



Configuring the XML Interface to Syslog Messages

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.

Specifications for the XML Interface to Syslog Messages Feature

Feature History

Release	Modification
12.2(15)T	This feature was introduced.

Supported Platforms¹

All platforms that support standard system message logging. For details, see Cisco Feature Navigator.

1. For image and platform support details and updates, see Cisco Feature Navigator. 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 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)
- [Glossary, page 10](#)



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

© 2007 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](#)
- [XML-Formatted System Message Logging](#)
- [System Logging Message Formatting](#)

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** global configuration mode command. The **service sequence-numbers** global configuration command 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><args></args></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> <p>All these XML tags add significant overhead to a message. In case the message length exceeds the limit of IOS message logging, the “<code><args>...</args></code>” part will be replaced with “<code><args-warning>*** LOG OVERRUN ***</args-warning></code>”</p>
<code><arg id="x"></arg></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>000013</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.

COMMAND SUMMARY

To enable XML formatting for syslog messages, use one of the following commands in global configuration mode:

- **logging console xml**
- **logging monitor xml**
- **logging buffered xml**
- **logging host {ip-address | host-name} xml**

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.

COMMAND DETAILS

Command or Action	Purpose
<p>logging console xml [<i>severity-level</i>]</p> <p>Example: 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>logging monitor xml [<i>severity-level</i>]</p> <p>Example: 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 terminal monitor EXEC mode command.</p>

Command or Action	Purpose
<p>logging buffered xml [<i>xml-buffer-size</i>]</p> <p>Example: 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 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.</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>logging host {<i>ip-address</i> <i>host-name</i>} xml</p> <p>Example: Router(config)#logging host 209.165.202.132 xml Router(config)#logging host 209.165.201.20 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>Note 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 logging host (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 logging trap 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><arg id="1">console</arg></args></ios-log-msg>
Router#

```

Additional References

For additional information related to XML Interface to Syslog Messages feature, refer to the following references:

Related Documents

Related Topic	Document Title
System Message Logging	Troubleshooting and Fault Management module
Debug-level System Messages	Cisco IOS Debug Command Reference

Standards

XML is not currently an Internet Standard. The XML 1.0 Recommendation (“Extensible Markup Language (XML) 1.0 (Second Edition)”) is defined at <http://www.w3.org/TR/>. See also RFC 3076.

MIBs

No relevant MIBs are associated with this feature.

RFCs

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

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
<p>Technical Assistance Center (TAC)</p> <p>The Cisco TAC home page contains 30,000 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.</p>	http://www.cisco.com/public/support/tac/home.shtml
<p>System Error Message Decoder tool</p> <p>For help with researching and resolving your Cisco IOS error messages, try the Cisco IOS Error Message Decoder tool. This tool is made available by the Cisco Technical Assistance Center (TAC) for registered Cisco.com users.</p>	http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl

Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/en/US/docs/ios/mcl/124mainlinemcl/124_book.html.

- **clear logging xml**
- **logging buffered xml**
- **logging console xml**
- **logging host**
- **logging monitor xml**
- **show logging xml**



Note

The **logging host** command replaced the **logging** command in Release 12.2(15)T.

Glossary



Note

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this 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.”

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

© 2009 Cisco Systems, Inc. All rights reserved.