  <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 level</b>  <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> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging history level</b>  <b>Example:</b> Switch(config)# <b>logging history 3</b>	Changes the default level of syslog messages stored in the history file and sent to the SNMP server.  By default, <b>warnings, errors, critical, alerts, and emergencies</b> messages are sent.
Step 3	<b>logging history size number</b>  <b>Example:</b> Switch(config)# <b>logging history size 200</b>	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> Switch(config)# <b>end</b>	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**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	Add a line to the file <code>/etc/syslog.conf</code> .  <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

<b>Command</b>	<b>Purpose</b>
<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

## Stacking System Message: Example

This example shows a partial switch system message for and a stack member (hostname *Switch-2*):

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, 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 GigabitEthernet1/0/1, 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)

00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
state to down 2 (Switch-2)
```

## Switch System Message: Example

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

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell, 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)
```

## Additional References for System Message Logs

### Related Documents

Related Topic	Document Title
Command reference	<i>System Management Command Reference (Catalyst 3850 Switches)</i>

Related Topic	Document Title
Platform-independent command references	<i>Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</i>
Platform-independent configuration information	<i>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</i>  <i>IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

# Additional References for System Message Logs

## Related Documents

Related Topic	Document Title
System message log commands	
Platform-independent command references	<i>Cisco IOS 15.3M&amp;T Command References</i>
Platform-independent configuration information	<i>Cisco IOS 15.3M&amp;T Configuration Guides</i>

## Standards and RFCs

Standard/RFC	Title
None	—

## MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

**Feature History and Information For System Message Logs**

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.