



Configuring System Message Logging

This chapter describes how to configure system message logging on your access point.



Note

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

Understanding System Message Logging

By default, access points 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 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 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.

Configuring System Message Logging

This section describes how to configure system message logging. It contains this configuration information:

- [System Log Message Format, page 25-2](#)
- [Default System Message Logging Configuration, page 25-3](#)
- [Disabling and Enabling Message Logging, page 25-4](#)
- [Setting the Message Display Destination Device, page 25-5](#)
- [Enabling and Disabling Timestamps on Log Messages, page 25-6](#)
- [Enabling and Disabling Sequence Numbers in Log Messages, page 25-6](#)
- [Defining the Message Severity Level, page 25-7](#)
- [Limiting Syslog Messages Sent to the History Table and to SNMP, page 25-8](#)
- [Setting a Logging Rate Limit, page 25-9](#)
- [Configuring the System Logging Facility, page 25-10](#)

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 25-1](#) describes the elements of syslog messages.

Table 25-1 **System Log Message Elements**

| Element | Description |
|--|--|
| <i>seq no:</i> | Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. For more information, see the “Enabling and Disabling Sequence Numbers in Log Messages” section on page 25-6 . |
| <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 service timestamps log [datetime log] global configuration command is configured. For more information, see the “Enabling and Disabling Timestamps on Log Messages” section on page 25-6 . |
| <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 Table 25-3 on page 25-8 . |
| <i>MNEMONIC</i> | Text string that uniquely describes the message. |
| <i>description</i> | Text string containing detailed information about the event being reported. |

This example shows a partial access point system message:

```
*Mar 1 00:00:29.219: %LINK-6-UPDOWN: Interface GigabitEthernet0, changed state to up
*Mar 1 00:00:29.335: Starting Ethernet promiscuous mode
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
*Apr 13 15:29:28.007: %SYS-5-RESTART: System restarted --
```

Default System Message Logging Configuration

[Table 25-2](#) shows the default system message logging configuration.

Table 25-2 **Default System Message Logging Configuration**

| Feature | Default Setting |
|---------------------------------------|--|
| System message logging to the console | Enabled |
| Console severity | Debugging (and numerically lower levels; see Table 25-3 on page 25-8) |
| Logging buffer size | 4096 bytes |
| Logging history size | 1 message |
| Timestamps | Disabled |

Table 25-2 *Default System Message Logging Configuration (continued)*

| Feature | Default Setting |
|--------------------------|--|
| Synchronous logging | Disabled |
| Logging server | Disabled |
| Syslog server IP address | None configured |
| Server facility | Local7 (see Table 25-4 on page 25-10) |
| Server severity | Informational (and numerically lower levels; see Table 25-3 on page 25-8) |

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.

Beginning in privileged EXEC mode, follow these steps to disable message logging:

| | Command | Purpose |
|--------|---|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | no logging on | Disable message logging. |
| Step 3 | end | Return to privileged EXEC mode. |
| Step 4 | show running-config or show logging | Verify your entries. |
| Step 5 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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 Timestamps on Log Messages](#)” section on page 25-6.

To re-enable 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. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages:

| | Command | Purpose |
|--------|--|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | logging buffered <i>[size]</i> <i>[level]</i> | Log 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. Note Do not make the buffer size too large because the access point could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the access point; however, this value is the maximum available, and you should <i>not</i> set the buffer size to this amount. |
| Step 3 | logging <i>host</i> | Log messages to a 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 “Configuring the System Logging Facility” section on page 25-10. |
| Step 4 | end | Return to privileged EXEC mode. |
| Step 5 | terminal monitor | Log 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. |
| Step 6 | show running-config | Verify your entries. |
| Step 7 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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** privileged EXEC command. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the **clear logging** privileged EXEC command.

To disable logging to the console, use the **no logging console** global configuration command.

Enabling and Disabling Timestamps on Log Messages

By default, log messages are not timestamped.

Beginning in privileged EXEC mode, follow these steps to enable timestamping of log messages:

| | Command | Purpose |
|--------|---|--|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | service timestamps log uptime or service timestamps log datetime [msec] [localtime] [show-timezone] | Enable 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 | end | Return to privileged EXEC mode. |
| Step 4 | show running-config | Verify your entries. |
| Step 5 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

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

This example shows part of a logging display with the **service timestamps log uptime** global configuration command enabled:

```
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down
```

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.

Beginning in privileged EXEC mode, follow these steps to enable sequence numbers in log messages:

| | Command | Purpose |
|--------|---|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | service sequence-numbers | Enable sequence numbers. |
| Step 3 | end | Return to privileged EXEC mode. |
| Step 4 | show running-config | Verify your entries. |
| Step 5 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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

This 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 displayed to the selected device by specifying the severity level of the message, which are described in [Table 25-3](#).

Beginning in privileged EXEC mode, follow these steps to define the message severity level:

| | Command | Purpose |
|--------|---|--|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | logging console <i>level</i> | Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 25-3 on page 25-8). |
| Step 3 | logging monitor <i>level</i> | Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 25-3 on page 25-8). |
| Step 4 | logging trap <i>level</i> | Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 25-3 on page 25-8). For complete syslog server configuration steps, see the “ Configuring the System Logging Facility ” section on page 25-10. |
| Step 5 | end | Return to privileged EXEC mode. |
| Step 6 | show running-config or show logging | Verify your entries. |
| Step 7 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |



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

Table 25-3 describes the *level* keywords. It also lists the corresponding syslog definitions from the most severe level to the least severe level.

Table 25-3 Message Logging Level Keywords

| Level Keyword | Level | Description | Syslog Definition |
|----------------------|-------|----------------------------------|-------------------|
| emergencies | 0 | System unstable | LOG_EMERG |
| alerts | 1 | Immediate action needed | LOG_ALERT |
| critical | 2 | Critical conditions | LOG_CRIT |
| errors | 3 | Error conditions | LOG_ERR |
| warnings | 4 | Warning conditions | LOG_WARNING |
| notifications | 5 | Normal but significant condition | LOG_NOTICE |
| informational | 6 | Informational messages only | LOG_INFO |
| debugging | 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.
- 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** global configuration 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 25-3 on page 25-8) are stored in the history table even if syslog traps are not enabled.

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

| | Command | Purpose |
|--------|--|--|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | logging history <i>level</i> ¹ | Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 25-3 on page 25-8 for a list of <i>level</i> keywords. By default, warnings , errors , critical , alerts , and emergencies messages are sent. |
| Step 3 | logging history size <i>number</i> | Specify 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 | end | Return to privileged EXEC mode. |
| Step 5 | show running-config | Verify your entries. |
| Step 6 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

1. [Table 25-3](#) 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** global configuration command), 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** global configuration command. To return the number of messages in the history table to the default value, use the **no logging history size** global configuration command.

Setting a Logging Rate Limit

You can enable 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.

Beginning in privileged EXEC mode, follow these steps to enable a logging rate limit:

| | Command | Purpose |
|--------|--|--|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | logging rate-limit <i>seconds</i> [all console] [except <i>severity</i>] | Enable a logging rate limit in seconds. <ul style="list-style-type: none"> (Optional) Apply the limit to all logging or only to messages logged to the console. (Optional) Exempt a specific severity from the limit. |
| Step 3 | end | Return to privileged EXEC mode. |
| Step 4 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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

Configuring the 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 syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure system facility message logging:

| | Command | Purpose |
|--------|--|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | logging <i>host</i> | Log messages to a 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 | logging trap <i>level</i> | Limit messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 25-3 on page 25-8 for <i>level</i> keywords. |
| Step 4 | logging facility <i>facility-type</i> | Configure the syslog facility. See Table 25-4 on page 25-10 for <i>facility-type</i> keywords. The default is local7 . |
| Step 5 | end | Return to privileged EXEC mode. |
| Step 6 | show running-config | Verify your entries. |
| Step 7 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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

[Table 25-4](#) lists the system facilities supported by the Cisco IOS software. For more information about these facilities, consult the operator's manual for your syslog server.

Table 25-4 **Logged Facility-Type Keywords**

| Facility Type Keyword | Description |
|-----------------------|--------------------------|
| auth | Authorization system |
| cron | Cron facility |
| daemon | System daemon |
| kern | Kernel |
| local0-7 | Locally defined messages |
| lpr | Line printer system |
| mail | Mail system |
| news | USENET news |
| sys9 | System use |
| sys10 | System use |
| sys11 | System use |
| sys12 | System use |

Table 25-4 **Logging Facility-Type Keywords (continued)**

| Facility Type Keyword | Description |
|-----------------------|--------------------------|
| 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** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference* guide.

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

■ Displaying the Logging Configuration