# Embedded Syslog Manager Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

**First Published:** January 11, 2013

**Last Modified:** January 11, 2013

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

# A through Z Commands

# logging buffered filtered

To enable Embedded Syslog Manager (ESM) filtered system message logging to the standard syslog buffer, use the **logging buffered filtered** command in global configuration mode. To disable all logging to the buffer and return the size of the buffer to the default, use the **no** form of this command.

**logging buffered filtered** [ *severity-level* ]

**no logging buffered filtered**

## Syntax Description

| | |
|---|---|
| *severity-level* | (Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword):<br>[**0** \| **emergencies**]—System is unusable<br>[**1** \| **alerts**] —Immediate action needed<br>[**2** \| **critical**]—Critical conditions<br>[**3** \| **errors**]—Error conditions<br>[**4** \| **warnings**]—Warning conditions<br>[**5** \| **notifications**]—Normal but significant conditions<br>[**6** \| **informational**]—Informational messages<br>[**7** \| **debugging**]—Debugging messages<br>The default severity level varies by platform but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged. |

## Command Default

Logging to the buffer is enabled.

ESM filtering of system logging messages sent to the buffer is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.3(2)XE | This command was integrated into Cisco IOS Release 12.3(2)XE. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |
| 12.2(50)SY | This command was integrated into Cisco IOS Release 12.2(50)SY. |

## Usage Guidelines

If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging buffered filtered** command.

Standard logging is enabled by default, but filtering by the ESM is disabled by default.

ESM uses syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before filtered output can be sent to the buffer.

When ESM filtering is enabled, all messages sent to the buffer have the configured syslog filter modules applied. To return to standard logging to the buffer, use the plain form of the **logging buffered** command (without the **filtered** keyword). To disabled all logging to the buffer, use the **no logging buffered** command, with or without the **filtered** keyword.

The buffer is circular, so newer messages overwrite older messages as the buffer is filled. To change the size of the buffer, use the **logging buffered** *buffer-size* command, then issue the **logging buffered filtered** command to start (or restart) filtered logging.

To display the messages that are logged in the buffer, use the **show logging** command in EXEC mode. The first message displayed is the oldest message in the buffer.

## Examples

The following example shows how to enable ESM filtered logging to the buffer:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging buffer filtered
```

## Related Commands

| Command | Description |
|---|---|
| **clear logging** | Clears all messages from the system message logging (syslog) buffer. |
| **logging buffered** | Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer. |

| Command | Description |
|---|---|
| **logging filter** | Specifies the name and location of a syslog filter module to be applied to generated system logging messages. |
| **logging on** | Globally controls (enables or disables) system message logging. |
| **show logging** | Displays the state of system message logging, followed by the contents of the logging buffer. |

# logging console filtered

To enable Embedded Syslog Monitor (ESM) filtered system message logging to the console connections, use the **logging console filtered** command in global configuration mode. To disable all logging to the console connections, use the **no** form of this command.

**logging console filtered** [ *severity-level* ]

**no logging console**

## Syntax Description

| | |
|---|---|
| *severity-level* | (Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword):<br>[**0** \| **emergencies**]—System is unusable<br>[**1** \| **alerts**]—Immediate action needed<br>[**2** \| **critical**]—Critical conditions<br>[**3** \| **errors**]—Error conditions<br>[**4** \| **warnings**]—Warning conditions<br>[**5** \| **notifications**]—Normal but significant conditions<br>[**6** \| **informational**]—Informational messages<br>[**7** \| **debugging**]—Debugging messages<br>The default severity level varies by platform but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged. |

## Command Default

Logging to the console is enabled.

ESM filtering of system logging messages sent to the console is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.3(2)XE | This command was integrated into Cisco IOS Release 12.3(2)XE. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |

## Usage Guidelines

If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging console filtered** command.

Standard logging is enabled by default, but filtering by the ESM is disabled by default.

ESM uses syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before system logging messages can be filtered.

When ESM filtering is enabled, all messages sent to the console have the configured syslog filter modules applied. To disable filtered logging to the console and return to standard logging, use the standard **logging console** command (without the **filtered**keyword). To disable all logging to the console, use the **no logging console** command, with or without the **filtered** keyword.

## Examples

The following example shows how to enable ESM filtered logging to the console for severity levels 0 through 3:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging console filtered 3
```

## Related Commands

| Command | Description |
|---|---|
| **logging console** | Enables standard system message logging (syslog) to all console (CTY) connections and sets the severity level. |
| **logging filter** | Specifies the name and location of a syslog filter module to be applied to generated system logging messages. |
| **logging on** | Globally controls (enables or disables) system message logging. |
| **show logging** | Displays the state of system message logging, followed by the contents of the logging buffer. |

# logging filter

To specify a syslog filter module to be used by the Embedded Syslog Manager (ESM), use the **logging filter** command in global configuration mode. To remove a module from the filter chain, use the **no** form of this command.

**logging filter** *filter-url* [ *position* ] [**args** *filter-arguments*]

**no logging filter** *filter-url*

## Syntax Description

| | |
|---|---|
| *filter-url* | Specifies the location of the syslog filter module (script file), using the standard Cisco IOS File System URL syntax.<br>• The location can be a local memory location, such as **flash:** or **slot0:**, or a remote file server system, such as **tftp:**, **ftp:**, or **rcp:**.<br>• The *filter-url* should include the name of the syslog filter module, such as email.tcl or email.txt. |
| *position* | (Optional) An integer that specifies the order in which the syslog filter modules should be executed. The valid value for this argument is *n* + 1, where *n* is the current number of configured filters.<br>• If this argument is omitted, the specified module will be positioned as the last module in the chain (the *n*th+1 position). |
| **args** *filter-arguments* | (Optional) Adds values to be passed by the ESM file chain. The ESM filter modules will determine what arguments you should use. |

## Command Default

No ESM filters are applied to system logging messages.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.3(2)XE | This command was integrated into Cisco IOS Release 12.3(2)XE. |

| Release | Modification |
|---|---|
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |

## Usage Guidelines

Use this command to enable the Embedded Syslog Manager by specifying the filter that should be applied to logging messages generated by the system. Repeat this command for each syslog filter module that should be used.

Syslog filter modules are Tool Command Language (Tcl) script files. These files can be stored as plain text files (.txt) or as precompiled Tcl scripts (.tcl). When you position (order) the modules, remember that the output of each filter module is used as input for the next filter module in the chain.

By default, syslog filter modules are executed in the order in which they appear in the system configuration file. The *position* argument can be used to order the filter modules manually. You can also reorder the filter modules at any time by reentering the **logging filter** command and specifying a different position for a given filter module.

The optional **args** *filter-arguments* syntax can be added to pass arguments to the specified filter. Multiple arguments can be specified. The number and type of arguments should be defined in the syslog filter module. For example, if the syslog filter module is designed to accept a specific e-mail address as an argument, you could pass the e-mail address using the **args user@host.com** syntax. Multiple arguments are typically delimited by spaces.

To remove a module from the list of modules to be executed, use the **no** form of this command. Modules not referenced in the configuration will not be executed, regardless of their "position" number.

## Examples

The following example shows how to enable ESM filtered logging to the console for severity levels 0 through 3:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging filter slot0:/email_guts.tcl

Router(config)# logging console filtered 3
```

## Related Commands

| Command | Description |
|---|---|
| **logging buffer filtered** | Enables ESM filtered system message logging to the system logging buffer. |
| **logging console filtered** | Enables ESM filtered system message logging to all console connections. |

| Command | Description |
|---|---|
| **logging host** | Enables system message logging to a remote host (syslog collector). |
| **logging monitor filtered** | Enables ESM filtered system message logging to all monitor (TTY) connections. |
| **show logging** | Displays the status of system message logging, followed by the contents of the logging buffer. |

# logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

**logging host** {{*ip-address*| *hostname*} [**vrf** *vrf-name*]| **ipv6** {*ipv6-address*| *hostname*}} [**discriminator** *discr-name*| [**filtered** [**stream** *stream-id*]| **xml**]] [**transport** {[**beep [audit]** [**channel** *chnl-number*] [**sasl** *profile-name*] [**tls cipher** [ *cipher-num* ] **trustpoint** *trustpt-name*]]| **tcp [audit]| udp**} [**port** *port-num*]] **[sequence-num-session]** [**session-id** {**hostname| ipv4| ipv6**| **string** *custom-string*}]

**no logging host** {{*ip-address*| *hostname*}| **ipv6** {*ipv6-address*| *hostname*}}

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the host that will receive the system logging (syslog) messages. |
| *hostname* | Name of the IP or IPv6 host that will receive the syslog messages. |
| **vrf** *vrf-name* | (Optional) Specifies a VPN routing and forwarding instance (VRF) that connects to the syslog server host. Name of the VRF that connects to the syslog server host. |
| **ipv6** | Indicates that an IPv6 address will be used for a host that will receive the syslog messages. |
| *ipv6-address* | IPv6 address of the host that will receive the syslog messages. |
| **discriminator** *discr-name* | (Optional) Specifies a message discriminator for the session. Name of the message discriminator. |
| **filtered** | (Optional) Specifies that logging messages sent to this host should first be filtered by the Embedded Syslog Manager (ESM) syslog filter modules specified in the **logging filter** commands. |
| **stream** *stream-id* | (Optional) Specifies that only ESM filtered messages with the stream identification number specified in the *stream-id* argument should be sent to this host. Number from 10 to 65535 that identifies the message stream. |
| **xml** | (Optional) Specifies that the logging output should be tagged using the XML tags defined by Cisco. |

| | |
|---|---|
| **transport** | (Optional) Method of transport to be used. UDP is the default. |
| **beep** | (Optional) Specifies that the Blocks Extensible Exchange Protocol (BEEP) transport will be used. |
| **audit** | (Optional) Available only for BEEP and TCP. When the **audit** keyword is used, the specified host is identified for firewall audit logging. |
| **channel** *chnl-number* | (Optional) Specifies the BEEP channel number to use. Number of the BEEP channel. Valid values are 1, 3, 5, 7, 9, 11, 13, and 15. The default is 1. |
| **sasl** | (Optional) Applies the Simple Authentication and Security Layer (SASL) BEEP profile. |
| *profile-name* | (Optional) Name of the SASL profile. |
| **tls cipher** | (Optional) Specifies the cipher suites to be used for a connection. Cipher suites are referred to by mask values. Multiple cipher suites can be chosen by adding the mask values. The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images. |
| *cipher-num* | (Optional) Integer from 32 to 224 that is the mask value of a cipher suite (sum of up to three numbers: 32, 64, and 128) and refers to the following:<br>• ENC_FLAG_TLS_RSA_WITH_NULL_SHA - 32<br>• ENC_FLAG_TLS_RSA_WITH_RC4_128_MD5 - 64<br>• ENC_FLAG_TLS_RSA_WITH_AES_128_CBC_SHA - 128<br>The **tls cipher** *cipher-num* keyword and argument pair is available only in crypto images. |
| **trustpoint** *trustpt-name* | (Optional) Specifies a trustpoint for identity information and certificates. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images. Name of the trustpoint. If you previously declared the trustpoint and want only to update its characteristics, specify the name you previously created. The **trustpoint** *trustpt-name* keyword and argument pair is available only in crypto images. |

| | |
|---|---|
| **tcp** | (Optional) Specifies that the TCP transport will be used. |
| **udp** | (Optional) Specifies that the UDP transport will be used. |
| **port** *port-number* | (Optional) Specifies that a port will be used.<br>Integer from 1 through 65535 that defines the port.<br>If a port number is not specified, the standard Cisco default port number for TCP is 601, for BEEP is 601, and for UDP is 514. |
| **sequence-num-session** | (Optional) Includes a session sequence number tag in the syslog message. |
| **session-id** | (Optional) Specifies syslog message session ID tagging. |
| **hostname** | Includes the hostname in the session ID tag. |
| **ipv4** | Includes the logging source IP address in the session ID tag. |
| **ipv6** | Includes the logging source IPv6 address in the session ID tag. |
| **string** *custom-string* | Includes the custom string in the session ID tag.<br>Custom string in the s_id="custom_string" tag. |

## Command Default

System logging messages are not sent to any remote host. When this command is entered without the **xml** or **filtered** keyword, messages are sent in the standard format.

## Command Modes

Global configuration (config)

## Command History

| T Release | Modification |
|---|---|
| 10.0 | The **logging** command was introduced. |
| 12.2(15)T | The **logging host** command replaced the **logging** command. The **xml** keyword was added. |
| 12.3(2)T | The **filtered** [**stream**] *stream-id* syntax was added as part of the ESM feature. |
| 12.3(14)T | The **trasport** keyword was added. |

| T Release | Modification |
|---|---|
| 12.4(4)T | The **ipv6** *ipv6-address* keyword-argument pair was added. |
| 12.4(11)T | Support for BEEP and the **discriminator**, **sequence-num-session**, and **session-id** keywords and *discr-name* argument was added. |
| **S Release** | **Modification** |
| 12.0(14)S | The **logging host** command replaced the **logging** command. |
| 12.0(14)ST | The **logging host** command replaced the **logging** command. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S and the **vrf** *vrf-name* keyword-argument pair was added. |
| **SR Release** | **Modification** |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. The **vrf** *vrf-name* and **xml** keywords were supported. |
| **SX Release** | **Modification** |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. Support was added for **vrf** *vrf-name* and **xml** keywords and argument. |
| 12.2(33)SXI | Support for BEEP and the **discriminator**, **sequence-num-session**, and **session-id** keywords and *discr-name* argument were added. |
| **XE Release** | **Modification** |
| 12.3(2)XE | This command was integrated into Cisco IOS Release 12.3(2)XE. |
| **SB Release** | **Modification** |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. Support was added for the **vrf** *vrf-name* and **xml** keywords and argument. |
| 12.2(31)SB2 | This command was implemented on the Cisco 10000 series routers. Support was added for the **vrf** *vrf-name* and **xml** keywords and argument. |

## Usage Guidelines

Standard system logging is enabled by default. If logging is disabled on your system (using the **no logging on** command), you must enter the **logging on** command to reenable logging before you can use the **logging host** command.

The **logging host** command identifies a remote host (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of hosts that receive logging messages.

To specify the severity level for logging to all hosts, use the **logging trap** command.

Use the **vrf** *vrf-name* keyword and argument to enable a syslog client (a provider edge [PE] router) to send syslog messages to a syslog server host connected through a VRF interface. To delete the configuration of the syslog server host from the VRF, use the **no logging host** command with the **vrf** *vrf-name* keyword and argument.

When XML-formatted syslog is enabled using the **logging host** command with the **xml** keyword, messages are sent to the specified host with the system-defined XML tags. These tags are predefined and cannot be configured by a user. XML formatting is not applied to debug output.

If you are using the ESM feature, you can enable ESM-filtered syslog messages to be sent to one or more hosts using the **logging host filtered** command. To use the ESM feature, you must first specify the syslog filter modules that should be applied to the messages using the **logging filter** command. See the description of the **logging filter** command for more information about the ESM feature.

**Note** ESM and message discriminator usage is mutually exclusive in a given syslog session.

Using the BEEP transport protocol, you can have reliable and secure delivery for syslog messages and configure multiple sessions over eight BEEP channels. The **sasl** *profile-name*, **tls cipher** *cipher-num*, **trustpoint** *trustpt-name* keywords and arguments are available only in crypto images.

To configure standard logging to a specific host after configuring XML-formatted or ESM-filtered logging to that host, use the **logging host** command without the **xml** or **filtered** keyword. Issuing the standard **logging host** command replaces an XML- or ESM-filtered **logging host** command, and vice versa, if the same host is specified.

You can configure the system to send standard messages to one or more hosts, XML-formatted messages to one or more hosts, and ESM-filtered messages to one or more hosts by repeating this command as many times as desired with the appropriate syntax. (See the “Examples” section.)

When the **no logging host** command is issued with or without the optional keywords, all logging to the specified host is disabled.

## Examples

In the following example, messages at severity levels 0 (emergencies) through 5 (notifications) (**logging trap** command severity levels) are logged to a host at 192.168.202.169:

```
Router(config)# logging host 192.168.202.169

Router(config)# logging trap 5
```

In the following example, standard system logging messages are sent to the host at 192.168.200.225, XML-formatted system logging messages are sent to the host at 192.168.200.226, ESM-filtered logging messages with the stream 10 value are sent to the host at 192.168.200.227, and ESM-filtered logging messages with the stream 20 value are sent to host at 192.168.202.129:

```
Router(config)# logging host 192.168.200.225

Router(config)# logging host 192.168.200.226 xml

Router(config)# logging host 192.168.200.227 filtered stream 10

Router(config)# logging host 192.168.202.129 filtered stream 20
```

In the following example, messages are logged to a host with an IP address of 172.16.150.63 connected through a VRF named vpn1:

```
Router(config)# logging host 172.16.150.63 vrf vpn1
```

In the following example, the default UDP on an IPv6 server is set because no port number is specified. The default port number of 514 is used:

```
Router(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF
```

In the following example, TCP port 1774 on an IPv6 server is set:

```
Router(config)# logging host ipv6 BBBB:CCCC:DDDD:FFFF::1234 transport tcp port 1774
```

In the following example, the UDP port default is used on an IPv6 server with a hostname of v6-hostname:

```
Router(config)# logging host ipv6 v6-hostname transport udp port 514
```

In the following example, a message discriminator named fltr1 is specified along with the BEEP protocol for port 600 and channel 3.

```
Router(config)# logging host host2 dicriminator fltr1 transport beep channel 3 port 600
```

## Related Commands

| Command | Description |
|---|---|
| **logging filter** | Specifies a syslog filter module to be used by the ESM. |
| **logging on** | Globally controls (enables or disables) system message logging. |
| **logging trap** | Limits messages sent to the syslog servers based on severity level. |
| **show logging** | Displays the state of system message logging, followed by the contents of the standard syslog buffer. |
| **show logging xml** | Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer. |

# logging monitor filtered

To enable Embedded Syslog Manager (ESM) filtered system message logging to monitor connections, use the **logging monitor filtered** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

**logging monitor filtered** [ *severity-level* ]

**no logging monitor filtered**

## Syntax Description

| | |
|---|---|
| *severity-level* | (Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword):<br>[**0** \| **emergencies**]—System is unusable<br>[**1** \| **alerts**]—Immediate action needed<br>[**2** \| **critical**]—Critical conditions<br>[**3** \| **errors**]—Error conditions<br>[**4** \| **warnings**]—Warning conditions<br>[**5** \| **notifications**]—Normal but significant conditions<br>[**6** \| **informational**]—Informational messages<br>[**7** \| **debugging**]—Debugging messages<br>The default severity level varies by platform but is generally level 7 (“debugging”), meaning that messages at all severity levels (0 through 7) are logged. |

## Command Default

Logging to monitor connections is enabled.

ESM filtering of system logging messages sent to the monitor connections is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.3(2)XE | This command was integrated into Cisco IOS Release 12.3(2)XE. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |

## Usage Guidelines

The **monitor** keyword specifies the TTY (TeleTYpe) line connections at all line ports. TTY lines (also called ports) communicate with peripheral devices such as terminals, modems, and serial printers. An example of a TTY connection is a PC with a terminal emulation program connected to the device using a dialup modem, or a Telnet connection.

Standard logging is enabled by default, but filtering by the ESM is disabled by default. If standard logging has been disabled on your system (using the **no logging on** command), standard logging must be reenabled using the **logging on** command before using the **logging monitor filtered** command.

ESM uses syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device. The syslog filter modules must be configured using the **logging filter** command before system logging messages can be filtered.

When ESM filtering is enabled, all messages sent to the monitor have the configured syslog filter modules applied. To disable filtered logging to the monitor and return to standard logging, issue the standard **logging monitor** command (without the **filtered** keyword). To disable all logging to the monitor connections, use the **no logging monitor** command, with or without the **filtered** keyword.

## Examples

The following example shows how to enable ESM filtered logging to the monitor connections:

```
Router(config)# logging filter tftp://209.165.200.225/ESM/escalate.tcl
Router(config)# logging filter slot0:/email.tcl user@example.com
Router(config)# logging monitor filtered
```

## Related Commands

| Command | Description |
|---|---|
| **logging monitor** | Enables standard system message logging to all monitor (TTY) connections. |
| **show logging xml** | Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer. |

# logging origin-id

To add an origin identifier to system logging messages sent to remote hosts, use the **logging origin-id** command in global configuration mode. To disable the origin identifier, use the **no** form of this command.

**logging origin-id** {**hostname**| **ip**| **ipv6**| **string** *user-defined-id*}

**no logging origin-id**

## Syntax Description

| | |
|---|---|
| **hostname** | Specifies that the hostname will be used as the message origin identifier. |
| **ip** | Specifies that the IP address of the sending interface will be used as the message origin identifier. |
| **ipv6** | Specifies that the IPv6 address of the sending interface will be used as the message origin identifier. |
| **string** *user-defined-id* | Allows you to enter your own identifying description. The *user-defined-id* argument is a string you specify.<br>• You can enter a string with no spaces or use delimiting quotation marks to enclose a string with spaces. |

## Command Default

This command is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.3(1) | The **string** *user-defined-id* keyword-argument pair was added. |
| 12.3(2)XE | This command was integrated into Cisco IOS Release 12.3(2)XE. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.4(4)T | The **ipv6** keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

| Release | Modification |
|---|---|
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |

## Usage Guidelines

The origin identifier is added to the beginning of all system logging (syslog) messages sent to remote hosts. The identifier can be the hostname, the IP address, the IPv6 address, or any text that you specify. The origin identifier is not added to messages sent to local destinations (the console, monitor, or buffer).

The origin identifier is useful for identifying the source of system logging messages in cases where you send syslog output from multiple devices to a single syslog host.

When you specify your own identification string using the **logging origin-id string** *user-defined-id* command, the system expects a string without spaces. For example:

```
Router(config)# logging origin-id string Cisco_Systems
```

To use spaces (multiple words) or additional syntax, enclose the string with quotation marks (“ ”). For example:

```
Router(config)# logging origin-id string "Cisco Systems, Inc."
```

## Examples

In the following example, the origin identifier “Domain 1, router B” will be added to the beginning of all system logging messages sent to remote hosts:

```
Router(config)# logging origin-id string Domain 1, router B
```

In the following example, all logging messages sent to remote hosts will have the IP address configured for serial interface 1 added to the beginning of the message:

```
Router(config)# logging host 209.165.200.225
Router(config)# logging trap 5
Router(config)# logging source-interface serial 1
Router(config)# logging origin-id ip
```

## Related Commands

| Command | Description |
|---|---|
| **logging host** | Enables system message logging to a remote host. |
| **logging source-interface** | Forces logging messages to be sent from a specified interface, instead of any available interface. |
| **logging trap** | Configures the severity level at or numerically below which logging messages should be sent to a remote host. |

# logging source-interface

To specify the source IPv4 or IPv6 address of system logging packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

**logging source-interface** {**interface-name** *number* **vrf** *vrf-name*}

**no logging source-interface**{**interface-name** *number* **vrf** *vrf-name*}

## Syntax Description

| | |
|---|---|
| **Interface-name** *number* | Interface type and number. |
| **vrf***vrf -name* | Provides logging source-interface setting capability to Virtual Routing and Forwarding (VRF) syslog destinations. Name assigned to the VRF. |

## Command Default

The wildcard interface address is used.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.4(4)T | This command was modified. IPv6 support was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. The **vrf** keyword and *vrf-name* argument were added |

## Usage Guidelines

This command can be configured on the VRF and non-VRF interfaces. Normally, a syslog message contains the IPv4 or IPv6 address of the interface used to exit the router. The **logging source-interface** command configures the syslog packets that contain the IPv4 or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

When no specific interface is configured, a wildcard interface address of 0.0.0.0 (for IPv4) or :: (for IPv6) is used, and the IP socket selects the best outbound interface.

## Examples

The following example shows how to specify that the IP address of Ethernet interface 0 as the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 0 vrf1
```

The following example shows how to specify the IP address for Ethernet interface 2/1 as the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 2/1 vrf1
```

The following sample output displays that the **logging source-interface** command is configured on a VRF source interface:

```
Router# show running interface loopback49

             Building configuration...
             Current configuration : 84 bytes
             !
             interface Loopback49
              ip vrf forwarding vrf1
              ip address 10.4.2.39 255.0.0.0
             end
Router# show running | includes logging
      logging source-interface Loopback49 vrf1
      logging host 192.0.2.1 vrf1
```

## Related Commands

| Command | Description |
|---|---|
| **logging** | Logs messages to a syslog server host. |