



## System Message Logging

---

This module describes how to configure system message logging on your wireless device in the following sections:

- [Understanding System Message Logging, page 1](#)
- [Configuring System Message Logging, page 2](#)
- [Displaying the Logging Configuration, page 11](#)



**Note**

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.4*.

---

## Understanding System Message Logging

By default, wireless devices send the output from system messages and **debug** privileged EXEC commands to a logging process. 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.



**Note**

---

The syslog format is compatible with 4.3 BSD UNIX.

---

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 are displayed on the console 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 console and each of the destinations. You can timestamp log messages or set the syslog source address to enhance real-time debugging and management.

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



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Configuring System Message Logging

This section describes how to configure system message logging in the following sections:

- [System Log Message Format, page 2](#)
- [Default System Message Logging Configuration, page 3](#)
- [Disabling and Enabling Message Logging, page 4](#)
- [Setting the Message Display Destination Device, page 4](#)
- [Enabling and Disabling Time Stamps on Log Messages, page 5](#)
- [Enabling and Disabling Sequence Numbers in Log Messages, page 6](#)
- [Defining the Message Severity Level, page 6](#)
- [Limiting Syslog Messages Sent to the History Table and to SNMP, page 8](#)
- [Setting a Logging Rate Limit, page 9](#)
- [Configuring UNIX Syslog Servers, page 9](#)

## System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or timestamp information, if configured. Messages are displayed in this format:

*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](#) describes the elements of syslog messages.

**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.  For more information, see the “ <a href="#">Enabling and Disabling Sequence Numbers in Log Messages</a> ” section on page 6.
<i>timestamp</i> formats: <i>mm/dd hh: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.  For more information, see the “ <a href="#">Enabling and Disabling Time Stamps on Log Messages</a> ” section on page 5.
<i>facility</i>	The facility to which the message refers (for example, SNMP, SYS, and so forth). A facility can be a hardware device, a protocol, or a module of the system software. It denotes the source or the cause of the system message.
<i>severity</i>	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see <a href="#">Table 3</a> on page 7.

**Table 1** System Log Message Elements (continued)

Element	Description
<i>MNEMONIC</i>	Text string that uniquely describes the message.
<i>description</i>	Text string containing detailed information about the event being reported.

The following example shows a partial access point system message:

```
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)
```

## Default System Message Logging Configuration

Table 2 shows the default system message logging configuration.

**Table 2** Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled
Console severity	Debugging (and numerically lower levels; see <a href="#">Table 3 on page 7</a> )
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 (see <a href="#">Table 4 on page 10</a> )
Server severity	Informational (and numerically lower levels; see <a href="#">Table 3 on page 7</a> )

## Disabling and Enabling 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.

To disable message logging, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>no logging on</b>	Disables message logging.
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b> or <b>show logging</b>	Verifies your entries.

Disabling the logging process can slow down the access point because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages are displayed 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. For more information, see the [“Enabling and Disabling Time Stamps on Log Messages”](#) section on page 5.

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

## Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. To specify the locations that receive messages, use one or more of the following commands, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging buffered</b> <i>[size]</i> <i>[level]</i>	Logs messages to an internal buffer. The default buffer size is 4096. The range is 4096 to 2147483647 bytes. Levels include emergencies 0, alerts 1, critical 2, errors 3, warnings 4, notifications 5, informational 6, and debugging 7.  <b>Note</b> Do not make the buffer size too large because the access point could run out of memory for other tasks. Use the <b>show memory</b> command in privileged EXEC mode to view the free processor memory on the access point; however, this processor memory value is the maximum available, and you should <i>not</i> set the buffer size to this amount.

	Command	Purpose
Step 3	<b>logging</b> <i>host</i>	Logs messages to a UNIX syslog server host.  For <i>host</i> , specify 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.  For complete syslog server configuration steps, see the “ <a href="#">Configuring UNIX Syslog Servers</a> ” section on page 9.
Step 4	<b>end</b>	Returns to privileged EXEC mode.
Step 5	<b>terminal monitor</b>	Logs messages to a non-console terminal during the current session.  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.

The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** command, in privileged EXEC mode. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the **clear logging** command, in privileged EXEC mode.

To disable logging to the console, use the **no logging console** command in global configuration mode. To disable logging to a file, use the **no logging file** [*severity-level-number* | *type*] command in global configuration mode.

## Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time stamped.

To enable timestamping of log messages, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>service timestamps log uptime</b> or <b>service timestamps log datetime</b> [msec] [localtime] [show-timezone]	Enables log timestamps.  The first command enables timestamps on log messages, showing the time since the system was rebooted.  The second command enables timestamps on log messages. Depending on the options selected, the timestamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.
Step 3	<b>end</b>	Returns to privileged EXEC mode.

To disable timestamps for both debug and log messages, use the **no service timestamps** command in mode global configuration.

The following example shows part of a logging display with the **service timestamps log datetime** command enabled:

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

The following example shows part of a logging display with the **service timestamps log uptime** command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

## Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same timestamp, you can display messages with sequence numbers so that you can unambiguously refer to a single message. By default, sequence numbers in log messages are not displayed.

To enable sequence numbers in log messages, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>service sequence-numbers</b>	Enables sequence numbers.
Step 3	<b>end</b>	Returns to privileged EXEC mode.

To disable sequence numbers, use the **no service sequence-numbers** global configuration command.

The following example shows part of a logging display with sequence numbers enabled:

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

## Defining the Message Severity Level

You can limit messages that are displayed to the selected device by specifying the severity level of the message. [Table 3](#) describes the severity level.

To define the message severity level, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging console <i>level</i></b>	Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see <a href="#">Table 3 on page 7</a> ).
Step 3	<b>logging monitor <i>level</i></b>	Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see <a href="#">Table 3 on page 7</a> ).

	Command	Purpose
Step 4	<b>logging trap</b> <i>level</i>	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see <a href="#">Table 3 on page 7</a> ). For complete steps for configuring syslog servers, see the “ <a href="#">Configuring UNIX Syslog Servers</a> ” section on page 9.
Step 5	<b>end</b>	Returns to privileged EXEC mode.

**Note**

Specifying a *level* causes messages at that level and numerically lower levels to be displayed at the destination.

To disable logging to the console, use the **no logging console** command in global configuration mode. To disable logging to a terminal other than the console, use the **no logging monitor** command in global configuration mode. To disable logging to syslog servers, use the **no logging trap** command in global configuration mode.

[Table 3](#) describes the severity *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

**Table 3** Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
<b>emergencies</b>	0	System unstable	LOG_EMERG
<b>alerts</b>	1	Immediate action needed	LOG_ALERT
<b>critical</b>	2	Critical conditions	LOG_CRIT
<b>errors</b>	3	Error conditions	LOG_ERR
<b>warnings</b>	4	Warning conditions	LOG_WARNING
<b>notifications</b>	5	Normal but significant condition	LOG_NOTICE
<b>informational</b>	6	Informational messages only	LOG_INFO
<b>debugging</b>	7	Debugging messages	LOG_DEBUG

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**: these types of messages mean that the functionality of the access point is affected.
- Output from the **debug** commands, displayed at the **debugging** level: debug commands are typically used only by the Technical Assistance Center (TAC).
- Interface up or down transitions and system restart messages, displayed at the **notifications** level: this message is only for information; access point functionality is not affected.
- Reload requests and low-process stack messages, displayed at the **informational** level: this message is only for information; access point functionality is not affected.

**Note**

Authentication request log messages are not logged on to a syslog server. This feature is not supported on Cisco Aironet access points.

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

If you have enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** command, you can change the level of messages sent and stored in the access point history table. You can also 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 (see [Table 3 on page 7](#)) are stored in the history table even if syslog traps are not enabled.

To change the level and history table size defaults, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging history level<sup>1</sup></b>	Changes the default level of syslog messages stored in the history file and sent to the SNMP server.  See <a href="#">Table 3 on page 7</a> for a list of <i>level</i> keywords.  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>	Specifies the number of syslog messages that can be stored in the history table.  The default is to store one message. The range is 1 to 500 messages.
Step 4	<b>end</b>	Returns to privileged EXEC mode.

1. [Table 3](#) 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.

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

To return the logging of syslog messages to the default level, use the **no logging history** command in global configuration mode. To return the number of messages in the history table to the default value, use the **no logging history size** command in global configuration mode.

## Setting a Logging Rate Limit

You can set a limit on the number of messages that the access point logs per second. You can enable the limit for all messages or for messages sent to the console, and you can specify that messages of a specific severity are exempt from the limit.

To enable a logging rate limit, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging rate-limit</b> <i>seconds</i> [all   console] [except <i>severity</i> ]	Enables a logging rate limit in seconds. <ul style="list-style-type: none"> <li>(Optional) Apply the limit to all logging or only to messages logged to the console.</li> <li>(Optional) Exempt a specific severity from the limit.</li> </ul>
Step 3	<b>end</b>	Returns to privileged EXEC mode.

To disable the rate limit, use the **no logging rate-limit** command in global configuration mode.

## Configuring UNIX Syslog Servers

The next sections describe how to configure the 4.3 BSD UNIX server syslog daemon and define the UNIX system logging facility.

### Logging Messages to a UNIX Syslog Daemon

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



#### 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 determine what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

**Step 1** Add a line such as the following to the file `/etc/syslog.conf`:

```
local7.debug /usr/adm/logs/cisco.log
```

The **local7** keyword specifies the logging facility to be used; see [Table 4 on page 10](#) for information on the facilities. The **debug** keyword specifies the syslog level; see [Table 3 on page 7](#) for information on the severity levels. The syslog daemon sends messages at this level or at a greater severity level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

**Step 2** Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /usr/adm/log/cisco.log
$ chmod 666 /usr/adm/log/cisco.log
```

**Step 3** Ensure the syslog daemon reads the new changes by entering this command:

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

For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

## Configuring the UNIX System Logging Facility

When sending system log messages to an external device, you can cause the access point to identify its messages as originating from any of the UNIX syslog facilities.

To configure UNIX system facility message logging, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging host</b>	Logs messages to a UNIX syslog server host by entering its IP address. To build a list of syslog servers that receive logging messages, enter this command more than once.
Step 3	<b>logging trap level</b>	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and lower. See <a href="#">Table 3 on page 7</a> for <i>level</i> keywords.
Step 4	<b>logging facility facility-type</b>	Configures the syslog facility. See <a href="#">Table 4 on page 10</a> for <i>facility-type</i> keywords. The default is <b>local7</b> .
Step 5	<b>end</b>	Returns to privileged EXEC mode.

To remove a syslog server, use the **no logging host** command in global configuration mode, and specify the syslog server IP address. To disable logging to syslog servers, enter the **no logging trap** command in global configuration mode.

[Table 4](#) lists the 4.3 BSD UNIX system facilities that the Cisco IOS software supports. For more information about these facilities, consult the operator's manual for your UNIX operating system.

**Table 4** Logging Facility-Type Keywords

Facility Type Keyword	Description
<b>auth</b>	Authorization system
<b>cron</b>	Cron facility
<b>daemon</b>	System daemon
<b>kern</b>	Kernel
<b>local0-7</b>	Locally defined messages
<b>lpr</b>	Line printer system
<b>mail</b>	Mail system
<b>news</b>	USENET news

**Table 4** Logging Facility-Type Keywords (continued)

Facility Type Keyword	Description
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

## Displaying the Logging Configuration

To display the current logging configuration and the contents of the log buffer, use the **show logging** command in privileged EXEC mode. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

To display the logging history file, use the **show logging history** command in privileged EXEC mode.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

