



# XML Interface to Syslog Messages

---

**First Published: March 17, 2003**

**Last Updated: February 28, 2006**

The XML Interface to Syslog Messages feature provides command-line interface (CLI) commands for enabling syslog messages to be sent in an Extensible Markup Language (XML) format. Logs in a standardized XML format can be more readily used in external customized monitoring tools.

## History for the XML Interface to Syslog Messages Feature

Release	Modification
12.2(15)T	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About the XML Interface to Syslog Messages Feature, page 2](#)
- [How to Configure XML Formatting of Syslog Messages, page 4](#)
- [Configuration Examples for XML Formatting of Syslog Messages, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)
- [Glossary, page 23](#)



---

**Corporate Headquarters:**

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

© 2003, 2006 Cisco Systems, Inc. All rights reserved.

# Information About the XML Interface to Syslog Messages Feature

To configure the XML Interface to Syslog Messages feature, you must understand the following concepts:

- [Cisco IOS System Message Logging, page 2](#)
- [XML-Formatted System Message Logging, page 2](#)
- [System Logging Message Formatting, page 3](#)

## Cisco IOS System Message Logging

The Cisco IOS system message logging (syslog) process allows the system to report and save important error and notifications messages, either locally or to a remote logging server. These syslog messages include messages in a standardized format (often called system error messages) and output from **debug** commands. These messages are generated during network operation to assist users and Cisco TAC engineers with identifying the type and severity of a problem, or to aid users in monitoring router activity. Syslog messages can be sent to the console, a monitor (TTY and Telnet connections), the system buffer, or to remote hosts.

**Note**

The system message logging process in Cisco IOS software is abbreviated as “syslog”. The messages generated by this process are called “syslog messages”. However, syslog messages are also referred to in Cisco IOS documentation as “system error messages” or “SEMs”. Note that syslog messages are not restricted to error conditions, and can reflect purely informational messages.

## XML-Formatted System Message Logging

XML, a derivative of SGML, provides a representation scheme to structuralize consistently formatted data such as that found in syslog messages.

The XML Interface to Syslog Messages features provides CLI commands for enabling syslog messages to be sent in an XML format. Logs in a standardized XML format can be more readily used in external customized monitoring tools. Within the Cisco IOS software, a closed set of meaningful XML tags are defined and, when enabled, applied to the syslog messages sent to the console, monitor, buffer, or to remote hosts.

Two system logging formats exist in Cisco IOS software: the standard logging format and the XML logging format. This means that you can specify that the standard syslog messages be sent to one remote host while the XML-formatted syslog messages are sent to another host. Similarly, if logging messages are sent to the system buffer, the XML logging buffer is separate from the standard logging buffer, and you can have the standard and XML logging buffers running at the same time.

The XML logging process is dependant on the standard logging process. In most cases, settings for the standard logging process carry over to the XML logging process. For example, the severity level for the **logging buffered xml** command is determined by the level set for the standard **logging buffered** command (or, if not set, by the default severity level for the standard buffer). Similarly, the default size of the XML logging buffer is the same as the standard logging buffer’s default (the default buffer size varies by platform).

## System Logging Message Formatting

System logging messages take the following format:

```
%<facility>-<severity>-<mnemonic>: <message-text>
```

For example:

```
%LINK-5-CHANGED: Interface Serial3/3, changed state to administratively down
```

Usually, these messages are preceded by additional text, such as the timestamp and message sequence number:

```
<sequence-number>: <date or system-up-time> <time>:%<facility>-<severity>-<mnemonic>:
<message-text>
```

For example:

```
000013: Mar 18 14:52:10.039:%LINK-5-CHANGED: Interface Serial3/3, changed state to
administratively down
```



### Note

The timestamp format used in system logging messages is determined by the **service timestamps** command in the global configuration mode. The **service sequence-numbers** command in the global configuration mode enables or disables the leading sequence number. An asterisk (\*) before the time indicates that the time may be incorrect because the system clock has not synchronized to a reliable time source.

Table 1 shows the XML tags applied to syslog messages (the XML formatting):

**Table 1** XML Tags used for Syslog Message Fields

Tag Applied	Delimited Item
<ios-log-msg></ios-log-message>	Entire syslog message.
<facility></facility>	Facility Name. FACILITY is a code consisting of two or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software.
<severity></severity>	Severity Value. SEVERITY is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.
<msg-id></msg-id>	Mnemonic. The MNEMONIC is a code (usually an abbreviated description) that uniquely identifies the type of error or event.
<seq></seq>	The error sequence number.
<time></time>	The timestamp, including date and time, or the system uptime (time since last reboot).

**Table 1 XML Tags used for Syslog Message Fields**

Tag Applied	Delimited Item
<code>&lt;args&gt;&lt;/args&gt;</code>	<p>The variables within the message text. The full “human readable” text of the message is not retained in XML. Only the variables are extracted and formatted.</p> <p>The variables within a system error message are identified with brackets (<code>[chars]</code>, <code>[hex]</code>, <code>[int]</code>, and so on) in Cisco IOS documentation.</p> <p>For example:</p> <pre>%LINK-5-CHANGED: : Interface [chars], changed state to [chars]</pre> <p>For the complete text of syslog messages, see the <i>Cisco IOS System Error Messages</i> document, available on Cisco.com.</p>
<code>&lt;arg id="x"&gt;&lt;/arg&gt;</code>	A specific argument. “x” is a sequential variable I.D. number, starting with zero.

The following example shows a syslog message in standard format, followed by the same message with XML formatting applied:

#### Standard Syslog Message Format

```
000013: *Oct 11 14:52:10.039: %SYS-5-CONFIG_I: Configured from console by vty0
(172.19.208.14)
```

#### XML Syslog Message Format

```
<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><seq>0
00013</seq><time>*Oct 11 14:52:10.039</time><args><arg id="0">console</arg><arg
id="1">vty0 (172.19.208.14)</arg></args></ios-log-msg>
```



#### Note

System logging messages include debugging messages when debugging is enabled on the router and logging is configured to record severity level 7 messages. However, debugging messages do not use the system logging message format. XML formatting will not, therefore, be applied to these messages.

## How to Configure XML Formatting of Syslog Messages

Enabling logging in an XML format consists of simply using the appropriate logging command to indicate where syslog messages should be sent, followed by the **xml** keyword. Standard system message logging is enabled by default, but XML formatting of these messages is disabled by default.

As mentioned previously, the XML-formatted logging process is separate than (but dependant on) the standard logging process, so you can configure XML-formatted logging in addition to standard logging if the destination is a remote host or the system buffer.

This section contains the following procedure:

- [Enabling XML formatting for syslog messages, page 5](#)

## Enabling XML formatting for syslog messages

To enable XML formatting for syslog messages, perform the following steps.



**Note** To view the status of logging and the contents of the XML logging buffer, use the **show logging xml** command in EXEC mode. To clear the contents of the XML logging buffer, use the **clear logging xml** command in EXEC mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging console xml**  
or  
**logging monitor xml**  
or  
**logging buffered xml**  
or  
**logging host {ip-address | host-name} xml**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
<p><b>Step 3</b> <code>logging console xml [severity-level]</code></p> <p><b>Example:</b> Router(config)#logging console xml informational</p>	<p>Enables system message logging to the console connections in XML format.</p> <p>Messages at or numerically below the severity level will be logged. 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.</p>
<p><code>logging monitor xml [severity-level]</code></p> <p><b>Example:</b> Router(config)#logging monitor xml 6</p>	<p>Enables system message logging to the monitor connections (all available TTY or Telnet connections) in XML format.</p> <p>Messages at or numerically below the severity level will be logged. 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.</p> <p>Note that the display of logging messages is often disabled by default, meaning that messages will not be displayed when you log into the terminal until you issue the <b>terminal monitor</b> command in the EXEC mode.</p>
<p><code>logging buffered xml [xml-buffer-size]</code></p> <p><b>Example:</b> Router(config)#logging buffered xml 14336</p>	<p>Enables system message logging to the system buffer in XML format.</p> <p>The severity level for logged messages is determined by the setting of the <b>logging buffered</b> command. If the <b>logging buffered</b> command has not been used, the default severity level for that command is used. 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. For more information on severity levels, see the documentation of the <b>logging buffered</b> command.</p> <p>The default XML logging buffer size varies by platform. (The size of the XML logging buffer is the same as the standard logging buffer’s default.) The valid range for the XML buffer size is 4096 to 2147483647 bytes (4 Kilobytes to 2 Gigabytes).</p>
<p><code>logging host {ip-address   host-name} xml</code></p> <p><b>Example:</b> Router(config)#logging host 192.168.202.132 xml Router(config)#logging host 192.168.201.20 xml</p>	<p>Enables system message logging in XML format to the specified host.</p> <p>By issuing this command more than once, you build a list of syslog servers that receive logging messages.</p> <p><b>Note</b> To send standard logging output to one host and XML-formatted logging output to another host, you must specify a different IP address (or host name) in the <b>logging host</b> (standard) command.</p> <p>The default severity level varies by platform, but is generally level 5 (“notifications”), meaning that messages at severity levels 0 through 7 are logged. To specify the severity level for logging to all remote hosts, use the <b>logging trap</b> command.</p>

# Configuration Examples for XML Formatting of Syslog Messages

In the following example, logging is enabled and then logging to the standard buffer and to the XML buffer is enabled. The last two **show logging** commands compare the difference between the standard syslog buffer and the XML syslog buffer.

```
Router#show logging
Syslog logging: disabled (10 messages dropped, 5 messages rate-limited, 6 flush)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled, xml disabled
  Logging Exception size (8192 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 31 message lines logged
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging on
Router(config)#logging buffered
Router(config)#end
Router#show logging
Syslog logging: enabled (10 messages dropped, 5 messages rate-limited, 6 flushed)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: level debugging, 1 messages logged, xml disabled
  Logging Exception size (8192 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 32 message lines logged

Log Buffer (8192 bytes):

1w0d: %SYS-5-CONFIG_I: Configured from console by console
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging buffered xml
Router(config)#end
Router#show logging
Syslog logging: enabled (10 messages dropped, 5 messages rate-limited, 6 flushes, 0
overruns, xml enabled)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: level debugging, 2 messages logged, xml enabled (1 messages logged)
  Logging Exception size (8192 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 33 message lines logged

Log Buffer (8192 bytes):

1w0d: %SYS-5-CONFIG_I: Configured from console by console
1w0d: %SYS-5-CONFIG_I: Configured from console by console
Router#show logging xml
<syslog-logging status="enabled" msg-dropped="10" msg-rate-limited="5" flushes="6"
overruns="0"><xml>enabled</xml></syslog-logging>
  <console-logging>disabled</console-logging>
  <monitor-logging>disabled</monitor-logging>
  <buffer-logging level="debugging" messages-logged="2"><xml
messages-logged="1">enabled</xml></buffer-logging>
  <logging-exception size="8192 bytes"></logging-exception>
  <count-and-timestamp-logging status="disabled"></count-and-timestamp-logging>
  <trap-logging level="informational" messages-lines-logged="33"></trap-logging>

<log-xml-buffer size="8192 bytes"></log-xml-buffer>
```

```
<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>
1w0d</time><args><arg id="0">console</arg>
Router#
```

## Additional References

The following sections provide references related to XML Interface to Syslog Messages.

### Related Documents

Related Topic	Document Title
system message logging	“Troubleshooting and Fault Management” chapter in the <a href="#">Cisco IOS Configuration Fundamentals Configuration Guide</a> , Release 12.2
System Error Messages (SEMs)	“ <a href="#">Cisco IOS System Error Messages</a> , Release 12.2
Debug-level System Messages	<a href="#">Cisco IOS Debug Command Reference</a> , Release 12.4T

### Standards

Standard	Title
The XML 1.0 Recommendation (“Extensible Markup Language (XML) 1.0 (Second Edition)”)	<a href="#">W3C Technical Reports and Publications</a>

### MIBs

MIB	MIBs Link
None	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>

### RFCs

RFCs <sup>1</sup>	Title
RFC 3470	“ <i>Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols</i> ” (Status: BEST CURRENT PRACTICE)

1. Not all supported RFCs are listed.

## Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This section documents modified commands only.

- [clear logging xml](#)
- [logging buffered xml](#)
- [logging console xml](#)
- [logging host](#)
- [logging monitor xml](#)
- [show logging xml](#)

# clear logging xml

To clear the contents of the XML system message logging (syslog) buffer, use the **clear logging xml** command in User EXEC or Privileged EXEC mode..

## clear logging xml

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Usage Guidelines** This command clears the contents of the XML-formatted logging buffer, but does not clear the contents of the standard logging buffer. The system will prompt you to confirm the action before clearing the buffer.

**Examples** In the following example, the XML-specific buffer is cleared:

```
Router# clear logging xml
Clear XML logging buffer [confirm]?y
```

Related Commands	Command	Description
	<b>logging buffered xml</b>	Enables system message logging (syslog) to the XML-specific buffer in XML format.
	<b>show logging xml</b>	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

# logging buffered xml

To enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer, use the **logging buffered xml** command in global configuration mode. To disable the XML syslog buffer and return the size of the buffer to the default, use the **no** form of this command.

**logging buffered xml** [*xml-buffer-size*]

**no logging buffered xml** [*xml-buffer-size*]

## Syntax Description

<i>xml-buffer-size</i>	(Optional) Size of the buffer, from 4,096 to 4,294,967,295 bytes (4 kilobytes to 2 gigabytes). The default size varies by platform. This value is ignored if entered as part of the <b>no</b> form of this command.
------------------------	---

## Defaults

XML formatting of system logging messages is disabled.

The default XML syslog buffer size is the same size as the standard syslog buffer.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

Standard logging is enabled by default, but XML-formatted system message logging 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 buffered xml** command.

The **logging buffered xml** command copies logging messages to an internal XML buffer. The XML syslog buffer is separate from the standard syslog buffer (created using the **logging buffered** command).

The buffer is circular, so newer messages overwrite older messages as the buffer is filled.

The severity level for logged messages is determined by the setting of the **logging buffered** command. If the **logging buffered** command has not been used, the default severity level for that command is used. 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. For more information on severity levels, see the documentation of the **logging buffered** command.

Do not make the buffer size too large because the router could run out of memory for other tasks. You can use the **show memory** command in EXEC mode to view the free processor memory on the router; however, this value is the maximum available and should not be approached.

To return the size of the XML logging buffer to the default, use the **no logging buffered xml** command.

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

---

**Examples**

In the following example, the user enables logging to the XML syslog buffer and sets the XML syslog buffer size to 14 kilobytes:

```
Router(config)# logging buffered xml 14336
```

---

**Related Commands**

Command	Description
<b>clear logging xml</b>	Clears all messages from the XML-specific system message logging (syslog) buffer.
<b>logging buffered</b>	Enables standard system message logging (syslog) to a local buffer and sets the severity level and buffer size for the logging buffer.
<b>logging on</b>	Globally controls (enables or disables) system message logging.
<b>show logging xml</b>	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

# logging console xml

To enable XML-formatted system message logging to the console connections, use the **logging console xml** command in global configuration mode. To disable all logging to the console connections, use the **no** form of this command.

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

**no logging console xml**

## Syntax Description

<i>severity-level</i>	(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): <ul style="list-style-type: none"> <li>{<b>0</b>   <b>emergencies</b>}— System is unusable</li> <li>{<b>1</b>   <b>alerts</b>}—Immediate action needed</li> <li>{<b>2</b>   <b>critical</b>}—Critical conditions</li> <li>{<b>3</b>   <b>errors</b>}—Error conditions</li> <li>{<b>4</b>   <b>warnings</b>}—Warning conditions</li> <li>{<b>5</b>   <b>notifications</b>}—Normal but significant conditions</li> <li>{<b>6</b>   <b>informational</b>}—Informational messages</li> <li>{<b>7</b>   <b>debugging</b>}— Debugging messages</li> </ul>
-----------------------	---

## Defaults

Logging to the console is enabled.

XML-formatted logging to the console is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

To return system logging messages to standard text (without XML formatting), issue the standard **logging console** command (without the **xml** keyword extension).

---

**Examples**

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4:

```
Router(config)# logging console xml 4
```

---

**Related Commands**

Command	Description
<b>show logging xml</b>	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog 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} | {ipv6 ipv6-address | hostname}} [transport {udp [port
port-number] | tcp [port port-number] [audit]}}] [xml | filtered [stream stream-id]] [alarm
[severity]]
```

```
no logging host {{ip-address | hostname} | {ipv6 ipv6-address | hostname}} [transport {udp [port
port-number] | tcp [port port-number] [audit]}}] [xml | filtered [stream stream-id]] [alarm
[severity]]
```

## Syntax Description

<i>ip-address</i>	IP address of the host that will receive the system logging (syslog) messages.
<i>hostname</i>	Name of the IP or IPv6 host that will receive the syslog messages.
<b>ipv6</b>	Indicates that an IPv6 address will be used for a host that will receive the syslog messages.
<i>ipv6-address</i>	IPv6 address of the host that will receive the syslog messages.
<b>transport</b>	(Optional) Method of transport to be used.
<b>udp</b>	UDP transport will be used.
<b>port</b>	(Optional) The <b>port</b> keyword indicates that either a TCP or User Datagram Protocol (UDP) port will be used.
<i>port-number</i>	(Optional) Integer from 1 through 65535. <ul style="list-style-type: none"> <li>For TCP, it is required for users to specify the port number.</li> <li>For UDP, it is optional for users to specify the port number. If the port number is omitted, the default Cisco standard port number is 514.</li> </ul>
<b>tcp</b>	Specifies that TCP transport will be used.
<b>audit</b>	(Optional) Optional only for TCP. When the <b>audit</b> keyword is used, the specified host is identified as a special host for firewall auditing purposes.
<b>xml</b>	(Optional) Specifies that the logging output should be tagged using the Cisco defined extensible markup language (XML) tags.
<b>filtered</b>	(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 <b>logging filter</b> commands.
<b>stream</b>	(Optional) Specifies that only ESM filtered messages with the stream identification number specified in the <i>stream-id</i> argument should be sent to this host.
<i>stream-id</i>	(Optional) Number from 10 to 65535 that identifies the message stream.

<b>alarm</b>	(Optional) Specifies that system alarms will be logged.
<i>severity</i>	(Optional) Integer or string value that identifies the severity of an alarm. The integer value is from 1 to 4. String values are critical, major, minor, and informational. The default is 4, or informational. Severity levels are defined as follows: <ul style="list-style-type: none"> <li>• 1—Critical. The condition affects service.</li> <li>• 2—Major. Immediate action is needed.</li> <li>• 3—Minor. Minor warning conditions.</li> <li>• 4—Informational. No action is required.</li> </ul>

**Defaults**

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

**Command Modes**

Global configuration

**Command History**

Release	Modification
10.0	The <b>logging</b> command was introduced.
12.0(14)S	The <b>logging host</b> command replaced the <b>logging</b> command.
12.0(14)ST	The <b>logging host</b> command replaced the <b>logging</b> command.
12.2(15)T	The <b>logging host</b> command replaced the <b>logging</b> command. The <b>xml</b> keyword was added.
12.3(2)T	The <b>filtered</b> [ <b>stream</b> <i>stream-id</i> ] syntax was added as part of the ESM feature.
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 <b>ipv6</b> keyword and <i>ipv6-address</i> argument were added. The <b>alarm</b> keyword and <i>severity</i> argument were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Usage Guidelines**

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

If XML-formatted syslog is enabled using the **logging host** {*ip-address* | **ipv6** *ipv6-address* | *hostname*} **xml** command, messages will be sent to the specified host with the system-defined XML tags. These tags are predefined and cannot be configured by a user. XML formatting will not be applied to debugging 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** {*ip-address* | **ipv6** *ipv6-address* | *hostname*} **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.

To configure standard logging to a specific host after configuring XML-formatted or ESM filtered logging to that host, use the **logging host** {*ip-address* | **ipv6** *ipv6-address* | *hostname*}) command without the **xml** or **filtered** keywords. Issuing the standard **logging host** command will replace an XML or ESM filtered **logging host** command, and vice versa, if the same host is specified.

Use the **alarm** keyword and *severity* argument to limit the number of syslog messages generated.



#### Note

A **no logging host** command (with or without the optional keywords) will disable all logging to the specified host.

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.)

## Examples

In the following example, messages at severity levels 0 (emergencies) through 5 (notifications) 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, 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, on a host named host1 an alarm severity threshold of 3 is set for syslog messages:

```
Router(config)# logging host host1 alarm 3
```

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

# logging monitor xml

To enable XML-formatted system message logging to monitor connections, use the **logging console xml** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

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

**no logging monitor xml**

## Syntax Description

<i>severity-level</i>	(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): <ul style="list-style-type: none"> <li>{ <b>0</b>   <b>emergencies</b> }— System is unusable</li> <li>{ <b>1</b>   <b>alerts</b> }—Immediate action needed</li> <li>{ <b>2</b>   <b>critical</b> }—Critical conditions</li> <li>{ <b>3</b>   <b>errors</b> }—Error conditions</li> <li>{ <b>4</b>   <b>warnings</b> }—Warning conditions</li> <li>{ <b>5</b>   <b>notifications</b> }—Normal but significant conditions</li> <li>{ <b>6</b>   <b>informational</b> }—Informational messages</li> <li>{ <b>7</b>   <b>debugging</b> }— Debugging messages</li> </ul>
-----------------------	---

## Defaults

Logging to monitor connections is enabled.

XML-formatted logging to monitor connections is disabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

The **monitor** keyword specifies the tty line connections at all line ports. The 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 dial-up modem, or a Telnet connection.

To return system logging messages to standard text (without XML formatting), issue the standard **logging monitor** command (without the **xml** keyword extension).

**Examples**

In the following example, the user enables XML-formatted system message logging to the console for messages at levels 0 through 4 and XML-formatted system message logging to tty line connections at the default severity level:

```
Router(config)# logging console xml 4
Router(config)# logging monitor xml
```

**Related Commands**

Command	Description
<b>logging monitor</b>	Enables system message logging in standard (plain text) format to all monitor (TTY) connections.
<b>show logging xml</b>	Displays the state of XML-formatted system message logging, followed by the contents of the XML syslog buffer.

# show logging xml

To display the state of system message logging in an XML format, and to display the contents of the XML syslog buffer, use the **show logging xml** command in privileged EXEC mode.

## show logging xml

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Usage Guidelines** This command displays the same syslog state information as the standard **show logging** command, but displays the information in XML format. This command also displays the content of the XML syslog buffer (if XML-formatted buffer logging is enabled).

**Examples** The following example compares the output of the standard **show logging** command with the output of the **show logging xml** command so that you can see how the standard information is formatted in XML.

```
Router# show logging

Syslog logging: enabled (10 messages dropped, 6 messages rate-limited, 0 flushes, 0
overruns, xml enabled)
  Console logging: level debugging, 28 messages logged, xml enabled
  Monitor logging: level debugging, 0 messages logged, xml enabled
  Buffer logging: level debugging, 2 messages logged, xml enabled (2 messages logged)
  Logging Exception size (8192 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 35 message lines logged
    Logging to 10.2.3.4, 1 message lines logged, xml disabled
    Logging to 192.168.2.1, 1 message lines logged, xml enabled
```

Log Buffer (8192 bytes):

```
00:04:20: %SYS-5-CONFIG_I: Configured from console by console
00:04:41: %SYS-5-CONFIG_I: Configured from console by console
```

```
Router# show logging xml

<syslog-logging status="enabled" msg-dropped="10" msg-rate-limited="6" flushes="0"
overruns="0"><xml>enabled</xml></syslog-logging>
  <console-logging level="debugging"
messages-logged="28"><xml>enabled</xml></console-logging>
  <monitor-logging level="debugging"
messages-logged="0"><xml>enabled</xml></monitor-logging>
  <buffer-logging level="debugging" messages-logged="2"><xml
messages-logged="2">enabled</xml></buffer-logging>
```

```

<logging-exception size="8192 bytes"></logging-exception>
<count-and-timestamp-logging status="disabled"></count-and-timestamp-logging>
<trap-logging level="informational" messages-lines-logged="35"></trap-logging>
  <logging-to><dest id="0" ipaddr="10.2.3.4"
message-lines-logged="1"><xml>disabled</xml><dest></logging-to>
  <logging-to><dest id="1" ipaddr="192.168.2.1"
message-lines-logged="1"><xml>enabled</xml><dest></logging-to>

<log-xml-buffer size="44444 bytes"></log-xml-buffer>

<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>
00:04:20</time><args><arg id="0">console</arg><arg
id="1">console</arg></args></ios-log-msg>
<ios-log-msg><facility>SYS</facility><severity>5</severity><msg-id>CONFIG_I</msg-id><time>
00:04:41</time><args><arg id="0">console</arg><arg
id="1">console</arg></args></ios-log-msg>
Router#

```

Table 2 describes the significant fields shown in the displays.

**Table 2** *show logging and show logging xml Field Descriptions*

Field	Description	XML Tag
Syslog logging	The global state of system message logging (syslog); “enabled” or “disabled.”	syslog-logging
Console logging	State of logging to console connections.	console-logging
Monitor logging	State of logging to monitor (TTY and Telnet) connections.	monitor-logging
Buffer logging	State of logging to the local system logging buffer.	buffer-logging
Count and timestamp logging messages:	Indicates whether the logging count feature is enabled. Corresponds to the <b>logging count</b> command.	count-and-timestamp-logging
Trap logging	State of logging to a remote host.	trap-logging

#### Related Commands

Command	Description
<b>show logging</b>	Displays the contents of the standard syslog buffer.
<b>show logging count</b>	Displays counts of each system error message.
<b>show logging history</b>	Displays the contents of the SNMP syslog history table.

# Glossary

**console**—In the context of this feature, specifies the connection (CTY or console line) to the console port of the router. Typically, this is a terminal attached directly to the console port, or a PC with a terminal emulation program. Corresponds to the **show terminal** command.

**monitor**—In the context of this feature, specifies the TTY (TeleTYpe) line connection at a line port. In other words, the “monitor” keyword corresponds to a TTY line connection or a Telnet (terminal emulation) connection. 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 dial-up modem.

**SEMs**—Abbreviation for system error messages. “System error messages” is a term sometimes used for messages generated by the system logging (syslog) process. Syslog messages use a standardized format, and come in 8 severity levels, from “emergencies” (level 0) to “debugging” (level 7). The term “system error message” is actually misleading, as these messages can include notifications of router activity beyond “errors” (such as informational notices).

**syslog**—Abbreviation for the system message logging process in Cisco IOS software. Also used to identify the messages generated, as in “syslog messages.” Technically, the term “syslog” refers only to the process of logging messages to a remote host or hosts, but is commonly used to refer to all Cisco IOS system logging processes.

**trap**—A trigger in the system software for sending error messages. In the context of this feature, “trap logging” means logging messages to a remote host. The remote host is actually a syslog host from the perspective of the device sending the trap messages, but because the receiving device typically provides collected syslog data to other devices, the receiving device is also referred to as a “syslog server.”

**Note**

---

See [Networking Terms and Acronyms](#) for terms not included in this glossary.

---

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

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.

© 2003, 2006 Cisco Systems, Inc. All rights reserved.

