



---

Junos<sup>®</sup> OS

# System Basics: System Log Messages Configuration Guide

Release  
12.1



---

Published: 2012-03-13

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*Junos® OS System Basics: System Log Messages Configuration Guide*

12.1

Copyright © 2012, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Supported Platforms . . . . .	ix
	Using the Examples in This Manual . . . . .	ix
	Merging a Full Example . . . . .	x
	Merging a Snippet . . . . .	x
	Documentation Conventions . . . . .	xi
	Documentation Feedback . . . . .	xiii
	Requesting Technical Support . . . . .	xiii
	Self-Help Online Tools and Resources . . . . .	xiii
	Opening a Case with JTAC . . . . .	xiv
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>System Log Messages Overview . . . . .</b>	<b>3</b>
	Junos OS System Log Configuration Overview . . . . .	3
	Junos OS Platform-Specific Default System Log Messages . . . . .	4
	Single-Chassis System Logging Configuration Overview . . . . .	5
	Impact of Different Local and Forwarded Severity Levels on System Log	
	Messages on a TX Matrix Router . . . . .	7
	Messages Logged When the Local and Forwarded Severity Levels Are the	
	Same . . . . .	7
	Messages Logged When the Local Severity Level Is Lower . . . . .	7
	Messages Logged When the Local Severity Level Is Higher . . . . .	8
	Impact of Different Local and Forwarded Severity Levels on System Log	
	Messages on a TX Matrix Plus Router . . . . .	9
	Messages Logged When the Local and Forwarded Severity Levels Are the	
	Same . . . . .	9
	Messages Logged When the Local Severity Level Is Lower . . . . .	9
	Messages Logged When the Local Severity Level Is Higher . . . . .	10
	Displaying a Log File from a Single-Chassis System . . . . .	11
	Displaying a Log File from a Routing Matrix . . . . .	11
	Displaying and Interpreting System Log Message Descriptions . . . . .	12
	Interpreting Messages Generated in Structured-Data Format . . . . .	14
	Interpreting Messages Generated in Standard Format by a Junos Process or	
	Library . . . . .	18
	Interpreting Messages Generated in Standard Format by Services on a PIC . . . . .	19
	The message-source Field on a Single-Chassis System . . . . .	20
	The message-source Field on a TX Matrix Platform . . . . .	21
	The message-source Field on a T640 Routing Node in a Routing Matrix . . . . .	22

<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Configuring System Log Messages for a Single-Chassis System . . . . .</b>	<b>27</b>
	Junos OS System Log Configuration Hierarchy . . . . .	28
	Junos OS Minimum System Logging Configuration . . . . .	28
	Junos OS Default System Log Settings . . . . .	29
	Junos OS Platform-Specific Default System Log Messages . . . . .	30
	Specifying the Facility and Severity of Messages to Include in the Log . . . . .	31
	Directing System Log Messages to a Log File . . . . .	32
	Logging Messages in Structured-Data Format . . . . .	32
	Directing System Log Messages to a User Terminal . . . . .	33
	Directing System Log Messages to the Console . . . . .	34
	Directing System Log Messages to a Remote Machine or the Other Routing Engine . . . . .	34
	Specifying an Alternative Source Address for System Log Messages . . . . .	35
	Changing the Alternative Facility Name for Remote System Log Messages . . . . .	36
	System Log Default Facilities for Messages Directed to a Remote Destination . . . . .	37
	Junos OS System Log Alternate Facilities for Remote Logging . . . . .	38
	Adding a Text String to System Log Messages . . . . .	39
	Specifying Log File Size, Number, and Archiving Properties . . . . .	40
	Including Priority Information in System Log Messages . . . . .	41
	System Log Facility Codes and Numerical Codes Reported in Priority Information . . . . .	43
	Including the Year or Millisecond in Timestamps . . . . .	45
	Using Regular Expressions to Refine the Set of Logged Messages . . . . .	45
	Junos System Log Regular Expression Operators for the match Statement . . . . .	47
	Disabling the System Logging of a Facility . . . . .	48
<b>Chapter 3</b>	<b>Configuring System Log Messages for a TX Matrix Router . . . . .</b>	<b>51</b>
	Configuring System Logging for a TX Matrix Router . . . . .	51
	Configuring Message Forwarding to the TX Matrix Router . . . . .	53
	Configuring Optional Features for Forwarded Messages on a TX Matrix Router . . . . .	54
	Including Priority Information in Forwarded Messages . . . . .	54
	Adding a Text String to Forwarded Messages . . . . .	55
	Using Regular Expressions to Refine the Set of Forwarded Messages . . . . .	55
	Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router . . . . .	55
	Configuring System Logging Differently on Each T640 Router in a Routing Matrix . . . . .	56
<b>Chapter 4</b>	<b>Configuring System Log Messages for a TX Matrix Plus Router . . . . .</b>	<b>59</b>
	Configuring System Logging for a TX Matrix Plus Router . . . . .	59
	Configuring Message Forwarding to the TX Matrix Plus Router . . . . .	61
	Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router . . . . .	62
	Including Priority Information in Forwarded Messages . . . . .	63
	Adding a Text String to Forwarded Messages . . . . .	63
	Using Regular Expressions to Refine the Set of Forwarded Messages . . . . .	63

	Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router . . . . .	63
	Configuring System Logging Differently on Each T1600 Router in a Routing Matrix . . . . .	65
<b>Chapter 5</b>	<b>Examples . . . . .</b>	<b>67</b>
	Examples: Configuring System Logging . . . . .	67
	Examples: Assigning an Alternative Facility . . . . .	69
	Examples: Displaying a Log File . . . . .	69
	Examples: Displaying System Log Message Descriptions . . . . .	70
<b>Chapter 6</b>	<b>Configuration Statements . . . . .</b>	<b>73</b>
	System Management Configuration Statements . . . . .	73
	allow-duplicates . . . . .	80
	archive (All System Log Files) . . . . .	81
	archive (Individual System Log File) . . . . .	82
	console (System Logging) . . . . .	83
	destination-override . . . . .	84
	explicit-priority . . . . .	85
	facility-override . . . . .	85
	file (System Logging) . . . . .	86
	files . . . . .	87
	host . . . . .	88
	log-prefix . . . . .	90
	log-rotate-frequency . . . . .	90
	match . . . . .	91
	no-remote-trace . . . . .	91
	port . . . . .	91
	size . . . . .	92
	system . . . . .	92
	structured-data . . . . .	93
	syslog . . . . .	94
	time-format . . . . .	96
	tracing . . . . .	97
	user (System Logging) . . . . .	98
	world-readable . . . . .	99
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 7</b>	<b>Administrative Commands . . . . .</b>	<b>103</b>
	clear log . . . . .	104
<b>Chapter 8</b>	<b>Monitoring Commands . . . . .</b>	<b>105</b>
	monitor list . . . . .	106
	monitor start . . . . .	107
	show log . . . . .	109
	monitor stop . . . . .	111
<b>Part 4</b>	<b>Index</b>	
	Index . . . . .	115



# List of Tables

	<b>About the Documentation . . . . .</b>	<b>ix</b>
	Table 1: Notice Icons . . . . .	xi
	Table 2: Text and Syntax Conventions . . . . .	xi
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>System Log Messages Overview . . . . .</b>	<b>3</b>
	Table 3: Example: Local and Forwarded Severity Level Are Both info . . . . .	7
	Table 4: Example: Local Severity Is notice, Forwarded Severity Is critical . . . . .	8
	Table 5: Example: Local Severity Is critical, Forwarded Severity Is notice . . . . .	8
	Table 6: Example: Local and Forwarded Severity Level Are Both info . . . . .	9
	Table 7: Example: Local Severity Is notice, Forwarded Severity Is critical . . . . .	10
	Table 8: Example: Local Severity Is critical, Forwarded Severity Is notice . . . . .	10
	Table 9: Fields in System Log Message Descriptions . . . . .	12
	Table 10: Fields in Structured-Data Messages . . . . .	14
	Table 11: Facility and Severity Codes in the priority-code Field . . . . .	16
	Table 12: Platform Identifiers in the platform Field . . . . .	17
	Table 13: Fields in Standard-Format Messages Generated by a Junos Process or Library . . . . .	18
	Table 14: Fields in Messages Generated by a PIC . . . . .	20
	Table 15: Format of message-source Field in Messages Logged on TX Matrix Platform . . . . .	21
	Table 16: Format of message-source Field in Messages Logged on TX Matrix Platform . . . . .	22
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Configuring System Log Messages for a Single-Chassis System . . . . .</b>	<b>27</b>
	Table 17: Minimum Configuration Statements for System Logging . . . . .	29
	Table 18: Default System Logging Settings . . . . .	29
	Table 19: Default Facilities for Messages Directed to a Remote Destination . . . . .	38
	Table 20: Facilities for the facility-override Statement . . . . .	38
	Table 21: Facility Codes Reported in Priority Information . . . . .	43
	Table 22: Numerical Codes for Severity Levels Reported in Priority Information . . . . .	44
	Table 23: Regular Expression Operators for the match Statement . . . . .	46
	Table 24: Regular Expression Operators for the match Statement . . . . .	47
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 8</b>	<b>Monitoring Commands . . . . .</b>	<b>105</b>

Table 25: monitor list Output Fields .....	106
Table 26: monitor start Output Fields .....	107



# About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Using the Examples in This Manual on page ix
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- M Series
- MX Series
- T Series
- J Series

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the [Junos OS CLI User Guide](#).

## Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b> No alarms currently active

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<b>stub</b> <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members [</b> <i>community-ids</i> <b>]</b>
Indentation and braces ( { } )	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>J-Web GUI Conventions</b>		
<b>Bold text like this</b>	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

## PART 1

# Overview

- [System Log Messages Overview on page 3](#)





## CHAPTER 1

# System Log Messages Overview

- [Junos OS System Log Configuration Overview on page 3](#)
- [Junos OS Platform-Specific Default System Log Messages on page 4](#)
- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router on page 7](#)
- [Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router on page 9](#)
- [Displaying a Log File from a Single-Chassis System on page 11](#)
- [Displaying a Log File from a Routing Matrix on page 11](#)
- [Displaying and Interpreting System Log Message Descriptions on page 12](#)
- [Interpreting Messages Generated in Structured-Data Format on page 14](#)
- [Interpreting Messages Generated in Standard Format by a Junos Process or Library on page 18](#)
- [Interpreting Messages Generated in Standard Format by Services on a PIC on page 19](#)
- [The message-source Field on a Single-Chassis System on page 20](#)
- [The message-source Field on a TX Matrix Platform on page 21](#)
- [The message-source Field on a T640 Routing Node in a Routing Matrix on page 22](#)

## Junos OS System Log Configuration Overview

---

The Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the router, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a peer process
- Emergency or critical conditions, such as router power-down due to excessive temperature

Each system log message identifies the Junos OS process that generated the message and briefly describes the operation or error that occurred. For detailed information about specific system log messages, see the [Junos OS System Log Messages Reference](#).



**NOTE:** This topic describes system log messages for Junos OS processes and libraries and not the system logging services on a Physical Interface Card (PIC) such as the Adaptive Services PIC. For information about configuring system logging for PIC services, see the [Junos OS Services Interfaces Configuration Guide](#).

**Related  
Documentation**

- [Junos OS System Log Configuration Hierarchy on page 28](#)
- [Junos OS Minimum System Logging Configuration on page 28](#)

---

## Junos OS Platform-Specific Default System Log Messages

---

The following messages are generated by default on specific routers. To view any of these types of messages, you must configure at least one destination for messages as described in “[Junos OS Minimum System Logging Configuration](#)” on page 28.

- On J Series routers, a message is logged when a process running in the kernel consumes 500 or more consecutive milliseconds of CPU time.

To log the kernel process message on an M Series, MX Series, or T Series router, include the **kernel info** statement at the appropriate hierarchy level:

```
[edit system syslog]
(console | file filename | host destination | user username) {
  kernel info;
}
```

- On a routing matrix composed of a TX Matrix router and T640 routers, the master Routing Engine on each T640 router forwards all messages with a severity of **info** and higher to the master Routing Engine on the TX Matrix router. This is equivalent to the following configuration statement included on the TX Matrix router:

```
[edit system syslog]
host scc-master {
  any info;
}
```

- Likewise, on a routing matrix composed of a TX Matrix Plus router and T1600 routers, the master Routing Engine on each T1600 router forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix Plus router:

```
[edit system syslog]
host sfc0-master {
  any info;
}
```

- Related Documentation**
- [Junos OS System Log Configuration Overview on page 3](#)
  - [Junos OS Default System Log Settings on page 29](#)

---

## Single-Chassis System Logging Configuration Overview

---

The Junos system logging utility is similar to the UNIX **syslogd** utility. This section describes how to configure system logging for a single-chassis system that runs the Junos OS.

System logging configuration for the Junos-FIPS software and for Juniper Networks routers in a Common Criteria environment is the same as for the Junos OS. For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

For information about configuring system logging for a routing matrix composed of a TX Matrix router and T640 routers, see [“Configuring System Logging for a TX Matrix Router” on page 51](#).

Each system log message belongs to a *facility*, which groups together related messages. Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions. You always specify the facility and severity of the messages to include in the log. For more information, see [“Specifying the Facility and Severity of Messages to Include in the Log” on page 31](#).

You direct messages to one or more destinations by including the appropriate statement at the **[edit system syslog]** hierarchy level:

- To a named file in a local file system, by including the **file** statement. See [“Directing System Log Messages to a Log File” on page 32](#).
- To the terminal session of one or more specific users (or all users) when they are logged in to the router, by including the **user** statement. See [“Directing System Log Messages to a User Terminal” on page 33](#).
- To the router console, by including the **console** statement. See [“Directing System Log Messages to the Console” on page 34](#).
- To a remote machine that is running the **syslogd** utility or to the other Routing Engine on the router, by including the **host** statement. See [“Directing System Log Messages to a Remote Machine or the Other Routing Engine” on page 34](#).

By default, messages are logged in a standard format, which is based on a UNIX system log format; for detailed information about message formatting, see the [Junos OS System Log Messages Reference](#). You can alter the content and format of logged messages in the following ways:

- You can log messages to a file in structured-data format instead of the standard Junos format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from the message. For more information, see [“Logging Messages in Structured-Data Format” on page 32](#).
- A message's facility and severity level are together referred to as its *priority*. By default, the standard Junos format for messages does not include priority information (structured-data format includes a priority code by default.) To include priority information in standard-format messages directed to a file or a remote destination, include the **explicit-priority** statement. For more information, see [“Including Priority Information in System Log Messages” on page 41](#).
- By default, the standard Junos format for messages specifies the month, date, hour, minute, and second when the message was logged. You can modify the timestamp on standard-format system log messages to include the year, the millisecond, or both. (Structured-data format specifies the year and millisecond by default.) For more information, see [“Including the Year or Millisecond in Timestamps” on page 45](#).
- When directing messages to a remote machine, you can specify the IP address that is reported in messages as their source. You can also configure features that make it easier to separate messages generated by the Junos OS or messages generated on particular routers. For more information, see [“Directing System Log Messages to a Remote Machine or the Other Routing Engine” on page 34](#).
- The predefined facilities group together related messages, but you can also use regular expressions to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination. For more information, see [“Using Regular Expressions to Refine the Set of Logged Messages” on page 45](#).

#### Related Documentation

- [Examples: Configuring System Logging on page 67](#)
- [Specifying the Facility and Severity of Messages to Include in the Log on page 31](#)
- [Junos OS System Logging Facilities and Message Severity Levels](#)
- [Directing System Log Messages to a Log File on page 32](#)
- [Directing System Log Messages to a User Terminal on page 33](#)
- [Directing System Log Messages to the Console on page 34](#)
- [Directing System Log Messages to a Remote Machine or the Other Routing Engine on page 34](#)

## Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router

This topic describes the impact of different local and forwarded severity levels configured for system log messages on a TX Matrix router:

- [Messages Logged When the Local and Forwarded Severity Levels Are the Same on page 7](#)
- [Messages Logged When the Local Severity Level Is Lower on page 7](#)
- [Messages Logged When the Local Severity Level Is Higher on page 8](#)

### Messages Logged When the Local and Forwarded Severity Levels Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix router contains all messages from the logs on the T640 routers. For example, you can specify severity **info** for the `/var/log/messages` file, which is the default severity level for messages forwarded by T640 routers:

```
[edit system syslog]
file messages {
  any info;
}
```

[Table 3 on page 7](#) specifies which messages are included in the logs on the T640 routers and the TX Matrix router.

**Table 3: Example: Local and Forwarded Severity Level Are Both info**

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	<b>info</b>
TX Matrix router	Local	<b>info</b>
	Forwarded from T640 routers	<b>info</b>

### Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix router includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, on a TX Matrix router, you can specify severity **notice** for the `/var/log/messages` file and severity **critical** for forwarded messages:

```
[edit system syslog]
file messages {
  any notice;
}
host scc-master {
```

```

    any critical;
}

```

Table 4 on page 8 specifies which messages in a routing matrix are included in the logs on the T640 routers and the TX Matrix router. The T640 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix router does not include the messages with severity **error**, **warning**, or **notice** that the T640 routers log locally.

**Table 4: Example: Local Severity Is notice, Forwarded Severity Is critical**

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	<b>notice</b>
TX Matrix router	Local	<b>notice</b>
	Forwarded from T640 routers	<b>critical</b>

### Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix router includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity **critical** for the `/var/log/messages` file and severity **notice** for forwarded messages:

```

[edit system syslog]
file messages {
    any critical;
}
host scc-master {
    any notice;
}

```

Table 5 on page 8 specifies which messages are included in the logs on the T640 routers and the TX Matrix router. Although the T640 routers forward messages with severity **notice** and higher, the TX Matrix router discards any of those messages with severity lower than **critical** (does not log forwarded messages with severity **error**, **warning**, or **notice**). None of the logs include messages with severity **error** or lower.

**Table 5: Example: Local Severity Is critical, Forwarded Severity Is notice**

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	<b>critical</b>
TX Matrix router	Local	<b>critical</b>
	Forwarded from T640 routers	<b>critical</b>

- Related Documentation
- [Configuring System Logging for a TX Matrix Router on page 51](#)

## Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router

This topic describes the impact of different local and forwarded severity levels configured for the system log messages on a TX Matrix Plus router:

- [Messages Logged When the Local and Forwarded Severity Levels Are the Same on page 9](#)
- [Messages Logged When the Local Severity Level Is Lower on page 9](#)
- [Messages Logged When the Local Severity Level Is Higher on page 10](#)

### Messages Logged When the Local and Forwarded Severity Levels Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix Plus router contains all messages from the logs on the T1600 routers in the routing matrix. For example, you can specify severity **info** for the `/var/log/messages` file, which is the default severity level for messages forwarded by T1600 routers:

```
[edit system syslog]
file messages {
  any info;
}
```

[Table 6 on page 9](#) specifies which messages in a routing matrix based on a TX Matrix Plus router are included in the logs on the T1600 routers and the TX Matrix Plus router:

Table 6: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	info
TX Matrix Plus router	Local	info
	Forwarded from T1600 routers	info

### Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix Plus router includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, on a TX Matrix Plus router, you can specify severity **notice** for the `/var/log/messages` file and severity **critical** for forwarded messages:

```
[edit system syslog]
file messages {
  any notice;
```

```

}
host sfc0-master {
  any critical;
}

```

Table 7 on page 10 specifies which messages in a routing matrix are included in the logs on the T1600 routers and the TX Matrix Plus router. The T1600 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix Plus router does not include the messages with severity **error**, **warning**, or **notice** that the T1600 routers log locally.

**Table 7: Example: Local Severity Is notice, Forwarded Severity Is critical**

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	<b>notice</b>
TX Matrix Plus router	Local	<b>notice</b>
	Forwarded from T1600 routers	<b>critical</b>

## Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix Plus router includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity **critical** for the `/var/log/messages` file and severity **notice** for forwarded messages:

```

[edit system syslog]
file messages {
  any critical;
}
host sfc0-master {
  any notice;
}

```

Table 8 on page 10 specifies which messages are included in the logs on the T1600 routers and the TX Matrix Plus router. Although the T1600 routers forward messages with severity **notice** and higher, the TX Matrix Plus router discards any of those messages with severity lower than **critical** (does not log forwarded messages with severity **error**, **warning**, or **notice**). None of the logs include messages with severity **error** or lower.

**Table 8: Example: Local Severity Is critical, Forwarded Severity Is notice**

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	<b>critical</b>
TX Matrix Plus router	Local	<b>critical</b>
	Forwarded from T1600 routers	<b>critical</b>



- Related Documentation**
- [Configuring System Logging for a TX Matrix Plus Router on page 59](#)

## Displaying a Log File from a Single-Chassis System

To display a log file stored on a single-chassis system, enter Junos OS CLI operational mode and issue either of the following commands:

```
user@host> show log log-filename
user@host> file show log-file-pathname
```

By default, the commands display the file stored on the local Routing Engine. To display the file stored on a particular Routing Engine, prefix the file- or pathname with the string **re0** or **re1** and a colon. The following examples both display the `/var/log/messages` file stored on the Routing Engine in slot 1:

```
user@host> show log re1:messages
user@host> file show re1:/var/log/messages
```

For information about the fields in a log message, see [“Interpreting Messages Generated in Standard Format by a Junos Process or Library” on page 18](#), [“Interpreting Messages Generated in Standard Format by Services on a PIC” on page 19](#), and [“Interpreting Messages Generated in Structured-Data Format” on page 14](#). For examples, see [“Examples: Displaying a Log File” on page 69](#).

## Displaying a Log File from a Routing Matrix

One way to display a log file stored on the local Routing Engine of any of the individual platforms in a routing matrix (T640 routing nodes or TX Matrix platform) is to log in to a Routing Engine on the platform, enter Junos OS CLI operational mode, and issue the **show log** or **file show** command described in [“Displaying a Log File from a Single-Chassis System” on page 11](#).

To display a log file stored on a T640 routing node during a terminal session on the TX Matrix platform, issue the **show log** or **file show** command and add a prefix that specifies the T640 routing node's LCC index number as **lccn**, followed by a colon. The index can be from 0 (zero) through 3:

```
user@host> show log lccn:log-filename
user@host> file show lccn:log-file-pathname
```

By default, the **show log** and **file show** commands display the specified log file stored on the master Routing Engine on the T640 routing node. To display the log from a particular Routing Engine, prefix the file- or pathname with the string **lccn-master**, **lccn-re0**, or **lccn-re1**, followed by a colon. The following examples all display the `/var/log/messages` file stored on the master Routing Engine (in slot 0) on routing node LCC2:

```
user@host> show log lcc2:messages
user@host> show log lcc2-master:messages
user@host> show log lcc2-re0:messages
user@host> file show lcc2:/var/log/messages
```

If the T640 routing nodes are forwarding messages to the TX Matrix platform (as in the default configuration), another way to view messages generated on a T640 routing node during a terminal session on the TX Matrix platform is simply to display a local log file. However, the messages are intermixed with messages from other T640 routing nodes and the TX Matrix platform itself. For more information about message forwarding, see “Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router” on page 7.

For information about the fields in a log message, see “Interpreting Messages Generated in Structured-Data Format” on page 14, “Interpreting Messages Generated in Standard Format by Services on a PIC” on page 19, and “Interpreting Messages Generated in Standard Format by a Junos Process or Library” on page 18. For examples, see “Examples: Displaying a Log File” on page 69.

## Displaying and Interpreting System Log Message Descriptions

This reference lists the messages available at the time of its publication. To display the list of messages that applies to the version of the Junos OS that is running on a routing platform, enter Junos OS CLI operational mode and issue the following command:

```
user@host> help syslog ?
```

To display the list of available descriptions for tags whose names begin with a specific character string, substitute the string (in all capital letters) for the variable **TAG-PREFIX** (there is no space between the prefix and the question mark):

```
user@host> help syslog TAG-PREFIX?
```

To display the complete descriptions for tags whose name includes a regular expression, substitute a Perl-based expression for the variable **regex**. The match is not case-sensitive. For information about Perl-based regular expressions, consult a Perl reference manual or website such as <http://perldoc.perl.org>.

```
user@host> help syslog regex
```

To display the complete description of a particular message, substitute its name for the variable **TAG** (in all capital letters):

```
user@host> help syslog TAG
```

Table 9 on page 12 describes the fields in a system log message description in this reference or in the CLI.

**Table 9: Fields in System Log Message Descriptions**

Field Name in Reference	Field Name in CLI	Description
—	<b>Name</b>	The message tag in all capital letters.

Table 9: Fields in System Log Message Descriptions (*continued*)

Field Name in Reference	Field Name in CLI	Description
<b>System Log Message</b>	<b>Message</b>	<p>Text of the message written to the system log. In the log, a specific value is substituted for each variable that appears in italics in this reference or in angle brackets (&lt; &gt;) in the CLI.</p> <p>In this reference, the message text appears on the second line of the <b>System Log Message</b> field. The first line is the message tag (the same text as in the CLI Name field). The prefix on each tag identifies the message source and the rest of the tag indicates the specific event or error.</p>
—	<b>Help</b>	<p>Short description of the message, which also appears in the right-hand column of CLI output for the <b>help syslog</b> command when the output lists multiple messages.</p>
<b>Description</b>	<b>Description</b>	More detailed explanation of the message.
<b>Type</b>	<b>Type</b>	<p>Category to which the message belongs:</p> <ul style="list-style-type: none"> <li>• <b>Error:</b> The message reports an error or failure condition that might require corrective action.</li> <li>• <b>Event:</b> The message reports a condition or occurrence that does not generally require corrective action.</li> </ul>
<b>Severity</b>	<b>Severity</b>	<p>Message severity level as described in Table: <b>System Log Message Severity Levels</b> in Specifying the Facility and Severity of Messages to Include in the Log.</p>
<b>Cause</b>	<b>Cause</b>	<p>(Optional) Possible cause for message generation. There can be more than one cause.</p>

Table 9: Fields in System Log Message Descriptions (*continued*)

Field Name in Reference	Field Name in CLI	Description
Action	Action	(Optional) Action you can perform to resolve the error or failure condition described in the message. If this field does not appear in an entry, either no action is required or the action is self-explanatory.

## Interpreting Messages Generated in Structured-Data Format

Beginning in Junos OS Release 8.3, when the **structured-data** statement is included in the configuration for a log file, Junos processes and software libraries write messages to the file in structured-data format instead of the standard Junos format. For information about the **structured-data** statement, see [“Logging Messages in Structured-Data Format” on page 32](#).

Structured-format makes it easier for automated applications to extract information from the message. In particular, the standardized format for reporting the value of variables (elements in the English-language message that vary depending on the circumstances that triggered the message) makes it easy for an application to extract those values. In standard format, the variables are interspersed in the message text and not identified as variables.

The structured-data format for a message includes the following fields (which appear here on two lines only for legibility):

```
<priority code>version timestamp hostname process processID TAG [junos@2636.platform
variable-value-pairs] message-text
```

[Table 10 on page 14](#) describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen ( - ) appears instead.

Table 10: Fields in Structured-Data Messages

Field	Description	Examples
<b>&lt;priority code&gt;</b>	Number that indicates the message's facility and severity. It is calculated by multiplying the facility number by 8 and then adding the numerical value of the severity. For a mapping of the numerical codes to facility and severity, see <a href="#">Table: Facility and Severity Codes in the priority-code Field</a> in <a href="#">Specifying the Facility and Severity of Messages to Include in the Log</a> .	<165> for a message from the pfe facility (facility=20) with severity notice (severity=5).
<b>version</b>	Version of the Internet Engineering Task Force (IETF) system logging protocol specification.	1 for the initial version

Table 10: Fields in Structured-Data Messages (*continued*)

Field	Description	Examples
<i>timestamp</i>	Time when the message was generated, in one of two representations: <ul style="list-style-type: none"> <li><b>YYYY-MM-DDTHH:MM:SS.MSZ</b> is the year, month, day, hour, minute, second and millisecond in Universal Coordinated Time (UTC)</li> <li><b>YYYY-MM-DDTHH:MM:SS.MS+/-HH:MM</b> is the year, month, day, hour, minute, second and millisecond in local time; the hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from UTC</li> </ul>	2007-02-15T09:17:15.719Z is 9:17 AM UTC on 15 February 2007. 2007-02-15T01:17:15.719-08:00 is the same timestamp expressed as Pacific Standard Time in the United States.
<i>hostname</i>	Name of the host that originally generated the message.	router1
<i>process</i>	Name of the Junos process that generated the message.	mgd
<i>processID</i>	UNIX process ID (PID) of the Junos process that generated the message.	3046
<i>TAG</i>	Junos system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
<i>junos@2636.platform</i>	An identifier for the type of hardware platform that generated the message. The <i>junos@2636</i> prefix indicates that the platform runs the Junos OS. It is followed by a dot-separated numerical identifier for the platform type. For a list of the identifiers, see <a href="#">Table 12 on page 17</a> .	junos@2636.1.1.2.18 for the M120 router
<i>variable-value-pairs</i>	A variable-value pair for each element in the <i>message-text</i> string that varies depending on the circumstances that triggered the message. Each pair appears in the format <b>variable = "value"</b> .	username="regress"
<i>message-text</i>	English-language description of the event or error (omitted if the brief statement is included at the [edit system syslog file filename structured-data] hierarchy level). For the text for each message, see the chapters following System Log Messages.	User 'regress' exiting configuration mode

By default, the structured-data version of a message includes English text at the end, as in the following example (which appears on multiple lines only for legibility):

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username="regress"] User 'regress' exiting configuration mode
```

When the brief statement is included at the `[edit system syslog file filename structured-data ]` hierarchy level, the English text is omitted, as in this example:

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username="regress"]
```

[Table 11 on page 16](#) maps the codes that appear in the **priority-code** field to facility and severity level.



**NOTE:** Not all of the facilities and severities listed in [Table 11 on page 16](#) can be included in statements at the `[edit system syslog]` hierarchy level (some are used by internal processes). For a list of the facilities and severity levels that can be included in the configuration, see [Specifying the Facility and Severity of Messages to Include in the Log](#).

**Table 11: Facility and Severity Codes in the priority-code Field**

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
kernel (0)	1	1	2	3	4	5	6	7
user (1)	8	9	10	11	12	13	14	15
mail (2)	16	17	18	19	20	21	22	23
daemon (3)	24	25	26	27	28	29	30	31
authorization (4)	32	33	34	35	36	37	38	39
syslog (5)	40	41	42	43	44	45	46	47
printer (6)	48	49	50	51	52	53	54	55
news (7)	56	57	58	59	60	61	62	63
uucp (8)	64	65	66	67	68	69	70	71
clock (9)	72	73	74	75	76	77	78	79
authorization-private (10)	80	81	82	83	84	85	86	87
ftp (11)	88	89	90	91	92	93	94	95
ntp (12)	96	97	98	99	100	101	102	103
security (13)	104	105	106	107	108	109	110	111

Table 11: Facility and Severity Codes in the priority-code Field (*continued*)

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
console (14)	112	113	114	115	116	117	118	119
local0 (16)	128	129	130	131	132	133	134	135
dfc (17)	136	137	138	139	140	141	142	143
local2 (18)	144	145	146	147	148	149	150	151
firewall (19)	152	153	154	155	156	157	158	159
pfe (20)	160	161	162	163	164	165	166	167
conflict-log (21)	168	169	170	171	172	173	174	175
change-log (22)	176	177	178	179	180	181	182	183
interactive-commands (23)	184	185	186	187	188	189	190	191

Table 12 on page 17 lists the numerical identifiers for routing platforms that appear in the **platform** field. The identifier is derived from the platform's SNMP object identifier (OID) as defined in the Juniper Networks routing platform MIB. For more information about OIDs, see the *Junos Network Management Configuration Guide*.

Table 12: Platform Identifiers in the platform Field

Identifier	Platform Name
1.1.1.2.1	M40 router
1.1.1.2.2	M20 router
1.1.1.2.3	M160 router
1.1.1.2.4	M10 router
1.1.1.2.5	M5 router
1.1.1.2.6	T640 routing node
1.1.1.2.7	T320 router
1.1.1.2.8	M40e router
1.1.1.2.9	M320 router
1.1.1.2.10	M7i router

Table 12: Platform Identifiers in the platform Field (*continued*)

Identifier	Platform Name
1.1.1.2.11	M10i router
1.1.1.2.13	J2300 Services Router
1.1.1.2.14	J4300 Services Router
1.1.1.2.15	J6300 Services Router
1.1.1.2.17	TX Matrix platform
1.1.1.2.18	M120 router
1.1.1.2.19	J4350 Services Router
1.1.1.2.20	J6350 Services Router
1.1.1.2.23	J2320 Services Router
1.1.1.2.24	J2350 Services Router
1.1.1.2.27	T1600 router
1.1.1.2.83	T4000 router

## Interpreting Messages Generated in Standard Format by a Junos Process or Library

The syntax of a standard-format message generated by a Junos OS process or subroutine library depends on whether it includes priority information:

- When the **explicit-priority** statement is included at the [**edit system syslog file *filename***] or [**edit system syslog host (*hostname* | other-routing-engine)**] hierarchy level, a system log message has the following syntax:

```
timestamp message-source: %facility-severity-TAG: message-text
```

- When directed to the console or to users, or when the **explicit-priority** statement is not included for files or remote hosts, a system log message has the following syntax:

```
timestamp message-source: TAG: message-text
```

Table 13 on page 18 describes the message fields.

Table 13: Fields in Standard-Format Messages Generated by a Junos Process or Library

Field	Description
<i>timestamp</i>	Time at which the message was logged.



Table 13: Fields in Standard-Format Messages Generated by a Junos Process or Library (*continued*)

Field	Description
<i>message-source</i>	Identifier of the process or component that generated the message and the routing platform on which the message was logged. This field includes two or more subfields, depending on how system logging is configured. See “ <a href="#">The message-source Field on a TX Matrix Platform</a> ” on page 21, “ <a href="#">The message-source Field on a T640 Routing Node in a Routing Matrix</a> ” on page 22, and “ <a href="#">The message-source Field on a Single-Chassis System</a> ” on page 20.
<i>facility</i>	Code that specifies the facility to which the system log message belongs. For a mapping of codes to facility names, see Table: <b>Facility Codes Reported in Priority Information</b> in Including Priority Information in System Log Messages.
<i>severity</i>	Numerical code that represents the severity level assigned to the system log message. For a mapping of codes to severity names, see Table: <b>Numerical Codes for Severity Levels Reported in Priority Information</b> in Including Priority Information in System Log Messages.
<i>TAG</i>	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating software process or library. The entries in this reference are ordered alphabetically by this prefix.  Not all processes on a routing platform use tags, so this field does not always appear.
<i>message-text</i>	Text of the message. For the text for each message, see the chapters following System Log Messages.

## Interpreting Messages Generated in Standard Format by Services on a PIC

Standard-format system log messages generated by services on a PIC, such as the Adaptive Services (AS) PIC, have the following syntax:

```
timestamp (FPC Slot fpc-slot, PIC Slot pic-slot) {service-set} [SERVICE]:
optional-string TAG: message-text
```



**NOTE:** System logging for services on PICs is not configured at the [edit system syslog] hierarchy level as discussed in this chapter. For configuration information, see the *Junos Services Interfaces Configuration Guide*.

The (FPC Slot *fpc-slot*, PIC Slot *pic-slot*) field appears only when the standard system logging utility that runs on the Routing Engine writes the messages to the system log. When the PIC writes the message directly, the field does not appear.

Table 14 on page 20 describes the message fields.

Table 14: Fields in Messages Generated by a PIC

Field	Description
<i>timestamp</i>	Time at which the message was logged.
<i>fpc-slot</i>	Slot number of the Flexible PIC Concentrator (FPC) that houses the PIC that generated the message.
<i>pic-slot</i>	Number of the PIC slot on the FPC in which the PIC that generated the message resides.
<i>service-set</i>	Name of the service set that generated the message.
<i>SERVICE</i>	Code representing the service that generated the message. The codes include the following: <ul style="list-style-type: none"> <li>• FWNAT—Network Address Translation (NAT) service</li> <li>• IDS—Intrusion detection service</li> </ul>
<i>optional-string</i>	A text string that appears if the configuration for the PIC includes the log-prefix statement at the [edit interfaces interface-name services-options syslog] hierarchy level. For more information, see the <i>Junos Services Interfaces Configuration Guide</i> .
<i>TAG</i>	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating PIC. The entries in this reference are ordered alphabetically by this prefix.
<i>message-text</i>	Text of the message. For the text of each message, see System Log Messages.

## The message-source Field on a Single-Chassis System

The format of the **message-source** field in a message on a single-chassis system depends on whether the message was generated on the local Routing Engine or the other Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the [edit system syslog host] hierarchy level.

- When the local Routing Engine generated the message, there are two subfields:

*hostname process[process-ID]*

- When the other Routing Engine generated the message, there are three subfields:

*hostname reX process[process-ID]*

**hostname** is the hostname of the local Routing Engine.

**process[process-ID]** is the name and PID of the process that generated the message. If the **reX** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [process-ID] part does not appear.

**reX** indicates that the other Routing Engine generated the message (*X* is **0** or **1**).

## The message-source Field on a TX Matrix Platform

The format of the *message-source* field in a message on a TX Matrix platform depends on several factors:

- Whether the message was generated on the TX Matrix platform or a T640 routing node in the routing matrix. By default, the master Routing Engine on each T640 routing node forwards messages from all facilities with severity info and higher to the master Routing Engine on the TX Matrix platform. When you configure system logging on the TX Matrix platform, its logs include the forwarded messages. For more information, see [“Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router”](#) on page 7.
- Whether the message was generated on the local Routing Engine or the other Routing Engine on the originating machine (TX Matrix platform or T640 routing node). Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the **[edit system syslog host]** hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 15 on page 21 specifies the format of the message-source field in the various cases.

**Table 15: Format of message-source Field in Messages Logged on TX Matrix Platform**

Generating Machine	Generating Routing Engine	Process or Component	Format
TX Matrix platform	Local	Process	<i>hostname process[processID]</i>
		Component	<i>hostname scc-reX process[processID]</i>
	Other	Process	<i>hostname scc-reX scc-componentZ process</i>
		Component	<i>hostname scc-reX scc-componentZ process</i>
T640 routing node	Local	Process	<i>hostname lccY-masterprocess[processID]</i>
		Component	<i>hostname lccY-master scc-componentZ process</i>
	Other	Process	<i>hostname lccY-master lccY-reX process[processID]</i>
		Component	<i>hostname lccY-master lccY-reX lccY-componentZ process</i>

**hostname** is the hostname of the local Routing Engine on the TX Matrix platform.

**lccY-master** is the master Routing Engine on the T640 routing node with the indicated LCC index number (*Y* is from 0 through 3).

**lccY-reX** indicates that the backup Routing Engine on the T640 routing node generated the message (*X* is 0 or 1). The routing node has the indicated LCC index number (*Y* matches the value in the **lccY-master** field).

**lccY-componentZ** process identifies the hardware component and process on the T640 routing node that generated the message (*Y* matches the value in the **lccY-master** field and the range of values for *Z* depends on the component type). For example, **lcc2-fpc1 PFEMAN** refers to a process on the FPC in slot 1 on the T640 routing node with index LCC2.

**process[process-ID]** is the name and PID of the kernel or user-space process that generated the message. If the **scc-reX** or **lccY-reX** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the **[process-ID]** part does not appear.

**scc-componentZ** process identifies the hardware component and process on the TX Matrix platform that generated the message (the range of values for *Z* depends on the component type). For example, **smb1 GSIB** refers to a process on one of the processor boards in the Switch Interface Board (SIB) with index 1.

**scc-reX** indicates that the other Routing Engine on the TX Matrix platform generated the message (*X* is 0 or 1).

## The message-source Field on a T640 Routing Node in a Routing Matrix

The format of the **message-source** field in a message on a T640 routing node in a routing matrix depends on two factors:

- Whether the message was generated on the local Routing Engine or the other Routing Engine. Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the **[edit system syslog host]** hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 16 on page 22 specifies the format of the **message-source** field in the various cases.

**Table 16: Format of message-source Field in Messages Logged on TX Matrix Platform**

Generating Routing Engine	Process or Component	Format
Local	Process	<i>hostname-lccY process[processID]</i>
	Component	<i>hostname-lccY lccY-componentZ process</i>

Table 16: Format of message-source Field in Messages Logged on TX Matrix Platform (*continued*)

Generating Routing Engine	Process or Component	Format
Other	Process	<i>hostname-lccY lccY-reX process[processID]</i>
	Component	<i>hostname-lccY lccY-reX lccY-componentZ process</i>

*hostname-lccY* is the hostname of the local Routing Engine and the T640 routing node's LCC index number.

*lccY-componentZ* process identifies the hardware component and process that generated the message (*Y* matches the value in the *hostname-lccY* field and the range of values for *Z* depends on the component type). For example, lcc0-fpc0 CMLC refers to a process on the FPC in slot 0. The T640 routing node has index LCC0 in the routing matrix.

*lccY-reX* indicates that the other Routing Engine on the routing node generated the message (*Y* matches the value in the *hostname-lccY* field and *X* is 0 or 1).

*process[process-ID]* is the name and PID of the kernel or user-space process that generated the message. If the *lccY-reX* field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the *[process-ID]* part does not appear.



## PART 2

# Configuration

- [Configuring System Log Messages for a Single-Chassis System on page 27](#)
- [Configuring System Log Messages for a TX Matrix Router on page 51](#)
- [Configuring System Log Messages for a TX Matrix Plus Router on page 59](#)
- [Examples on page 67](#)
- [Configuration Statements on page 73](#)





## CHAPTER 2

# Configuring System Log Messages for a Single-Chassis System

- [Junos OS System Log Configuration Hierarchy on page 28](#)
- [Junos OS Minimum System Logging Configuration on page 28](#)
- [Junos OS Default System Log Settings on page 29](#)
- [Junos OS Platform-Specific Default System Log Messages on page 30](#)
- [Specifying the Facility and Severity of Messages to Include in the Log on page 31](#)
- [Directing System Log Messages to a Log File on page 32](#)
- [Logging Messages in Structured-Data Format on page 32](#)
- [Directing System Log Messages to a User Terminal on page 33](#)
- [Directing System Log Messages to the Console on page 34](#)
- [Directing System Log Messages to a Remote Machine or the Other Routing Engine on page 34](#)
- [Specifying an Alternative Source Address for System Log Messages on page 35](#)
- [Changing the Alternative Facility Name for Remote System Log Messages on page 36](#)
- [System Log Default Facilities for Messages Directed to a Remote Destination on page 37](#)
- [Junos OS System Log Alternate Facilities for Remote Logging on page 38](#)
- [Adding a Text String to System Log Messages on page 39](#)
- [Specifying Log File Size, Number, and Archiving Properties on page 40](#)
- [Including Priority Information in System Log Messages on page 41](#)
- [System Log Facility Codes and Numerical Codes Reported in Priority Information on page 43](#)
- [Including the Year or Millisecond in Timestamps on page 45](#)
- [Using Regular Expressions to Refine the Set of Logged Messages on page 45](#)
- [Junos System Log Regular Expression Operators for the match Statement on page 47](#)
- [Disabling the System Logging of a Facility on page 48](#)

## Junos OS System Log Configuration Hierarchy

---

To configure the router to log system messages, include the **syslog** statement at the **[edit system]** hierarchy level:

```
[edit system]
syslog {
  archive <files number> <size size> <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
      brief;
    }
  }
  source-address source-address;
  time-format (year | millisecond | year millisecond);
  user (username | *) {
    facility severity;
    match "regular-expression";
  }
}
```

**Related Documentation**

- [Junos OS System Log Configuration Overview on page 3](#)

## Junos OS Minimum System Logging Configuration

---

To record or view system log messages, you must include the **syslog** statement at the **[edit system]** hierarchy level. Specify at least one destination for the messages, as described in [Table 17 on page 29](#). For more information about the configuration statements, see “[Single-Chassis System Logging Configuration Overview](#)” on [page 5](#).

Table 17: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration Statements
File	<pre>[edit system syslog] file <i>filename</i> {   <i>facility severity</i>; }</pre>
Terminal session of one, several, or all users	<pre>[edit system syslog] user (<i>username</i>   *) {   <i>facility severity</i>; }</pre>
Router or switch console	<pre>[edit system syslog] console {   <i>facility severity</i>; }</pre>
Remote machine or the other Routing Engine on the router or switch	<pre>[edit system syslog] host (<i>hostname</i>   other-routing-engine) {   <i>facility severity</i>; }</pre>

#### Related Documentation

- [Junos OS System Log Configuration Overview on page 3](#)
- Overview of Junos OS System Log Messages
- Overview of Single-Chassis System Logging Configuration

## Junos OS Default System Log Settings

Table 18 on page 29 summarizes the default system log settings that apply to all routers that run the Junos OS, and specifies which statement to include in the configuration to override the default value.

Table 18: Default System Logging Settings

Setting	Default	Overriding Statement	Instructions
Alternative facility for message forwarded to a remote machine	For <b>change-log</b> : local6 For <b>conflict-log</b> : local5 For <b>dfc</b> : local1 For <b>firewall</b> : local3 For <b>interactive-commands</b> : local7 For <b>pfe</b> : local4	<pre>[edit system syslog] host <i>hostname</i> {   facility-override <i>facility</i>; }</pre>	<a href="#">“Changing the Alternative Facility Name for Remote System Log Messages” on page 36</a>
Format of messages logged to a file	Standard Junos format, based on UNIX format	<pre>[edit system syslog] file <i>filename</i> {   structured-data; }</pre>	<a href="#">“Logging Messages in Structured-Data Format” on page 32</a>

Table 18: Default System Logging Settings (*continued*)

Setting	Default	Overriding Statement	Instructions
Maximum number of files in the archived set	10	<pre>[edit system syslog] archive {   files <i>number</i>; } file <i>filename</i> {   archive {     files <i>number</i>;   } }</pre>	<a href="#">“Specifying Log File Size, Number, and Archiving Properties” on page 40</a>
Maximum size of the log file	J Series: 128 kilobytes (KB) M Series, MX Series, and T Series: 1 megabyte (MB)  TX Matrix: 10 MB	<pre>[edit system syslog] archive {   size <i>size</i>; } file <i>filename</i> {   archive {     size <i>size</i>;   } }</pre>	<a href="#">“Specifying Log File Size, Number, and Archiving Properties” on page 40</a>
Timestamp format	Month, date, hour, minute, second  For example: <b>Aug 21 12:36:30</b>	<pre>[edit system syslog] time-format <i>format</i>;</pre>	<a href="#">“Including the Year or Millisecond in Timestamps” on page 45</a>
Users who can read log files	<b>root</b> user and users with the Junos <b>maintenance</b> permission	<pre>[edit system syslog] archive {   world-readable; } file <i>filename</i> {   archive {     world-readable;   } }</pre>	<a href="#">“Specifying Log File Size, Number, and Archiving Properties” on page 40</a>

- [Junos OS System Log Configuration Overview on page 3](#)
- [Junos OS Platform-Specific Default System Log Messages on page 4](#)

## Junos OS Platform-Specific Default System Log Messages

The following messages are generated by default on specific routers. To view any of these types of messages, you must configure at least one destination for messages as described in [“Junos OS Minimum System Logging Configuration” on page 28](#).

- On J Series routers, a message is logged when a process running in the kernel consumes 500 or more consecutive milliseconds of CPU time.

To log the kernel process message on an M Series, MX Series, or T Series router, include the **kernel info** statement at the appropriate hierarchy level:

```
[edit system syslog]
(console | file filename | host destination | user username) {
```

```
kernel info;  
}
```

- On a routing matrix composed of a TX Matrix router and T640 routers, the master Routing Engine on each T640 router forwards all messages with a severity of **info** and higher to the master Routing Engine on the TX Matrix router. This is equivalent to the following configuration statement included on the TX Matrix router:

```
[edit system syslog]  
host scc-master {  
  any info;  
}
```

- Likewise, on a routing matrix composed of a TX Matrix Plus router and T1600 routers, the master Routing Engine on each T1600 router forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix Plus router:

```
[edit system syslog]  
host sfc0-master {  
  any info;  
}
```

**Related  
Documentation**

- [Junos OS System Log Configuration Overview on page 3](#)
- [Junos OS Default System Log Settings on page 29](#)

---

## Specifying the Facility and Severity of Messages to Include in the Log

Each system log message belongs to a *facility*, which is a group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions.

When you configure logging for a facility and destination, you specify a severity level for each facility. Messages from the facility that are rated at that level or higher are logged to the destination:

```
[edit system syslog]  
(console | file filename | host destination | user username) {  
  facility severity;  
}
```

**Related  
Documentation**

- [Junos OS System Logging Facilities and Message Severity Levels](#)
- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Examples: Configuring System Logging on page 67](#)
- [Overview of Single-Chassis System Logging Configuration](#)

## Directing System Log Messages to a Log File

---

To direct system log messages to a file in the `/var/log` directory of the local Routing Engine, include the `file` statement at the `[edit system syslog]` hierarchy level:

```
[edit system syslog]
file filename {
  facility severity;
  archive <archive-sites (ftp-url <password password>)> <files number> <size size>
    <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
    no-world-readable>;
  explicit-priority;
  match "regular-expression";
  structured-data {
    brief;
  }
}
```

For the list of facilities and severity levels, see [“Specifying the Facility and Severity of Messages to Include in the Log” on page 31](#).

To prevent log files from growing too large, the Junos OS system logging utility by default writes messages to a sequence of files of a defined size. By including the `archive` statement, you can configure the number of files, their maximum size, and who can read them, either for all log files or for a certain log file. For more information, see [“Specifying Log File Size, Number, and Archiving Properties” on page 40](#).

For information about the following statements, see the indicated sections:

- `explicit-priority`—See [“Including Priority Information in System Log Messages” on page 41](#)
- `match`—See [“Using Regular Expressions to Refine the Set of Logged Messages” on page 45](#)
- `structured-data`—See [“Logging Messages in Structured-Data Format” on page 32](#)

### Related Documentation

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Overview of Junos OS System Log Messages](#)
- [Logging Messages in Structured-Data Format](#)
- [Examples: Configuring System Logging on page 67](#)
- [Examples: Configuring System Logging](#)

## Logging Messages in Structured-Data Format

---

You can log messages to a file in structured-data format instead of the standard Junos format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from a message.

The structured-data format complies with Internet draft draft-ietf-syslog-protocol-23, *The syslog Protocol*, which is at <http://tools.ietf.org/html/draft-ietf-syslog-protocol-23>. The draft establishes a standard message format regardless of the source or transport protocol for logged messages.

To output messages to a file in structured-data format, include the **structured-data** statement at the **[edit system syslog file filename]** hierarchy level:

```
[edit system syslog file filename]
facility severity;
structured-data {
  brief;
}
```

The optional **brief** statement suppresses the English-language text that appears by default at the end of a message to describe the error or event. For information about the fields in a structured-data format message, see the [Junos OS System Log Messages Reference](#).

The structured format is used for all messages logged to the file that are generated by a Junos process or software library.



**NOTE:** If you include either or both of the **explicit-priority** and **time-format** statements along with the **structured-data** statement, they are ignored. These statements apply to the standard Junos system log format, not to structured-data format.

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Examples: Configuring System Logging on page 67](#)

## Directing System Log Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged in to the local Routing Engine, include the **user** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
user (username | *) {
  facility severity;
  match "regular-expression";
}
```

Specify one or more Junos OS usernames, separating multiple values with spaces, or use the asterisk (\*) to indicate all users who are logged in to the local Routing Engine.

For the list of logging facilities and severity levels, see “[Specifying the Facility and Severity of Messages to Include in the Log](#)” on page 31. For information about the **match** statement, see “[Using Regular Expressions to Refine the Set of Logged Messages](#)” on page 45.

- Related Documentation**
- [Single-Chassis System Logging Configuration Overview on page 5](#)
  - [Overview of Single-Chassis System Logging Configuration](#)
  - [Examples: Configuring System Logging on page 67](#)
  - [Examples: Configuring System Logging](#)

---

## Directing System Log Messages to the Console

To direct system log messages to the console of the local Routing Engine, include the **console** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
console {
    facility severity;
}
```

For the list of logging facilities and severity levels, see “[Specifying the Facility and Severity of Messages to Include in the Log](#)” on page 31.

- Related Documentation**
- [Single-Chassis System Logging Configuration Overview on page 5](#)
  - [Overview of Single-Chassis System Logging Configuration](#)
  - [Examples: Configuring System Logging on page 67](#)
  - [Examples: Configuring System Logging](#)

---

## Directing System Log Messages to a Remote Machine or the Other Routing Engine

To direct system log messages to a remote machine or to the other Routing Engine on the router, include the **host** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
        brief;
    }
}
source-address source-address;
```

To direct system log messages to a remote machine, include the **host hostname** statement to specify the remote machine's IP version 4 (IPv4) address, IP version 6 (IPv6) address, or fully qualified hostname. The remote machine must be running the standard **syslogd** utility. We do not recommend directing messages to another Juniper Networks router. In each system log message directed to the remote machine, the hostname of the local



Routing Engine appears after the timestamp to indicate that it is the source for the message.

To direct system log messages to the other Routing Engine on a router with two Routing Engines installed and operational, include the **host other-routing-engine** statement. The statement is not automatically reciprocal, so you must include it in each Routing Engine configuration if you want the Routing Engines to direct messages to each other. In each message directed to the other Routing Engine, the string **re0** or **re1** appears after the timestamp to indicate the source for the message.

For the list of logging facilities and severity levels to configure under the **host** statement, see [“Specifying the Facility and Severity of Messages to Include in the Log” on page 31](#).

To record facility and severity level information in each message, include the **explicit-priority** statement. For more information, see [“Including Priority Information in System Log Messages” on page 41](#).

For information about the **match** statement, see [“Using Regular Expressions to Refine the Set of Logged Messages” on page 45](#).

When directing messages to remote machines, you can include the **source-address** statement to specify the IP address of the router that is reported in the messages as their source. In each **host** statement, include the **facility-override** statement to assign an alternative facility and the **log-prefix** statement to add a string to each message. You can include the **structured-data** statement to enable the forwarding of structured system log messages to a remote system log server in the IETF system log message format.

**Related  
Documentation**

- [Single-Chassis System Logging Configuration Overview on page 5](#)

---

## Specifying an Alternative Source Address for System Log Messages

---

To specify the source router to be reported in system log messages when the messages are directed to a remote machine, include the **source-address** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
source-address source-address;
```

**source-address** is a valid IPv4 or IPv6 address configured on one of the router interfaces. The address is reported in the messages directed to all remote machines specified in **host hostname** statements at the **[edit system syslog]** hierarchy level, but not in messages directed to the other Routing Engine.

**Related  
Documentation**

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Examples: Assigning an Alternative Facility on page 69](#)

## Changing the Alternative Facility Name for Remote System Log Messages

---

Some facilities assigned to messages logged on the local router or switch have Junos OS-specific names (see Junos OS System Logging Facilities and Message Severity Levels). In the recommended configuration, a remote machine designated at the **[edit system syslog host *hostname*]** hierarchy level is not a Juniper Networks router or switch, so its **syslogd** utility cannot interpret the Junos OS-specific names. To enable the standard **syslogd** utility to handle messages from these facilities when messages are directed to a remote machine, a standard **localX** facility name is used instead of the Junos OS-specific facility name.

[Table 19 on page 38](#) lists the default alternative facility name next to the Junos OS-specific facility name it is used for.

The **syslogd** utility on a remote machine handles all messages that belong to a facility in the same way, regardless of the source of the message (the Juniper Networks router or switch or the remote machine itself). For example, the following statements in the configuration of the router called **local-router** direct messages from the **authorization** facility to the remote machine **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
  authorization info;
}
```

The default alternative facility for the local **authorization** facility is also **authorization**. If the **syslogd** utility on **monitor** is configured to write messages belonging to the **authorization** facility to the file **/var/log/auth-attempts**, then the file contains the messages generated when users log in to **local-router** and the messages generated when users log in to **monitor**. Although the name of the source machine appears in each system log message, the mixing of messages from multiple machines can make it more difficult to analyze the contents of the **auth-attempts** file.

To make it easier to separate the messages from each source, you can assign an alternative facility to all messages generated on **local-router** when they are directed to **monitor**. You can then configure the **syslogd** utility on **monitor** to write messages with the alternative facility to a different file from messages generated on **monitor** itself.

To change the facility used for all messages directed to a remote machine, include the **facility-override** statement at the **[edit system syslog host *hostname*]** hierarchy level:

```
[edit system syslog host hostname]
facility severity;
facility-override facility;
```

In general, it makes sense to specify an alternative facility that is not already in use on the remote machine, such as one of the **localX** facilities. On the remote machine, you must also configure the **syslogd** utility to handle the messages in the desired manner.

[Table 20 on page 38](#) lists the facilities that you can specify in the **facility-override** statement.

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

The following example shows how to log all messages generated on the local router at the **error** level or higher to the **local0** facility on the remote machine called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
    any error;
    facility-override local0;
}
```

The following example shows how to configure routers located in California and routers located in New York to send messages to a single remote machine called **central-logger.mycompany.com**. The messages from California are assigned to alternative facility **local0** and the messages from New York are assigned to alternative facility **local2**.

- Configure California routers to aggregate messages in the **local0** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
    change-log info;
    facility-override local0;
}
```

- Configure New York routers to aggregate messages in the **local2** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
    change-log info;
    facility-override local2;
}
```

On **central-logger**, you can then configure the system logging utility to write messages from the **local0** facility to the file **california-config** and the messages from the **local2** facility to the file **new-york-config**.

#### Related Documentation

- [Table 19 on page 38](#)
- [Junos OS System Log Alternate Facilities for Remote Logging on page 38](#)
- [Examples: Assigning an Alternative Facility on page 69](#)
- [Examples: Assigning an Alternative Facility](#)

## System Log Default Facilities for Messages Directed to a Remote Destination

[Table 19 on page 38](#) lists the default alternative facility name next to the Junos OS-specific facility name for which it is used. For facilities that are not listed, the default alternative name is the same as the local facility name.

Table 19: Default Facilities for Messages Directed to a Remote Destination

Junos OS—specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6
conflict-log	local5
dfc	local1
firewall	local3
interactive-commands	local7
pfe	local4

**Related Documentation**

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- Overview of Single-Chassis System Logging Configuration

## Junos OS System Log Alternate Facilities for Remote Logging

Table 20 on page 38 lists the facilities that you can specify in the **facility-override** statement.

Table 20: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts
daemon	Actions performed or errors encountered by system processes
ftp	Actions performed or errors encountered by the FTP process
kernel	Actions performed or errors encountered by the Junos OS kernel
local0	Local facility number 0
local1	Local facility number 1
local2	Local facility number 2
local3	Local facility number 3
local4	Local facility number 4
local5	Local facility number 5

Table 20: Facilities for the facility-override Statement (*continued*)

Facility	Description
<b>local6</b>	Local facility number 6
<b>local7</b>	Local facility number 7
<b>user</b>	Actions performed or errors encountered by user-space processes

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

#### Related Documentation

- [Examples: Assigning an Alternative Facility on page 69](#)
- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Overview of Single-Chassis System Logging Configuration](#)

## Adding a Text String to System Log Messages

To add a text string to every system log message directed to a remote machine or to the other Routing Engine, include the **log-prefix** statement at the **[edit system syslog host]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
  facility severity;
  log-prefix string;
```

The string can contain any alphanumeric or special character except the equal sign ( = ) and the colon ( : ). It also cannot include the space character; do not enclose the string in quotation marks ( " ") in an attempt to include spaces in it.

The Junos OS system logging utility automatically appends a colon and a space to the specified string when the system log messages are written to the log. The string is inserted after the identifier for the Routing Engine that generated the message.

The following example shows how to add the string **M120** to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine **hardware-logger.mycompany.com**:

```
[edit system syslog]
  host hardware-logger.mycompany.com {
    any info;
    log-prefix M120;
  }
```

When these configuration statements are included on an M120 router called **origin1**, a message in the system log on **hardware-logger.mycompany.com** looks like the following:

Mar 9 17:33:23 origin1 M120:mgd[477]: UI\_CMDLINE\_READ\_LINE: user 'root', command 'run show version'

**Related  
Documentation**

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Specifying Log File Size, Number, and Archiving Properties on page 40](#)
- Overview of Single-Chassis System Logging Configuration

---

## Specifying Log File Size, Number, and Archiving Properties

---

To prevent log files from growing too large, by default the Junos system logging utility writes messages to a sequence of files of a defined size. The files in the sequence are referred to as *archive* files to distinguish them from the *active* file to which messages are currently being written. The default maximum size depends on the platform type:

- 128 kilobytes (KB) for J Series Services routers
- 1 megabyte (MB) for M Series, MX Series, and T Series routers
- 10 MB for TX Matrix or TX Matrix Plus routers
- 1 MB for the QFX Series

When an active log file called **logfile** reaches the maximum size, the logging utility closes the file, compresses it, and names the compressed archive file **logfile.0.gz**. The logging utility then opens and writes to a new active file called **logfile**. This process is also known as file rotation. When the new **logfile** reaches the configured maximum size, **logfile.0.gz** is renamed **logfile.1.gz**, and the new **logfile** is closed, compressed, and renamed **logfile.0.gz**. By default, the logging utility creates up to 10 archive files in this manner. When the maximum number of archive files is reached and when the size of the active file reaches the configured maximum size, the contents of the last archived file are overwritten by the current active file. The logging utility by default also limits the users who can read log files to the **root** user and users who have the Junos OS **maintenance** permission.

Junos OS provides a configuration statement **log-rotate-frequency** that configures the system log file rotation frequency by configuring the time interval for checking the log file size. The frequency can be set to a value of 1 minute through 59 minutes. The default frequency is 15 minutes.

To configure the log rotation frequency, include the **log-rotate-frequency** statement at the **[edit system syslog]** hierarchy level.

You can include the **archive** statement to change the maximum size of each file, how many archive files are created, and who can read log files.

To configure values that apply to all log files, include the **archive** statement at the **[edit system syslog]** hierarchy level:

**archive** <files *number*> <size *size*> <world-readable | no-world-readable>;

To configure values that apply to a specific log file, include the **archive** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
archive <archive-sites (ftp-url <password password>)> <files number> <size size>  
<start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |  
no-world-readable> ;
```

**archive-sites** *site-name* specifies a list of archive sites that you want to use for storing files. The *site-name* value is any valid FTP URL to a destination. If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the specified log filename. For information about how to specify valid FTP URLs, see [Format for Specifying Filenames and URLs in Junos OS CLI Commands](#).

**files** *number* specifies the number of files to create before the oldest file is overwritten. The value can be from 1 through 1000.

**size** *size* specifies the maximum size of each file. The value can be from 64 KB (**64k**) through 1 gigabyte (**1g**); to represent megabytes, use the letter **m** after the integer. There is no space between the digits and the **k**, **m**, or **g** units letter.

**start-time** "YYYY-MM-DD.hh:mm" defines the date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

**transfer-interval** *interval* defines the amount of time the current log file remains open (even if it has not reached the maximum possible size) and receives new statistics before it is closed and transferred to an archive site. This interval value can be from 5 through 2880 minutes.

**world-readable** enables all users to read log files. To restore the default permissions, include the **no-world-readable** statement.

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Examples: Configuring System Logging on page 67](#)
- [Overview of Single-Chassis System Logging Configuration](#)

---

## Including Priority Information in System Log Messages

The facility and severity level of a message are together referred to as its *priority*. By default, messages logged in the standard Junos OS format do not include information about priority. To include priority information in standard-format messages directed to a file, include the **explicit-priority** statement at the **[edit system syslog file filename]** hierarchy level:

```
[edit system syslog file filename]  
facility severity;  
explicit-priority;
```



**NOTE:** Messages logged in structured-data format include priority information by default. If you include the `structured-data` statement at the `[edit system syslog file filename]` hierarchy level along with the `explicit-priority` statement, the `explicit-priority` statement is ignored and messages are logged in structured-data format.

For information about the `structured-data` statement, see [“Logging Messages in Structured-Data Format” on page 32](#). For information about the contents of a structured-data message, see the [Junos OS System Log Messages Reference](#).

To include priority information in messages directed to a remote machine or the other Routing Engine, include the `explicit-priority` statement at the `[edit system syslog host (hostname | other-routing-engine)]` hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
explicit-priority;
```



**NOTE:** The `other-routing-engine` option does not apply to the QFX Series.

The priority recorded in a message always indicates the original, local facility name. If the `facility-override` statement is included for messages directed to a remote destination, the Junos OS system logging utility still uses the alternative facility name for the messages themselves when directing them to the remote destination. For more information, see [“Changing the Alternative Facility Name for Remote System Log Messages” on page 36](#).

When the `explicit-priority` statement is included, the Junos OS logging utility prepends codes for the facility name and severity level to the message tag name, if the message has one:

*FACILITY-severity*[-TAG]

(The tag is a unique identifier assigned to some Junos OS system log messages; for more information, see the [Junos OS System Log Messages Reference](#).)

In the following example, the `CHASSISD_PARSE_COMPLETE` message belongs to the `daemon` facility and is assigned severity `info` (6):

```
Aug 21 12:36:30 router1 chassisd[522]: %DAEMON-6-CHASSISD_PARSE_COMPLETE:
Using new configuration
```

When the `explicit-priority` statement is not included, the priority does not appear in the message:

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using new
configuration
```

For more information about message formatting, see the [Junos OS System Log Messages Reference](#).



- Related Documentation**
- [Single-Chassis System Logging Configuration Overview on page 5](#)
  - [Overview of Single-Chassis System Logging Configuration](#)
  - [Examples: Configuring System Logging on page 67](#)

## System Log Facility Codes and Numerical Codes Reported in Priority Information

Table 21 on page 43 lists the facility codes that can appear in system log messages and maps them to facility names.



**NOTE:** If the second column in Table 21 on page 43 does not include the Junos facility name for a code, the facility cannot be included in a statement at the [edit system syslog] hierarchy level. The Junos OS might use the facilities in Table 21 on page 43—and others that are not listed—when reporting on internal operations.

**Table 21: Facility Codes Reported in Priority Information**

Code	Junos Facility Name	Type of Event or Error
AUTH	authorization	Authentication and authorization attempts
AUTHPRIV		Authentication and authorization attempts that can be viewed by superusers only
CHANGE	change-log	Changes to the Junos configuration
CONFLICT	conflict-log	Specified configuration is invalid on the router type
CONSOLE		Messages written to <b>/dev/console</b> by the kernel console output r
CRON		Actions performed or errors encountered by the cron process
DAEMON	daemon	Actions performed or errors encountered by system processes
DFC	dfc	Actions performed or errors encountered by the dynamic flow capture process
FIREWALL	firewall	Packet filtering actions performed by a firewall filter
FTP	ftp	Actions performed or errors encountered by the FTP process
INTERACT	interactive-commands	Commands issued at the Junos OS CLI prompt or invoked by a client application such as a Junos XML protocol or NETCONF client
KERN	kernel	Actions performed or errors encountered by the Junos kernel

Table 21: Facility Codes Reported in Priority Information (*continued*)

Code	Junos Facility Name	Type of Event or Error
<b>NTP</b>		Actions performed or errors encountered by the Network Time Protocol (NTP)
<b>PFE</b>	<b>pfe</b>	Actions performed or errors encountered by the Packet Forwarding Engine
<b>SYSLOG</b>		Actions performed or errors encountered by the Junos system logging utility
<b>USER</b>	<b>user</b>	Actions performed or errors encountered by user-space processes

Table 22 on page 44 lists the numerical severity codes that can appear in system log messages and maps them to severity levels.

Table 22: Numerical Codes for Severity Levels Reported in Priority Information

Numerical Code	Severity Level	Description
<b>0</b>	<b>emergency</b>	System panic or other condition that causes the router to stop functioning
<b>1</b>	<b>alert</b>	Conditions that require immediate correction, such as a corrupted system database
<b>2</b>	<b>critical</b>	Critical conditions, such as hard errors
<b>3</b>	<b>error</b>	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
<b>4</b>	<b>warning</b>	Conditions that warrant monitoring
<b>5</b>	<b>notice</b>	Conditions that are not errors but might warrant special handling
<b>6</b>	<b>info</b>	Events or nonerror conditions of interest
<b>7</b>	<b>debug</b>	Software debugging messages (these appear only if a technical support representative has instructed you to configure this severity level)

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Examples: Configuring System Logging on page 67](#)

## Including the Year or Millisecond in Timestamps

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

```
Aug 21 12:36:30
```

To include the year, the millisecond, or both in the timestamp, include the **time-format** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
time-format (year | millisecond | year millisecond);
```

However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the **[edit system syslog time-format]** statement.

The modified timestamp is used in messages directed to each destination configured by a **file**, **console**, or **user** statement at the **[edit system syslog]** hierarchy level, but not to destinations configured by a **host** statement.

The following example illustrates the format for a timestamp that includes both the millisecond (**401**) and the year (**2006**):

```
Aug 21 12:36:30.401 2006
```



**NOTE:** Messages logged in structured-data format include the year and millisecond by default. If you include the structured-data statement at the **[edit system syslog file filename]** hierarchy level along with the **time-format** statement, the **time-format** statement is ignored and messages are logged in structured-data format.

For information about the structured-data statement, see “[Logging Messages in Structured-Data Format](#)” on page 32. For information about the contents of a structured-data message, see the *Junos OS System Log Messages Reference*.

### Related Documentation

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- [Examples: Configuring System Logging on page 67](#)

## Using Regular Expressions to Refine the Set of Logged Messages

The predefined facilities group together related messages, but you can also use regular expression matching to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination.

To specify the text string that must (or must not) appear in a message for the message to be logged to a destination, include the **match** statement and specify the regular expression which the text string must match:

```
match "regular-expression";
```

You can include this statement at the following hierarchy levels:

- **[edit system syslog file *filename*]** (for a file)
- **[edit system syslog user (*username* | \*)]** (for a specific user session or for all user sessions on a terminal)
- **[edit system syslog host (*hostname* | other-routing-engine)]** (for a remote destination)

In specifying the regular expression, use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions. Explaining regular expression syntax is beyond the scope of this document, but POSIX standards are available from the Institute of Electrical and Electronics Engineers (IEEE, <http://www.ieee.org>).

Table 23 on page 46 specifies which character or characters are matched by some of the regular expression operators that you can use in the match statement. In the descriptions, the term *term* refers to either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.



**NOTE:** The match statement is not case-sensitive.

**Table 23: Regular Expression Operators for the match Statement**

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
(pipe)	One of the terms that appears on either side of the pipe operator.
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS-specific.
^ (caret)	Start of a line, when the caret appears outside square brackets.  One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
\$ (dollar sign)	End of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen ( - ) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number.

Table 23: Regular Expression Operators for the match Statement (*continued*)

Operator	Matches
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

**Using Regular Expressions** Filter messages that belong to the **interactive-commands** facility, directing those that include the string **configure** to the terminal of the root user:

```
[edit system syslog]
user root {
  interactive-commands any;
  match ".*configure.*";
}
```

Messages like the following appear on the **root** user's terminal when a user issues a **configure** command to enter configuration mode:

```
timestamp router-name mgd[PID]: UI_CMDLINE_READ_LINE: User 'user', command
'configure private'
```

Filter messages that belong to the **daemon** facility and have a severity of **error** or higher, directing them to the file **/var/log/process-errors**. Omit messages generated by the SNMP process (**snmpd**), instead directing them to the file **/var/log/snmpd-errors**:

```
[edit system syslog]
file process-errors {
  daemon error;
  match "!(.*snmpd.*)";
}
file snmpd-errors {
  daemon error;
  match ".*snmpd.*";
}
```

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- Overview of Single-Chassis System Logging Configuration
- [Examples: Configuring System Logging on page 67](#)
- Examples: Configuring System Logging

## Junos System Log Regular Expression Operators for the match Statement

Table 24: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.

Table 24: Regular Expression Operators for the match Statement (*continued*)

Operator	Matches
<b>+</b> (plus sign)	One or more instances of the immediately preceding term.
<b>?</b> (question mark)	Zero or one instance of the immediately preceding term.
<b> </b> (pipe)	One of the terms that appear on either side of the pipe operator.
<b>!</b> (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS–specific.
<b>^</b> (caret)	The start of a line, when the caret appears outside square brackets.  One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
<b>\$</b> (dollar sign)	The end of a line.
<b>[ ]</b> (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen ( - ) to separate the beginning and ending characters of the range. For example, <b>[a-z0-9]</b> matches any letter or number.
<b>( )</b> (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

- Related Documentation**
- [Single-Chassis System Logging Configuration Overview on page 5](#)
  - [Examples: Configuring System Logging on page 67](#)

## Disabling the System Logging of a Facility

To disable the logging of messages that belong to a particular facility, include the **facility none** statement in the configuration. This statement is useful when, for example, you want to log messages that have the same severity level and belong to all but a few facilities. Instead of including a statement for each facility you want to log, you can include the **any severity** statement and then a **facility none** statement for each facility that you do not want to log. For example, the following logs all messages at the **error** level or higher to the console, except for messages from the **daemon** and **kernel** facilities. Messages from those facilities are logged to the file **>/var/log/internals** instead:

```
[edit system syslog]
console {
  any error;
  daemon none;
  kernel none;
}
file internals {
```

```
    daemon info;  
    kernel info;  
}
```

**Related  
Documentation**

- [Single-Chassis System Logging Configuration Overview on page 5](#)
- Overview of Single-Chassis System Logging Configuration





## CHAPTER 3

# Configuring System Log Messages for a TX Matrix Router

- [Configuring System Logging for a TX Matrix Router on page 51](#)
- [Configuring Message Forwarding to the TX Matrix Router on page 53](#)
- [Configuring Optional Features for Forwarded Messages on a TX Matrix Router on page 54](#)
- [Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router on page 55](#)
- [Configuring System Logging Differently on Each T640 Router in a Routing Matrix on page 56](#)

## Configuring System Logging for a TX Matrix Router

---

To configure system logging for all routers in a routing matrix composed of a TX Matrix router and T640 routers, include the **syslog** statement at the **[edit system]** hierarchy level on the TX Matrix router. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
syslog {
  archive <files number> <size size> <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
}
host (hostname | other-routing-engine | scc-master) {
  facility severity;
  explicit-priority;
  facility-override facility;
```

```
log-prefix string;  
match "regular-expression";  
source-address source-address;  
port port number;  
}  
source-address source-address;  
time-format (year | millisecond | year millisecond);  
(username | *) {  
    facility severity;  
    match "regular-expression";  
}  
}
```

When included in the configuration on the TX Matrix router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router in the routing matrix:

- **archive**—Sets the size and number of log files on each platform in the routing matrix. See [“Specifying Log File Size, Number, and Archiving Properties” on page 40](#).
- **console**—Directs the specified messages to the console of each platform in the routing matrix. See [“Directing System Log Messages to the Console” on page 34](#).
- **file**—Directs the specified messages to a file of the same name on each platform in the routing matrix. See [“Directing System Log Messages to a Log File” on page 32](#).
- **match**—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See [“Using Regular Expressions to Refine the Set of Logged Messages” on page 45](#).

The separate **match** statement at the **[edit system syslog host scc-master]** hierarchy level applies to messages forwarded from the T640 routers to the TX Matrix router. See [“Configuring Optional Features for Forwarded Messages on a TX Matrix Router” on page 54](#).

- **port**—Specifies the port number of the remote syslog server.
- **source-address**—Sets the IP address of the router to report in system log messages as the message source, when the messages are directed to the remote machines specified in all **host hostname** statements at the **[edit system syslog]** hierarchy level, for each platform in the routing matrix. On a routing matrix composed of a TX Matrix router and T640 routers, the address is not reported by the T640 routers in messages directed to the other Routing Engine on each router or to the TX Matrix router. See [“Specifying an Alternative Source Address for System Log Messages” on page 35](#).
- **structured-data**—Writes messages to a file in structured-data format. See [“Logging Messages in Structured-Data Format” on page 32](#).
- **time-format**—Adds the millisecond, year, or both to the timestamp in each standard-format message. See [“Including the Year or Millisecond in Timestamps” on page 45](#).
- **user**—Directs the specified messages to the terminal session of one or more specified users on each platform in the routing matrix that they are logged in to. See [“Directing System Log Messages to a User Terminal” on page 33](#).

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

**Related Documentation**

- [Configuring Message Forwarding to the TX Matrix Router on page 53](#)
- [Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router on page 7](#)
- [Configuring Optional Features for Forwarded Messages on a TX Matrix Router on page 54](#)
- [Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router on page 55](#)
- [Configuring System Logging Differently on Each T640 Router in a Routing Matrix on page 56](#)

## Configuring Message Forwarding to the TX Matrix Router

By default, the master Routing Engine on each T640 router forwards to the master Routing Engine on the TX Matrix router all messages from all facilities with severity level of **info** and higher. To change the facility, the severity level, or both, include the **host scc-master** statement at the **[edit system syslog]** hierarchy level on the TX Matrix router:

```
[edit system syslog]
host scc-master {
    facility severity;
}
```

To disable message forwarding, set the facility to **any** and the severity level to **none**:

```
[edit system syslog]
host scc-master {
    any none;
}
```

In either case, the setting applies to all T640 routers in the routing matrix.

To capture the messages forwarded by the T640 routers (as well as messages generated on the TX Matrix router itself), you must also configure system logging on the TX Matrix router. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the TX Matrix router:

- To a file, as described in [“Directing System Log Messages to a Log File” on page 32](#).
- To the terminal session of one or more specific users (or all users), as described in [“Directing System Log Messages to a User Terminal” on page 33](#).
- To the console, as described in [“Directing System Log Messages to the Console” on page 34](#).
- To a remote machine that is running the **syslogd** utility or to the other Routing Engine. For more information, see [“Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router” on page 55](#).

As previously noted, the configuration statements included on the TX Matrix router also configure the same destinations on each T640 router in the routing matrix.

When specifying the severity level for local messages (at the **[edit system syslog (file | host | console | user)]** hierarchy level) and forwarded messages (at the **[edit system syslog host scc-master]** hierarchy level), you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the **any** facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

**Related Documentation**

- [Configuring System Logging for a TX Matrix Router on page 51](#)

## Configuring Optional Features for Forwarded Messages on a TX Matrix Router

---

To configure additional optional features when specifying how the T640 routers forward messages to the TX Matrix router, include statements at the **[edit system syslog host scc-master]** hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the **explicit-priority** statement. To insert a text string in each forwarded message, include the **log-prefix** statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the **match** statement.

```
[edit system syslog]
host scc-master {
    facility severity;
    explicit-priority;
    log-prefix string;
    match "regular-expression";
}
```

You can also include the **facility-override** statement at the **[edit system syslog host scc-master]** hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the TX Matrix router, because it runs the Junos system logging utility and can interpret the Junos OS-specific facilities. For more information about alternative facilities, see “[Changing the Alternative Facility Name for Remote System Log Messages](#)” on page 36.

- [Including Priority Information in Forwarded Messages on page 54](#)
- [Adding a Text String to Forwarded Messages on page 55](#)
- [Using Regular Expressions to Refine the Set of Forwarded Messages on page 55](#)

### Including Priority Information in Forwarded Messages

When you include the **explicit-priority** statement at the **[edit system syslog host scc-master]** hierarchy level, messages forwarded to the TX Matrix router include priority information. For the information to appear in a log file on the TX Matrix router, you must also include the **explicit-priority** statement at the **[edit system syslog file filename]** hierarchy level for the file on the TX Matrix router. As a consequence, the log file with the

same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all routers in the routing matrix, also include the **explicit-priority** statement at the **[edit system syslog host *hostname*]** hierarchy level for the remote machine. For more information, see [“Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router” on page 55](#).

In the following example, the **/var/log/messages** file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix router also includes messages with those characteristics forwarded from the T640 routers.

```
[edit system syslog]
host scc-master {
  any notice;
  explicit-priority;
}
file messages {
  any notice;
  explicit-priority;
}
```

### Adding a Text String to Forwarded Messages

When you include the **log-prefix** statement at the **[edit system syslog host scc-master]** hierarchy level, the string that you define appears in every message forwarded to the TX Matrix router. For more information, see [“Adding a Text String to System Log Messages” on page 39](#).

### Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host scc-master]** hierarchy level, the regular expression that you specify controls which messages from the T640 routers are forwarded to the TX Matrix router. The regular expression is not applied to messages from the T640 router that are directed to destinations other than the TX Matrix router. For more information about regular expression matching, see [“Using Regular Expressions to Refine the Set of Logged Messages” on page 45](#).

## Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router

---

You can configure a routing matrix composed of a TX Matrix router and T640 routers to direct system logging messages to a remote machine or the other Routing Engine on each router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the TX Matrix router:

```
[edit system syslog]
host (hostname | other-routing-engine) {
  facility severity;
  explicit-priority;
  facility-override facility;
```

```
log-prefix string;  
match "regular-expression";  
}  
source-address source-address;
```

The TX Matrix router directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (**explicit-priority**, **facility-override**, **log-prefix**, **match**, and **source-address**) also have the same effect as on a single-chassis system. For more information, see [“Directing System Log Messages to a Remote Machine or the Other Routing Engine” on page 34](#).

For the TX Matrix router to include priority information when it directs messages that originated on a T640 router to the remote destination, you must also include the **explicit-priority** statement at the **[edit system syslog host scc-master]** hierarchy level.

The **other-routing-engine** statement does not interact with message forwarding from the T640 routers to the TX Matrix router. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (**re0**), the **re0** Routing Engine on each T640 router sends messages to the **re1** Routing Engine on its platform only. It does not also send messages directly to the **re1** Routing Engine on the TX Matrix router.

Because the configuration on the TX Matrix router applies to the T640 routers, any T640 router that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T640 routers are configured to forward messages to the TX Matrix router (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T640 router and the other from the TX Matrix router. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see [“Configuring Message Forwarding to the TX Matrix Router” on page 53](#).
- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers in the routing matrix report the same source address in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single router.
- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

**Related  
Documentation**

- [Configuring System Logging for a TX Matrix Router on page 51](#)

---

## Configuring System Logging Differently on Each T640 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix router and T640 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router in the routing matrix is experiencing problems with authentication, a Juniper

Networks support representative might instruct you to log messages from the **authorization** facility with severity **debug** on that router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix router:

- To configure settings that apply to the TX Matrix router but not the T640 routers, include them in the **re0** and **re1** configuration groups.
- To configure settings that apply to particular T640 routers, include them in the **lccn-re0** and **lccn-re1** configuration groups, where *n* is the line-card chassis (LCC) index number of the router.

When you use configuration groups, do not issue CLI configuration-mode commands to change statements at the **[edit system syslog]** hierarchy level on the TX Matrix router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T640 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T640 routers at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *Junos OS CLI User Guide*.

The following example shows how to configure the **/var/log/messages** files on three routers to include different sets of messages:

- On the TX Matrix router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T640 routers, because the **host scc-master** statement disables message forwarding.
- On the T640 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T640 router designated **LCC1**, messages with severity **notice** from all facilities.

```
[edit groups]
re0 {
  system {
    syslog {
      file messages {
        any info;
      }
      host scc-master {
        any none;
      }
    }
  }
}
re1 {
  ... same statements as for re0 ...
}
lcc0-re0 {
  system {
    syslog {
      file messages {
        authorization info;
      }
    }
  }
}
```

```
    }  
  }  
}  
lcc0-re1 {  
  ... same statements as for lcc0-re0 ...  
}  
lcc1-re0 {  
  system {  
    syslog {  
      file messages {  
        any notice;  
      }  
    }  
  }  
}  
lcc0-re1 {  
  ... same statements as for lcc1-re0 ...  
}
```

**Related Documentation**

- [Configuring System Logging for a TX Matrix Router on page 51](#)



## CHAPTER 4

# Configuring System Log Messages for a TX Matrix Plus Router

- [Configuring System Logging for a TX Matrix Plus Router on page 59](#)
- [Configuring Message Forwarding to the TX Matrix Plus Router on page 61](#)
- [Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router on page 62](#)
- [Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router on page 63](#)
- [Configuring System Logging Differently on Each T1600 Router in a Routing Matrix on page 65](#)

## Configuring System Logging for a TX Matrix Plus Router

---

To configure system logging for all routers in a routing matrix composed of a TX Matrix Plus router and T1600 routers, include the **syslog** statement at the **[edit system]** hierarchy level on the TX Matrix Plus router. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
syslog {
  archive <files number> <size size> <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
}
host (hostname | other-routing-engine | sfc0-master) {
  facility severity;
  explicit-priority;
```

```
    facility-override facility;  
    log-prefix string;  
    match "regular-expression";  
  }  
  source-address source-address;  
  time-format (year | millisecond | year millisecond);  
  (username | *) {  
    facility severity;  
    match "regular-expression";  
  }  
}
```

When included in the configuration on the TX Matrix Plus router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router in the routing matrix composed of the TX Matrix Plus router and T1600 routers:

- **archive**—Sets the size and number of log files on each router in the routing matrix. See [“Specifying Log File Size, Number, and Archiving Properties” on page 40](#).
- **console**—Directs the specified messages to the console of each router in the routing matrix. See [“Directing System Log Messages to the Console” on page 34](#).
- **file**—Directs the specified messages to a file of the same name on each router in the routing matrix. See [“Directing System Log Messages to a Log File” on page 32](#).
- **match**—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See [“Using Regular Expressions to Refine the Set of Logged Messages” on page 45](#).

The separate **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level applies to messages forwarded from the T1600 routers to the TX Matrix Plus router. See [“Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router” on page 62](#).

- **source-address**—Sets the IP address of the router as the message source in system log messages when the messages are directed to the remote machines specified in all **host hostname** statements at the **[edit system syslog]** hierarchy level, for each router in the routing matrix. On a routing matrix composed of a TX Matrix Plus router and T1600 routers, the address is not reported by the T1600 routers in messages directed to the other Routing Engine on each router or to the TX Matrix Plus router. See [“Specifying an Alternative Source Address for System Log Messages” on page 35](#).
- **structured-data**—Writes messages to a file in structured-data format. See [“Logging Messages in Structured-Data Format” on page 32](#).
- **time-format**—Adds the millisecond, year, or both to the timestamp in each standard-format message. See [“Including the Year or Millisecond in Timestamps” on page 45](#).
- **user**—Directs the specified messages to the terminal session of one or more specified users on each router in the routing matrix that they are logged in to. See [“Directing System Log Messages to a User Terminal” on page 33](#).

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

**Related Documentation**

- [Configuring Message Forwarding to the TX Matrix Plus Router on page 61](#)
- [Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router on page 9](#)
- [Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router on page 62](#)
- [Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router on page 63](#)
- [Configuring System Logging Differently on Each T1600 Router in a Routing Matrix on page 65](#)

---

## Configuring Message Forwarding to the TX Matrix Plus Router

By default, the master Routing Engine on each T1600 router forwards to the master Routing Engine on the TX Matrix Plus router all messages from all facilities with severity level of **info** and higher. To change the facility, the severity level, or both, include the **host sfc0-master** statement at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router:

```
[edit system syslog]
host sfc0-master {
    facility severity;
}
```

To disable message forwarding, set the facility to **any** and the severity level to **none**:

```
[edit system syslog]
host sfc0-master {
    any none;
}
```

In either case, the setting applies to all T1600 routers in the routing matrix.

To capture the messages forwarded by the T1600 routers (as well as messages generated on the TX Matrix Plus router itself), you must also configure system logging on the TX Matrix Plus router. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router:

- To a file, as described in [“Directing System Log Messages to a Log File” on page 32](#).
- To the terminal session of one or more specific users (or all users), as described in [“Directing System Log Messages to a User Terminal” on page 33](#).

- To the console, as described in [“Directing System Log Messages to the Console” on page 34](#).
- To a remote machine that is running the **syslogd** utility or to the other Routing Engine. For more information, see [“Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router” on page 63](#).

As previously noted, the configuration statements included on the TX Matrix Plus router also configure the same destinations on each T1600 router.

When specifying the severity level for local messages (at the **[edit system syslog (file | host | console | user)]** hierarchy level) and forwarded messages (at the **[edit system syslog host sfc0-master]** hierarchy level), you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the **any** facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

**Related  
Documentation**

- [Configuring System Logging for a TX Matrix Plus Router on page 59](#)

---

## Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router

To configure additional optional features when specifying how the T1600 routers forward messages to the TX Matrix Plus router, include statements at the **[edit system syslog host sfc0-master]** hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the **explicit-priority** statement. To insert a text string in each forwarded message, include the **log-prefix** statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the **match** statement.

```
[edit system syslog]
host sfc0-master {
  facility severity;
  explicit-priority;
  log-prefix string;
  match "regular-expression;
}
```

You can also include the **facility-override** statement at the **[edit system syslog host sfc0-master]** hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the TX Matrix Plus router, because it runs the Junos system logging utility and can interpret the Junos OS-specific facilities. For more information about alternative facilities, see [“Changing the Alternative Facility Name for Remote System Log Messages” on page 36](#).

1. [Including Priority Information in Forwarded Messages on page 63](#)
2. [Adding a Text String to Forwarded Messages on page 63](#)
3. [Using Regular Expressions to Refine the Set of Forwarded Messages on page 63](#)

## Including Priority Information in Forwarded Messages

When you include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level, messages forwarded to the TX Matrix Plus router include priority information. For the information to appear in a log file on the TX Matrix Plus router, you must also include the **explicit-priority** statement at the **[edit system syslog file filename]** hierarchy level for the file on the TX Matrix Plus router. As a consequence, the log file with the same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all routers in the routing matrix, also include the **explicit-priority** statement at the **[edit system syslog host hostname]** hierarchy level for the remote machine. For more information, see [“Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router” on page 63](#).

In the following example, the **/var/log/messages** file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix Plus router also includes messages with those characteristics forwarded from the T1600 routers.

```
[edit system syslog]
host sfc0-master {
  any notice;
  explicit-priority;
}
file messages {
  any notice;
  explicit-priority;
}
```

## Adding a Text String to Forwarded Messages

When you include the **log-prefix** statement at the **[edit system syslog host sfc0-master]** hierarchy level, the string that you define appears in every message forwarded to the TX Matrix Plus router. For more information, see [“Adding a Text String to System Log Messages” on page 39](#).

## Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level, the regular expression that you specify controls which messages from the T1600 routers are forwarded to the TX Matrix Plus router. The regular expression is not applied to messages from the T1600 routers that are directed to destinations other than the TX Matrix Plus router. For more information about regular expression matching, see [“Using Regular Expressions to Refine the Set of Logged Messages” on page 45](#).

## Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router

---

You can configure a routing matrix composed of a TX Matrix Plus router and T1600 routers to direct system logging messages to a remote machine or the other Routing

Engine on each routing router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router:

```
[edit system syslog]
host (hostname | other-routing-engine) {
  facility severity;
  explicit-priority;
  facility-override facility;
  log-prefix string;
  match "regular-expression";
}
source-address source-address;
```

The TX Matrix Plus router directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (**explicit-priority**, **facility-override**, **log-prefix**, **match**, and **source-address**) also have the same effect as on a single-chassis system. For more information, see [“Directing System Log Messages to a Remote Machine or the Other Routing Engine” on page 34](#).

For the TX Matrix Plus router to include priority information when it directs messages that originated on a T1600 router to the remote destination, you must also include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level.

The **other-routing-engine** statement does not interact with message forwarding from the T1600 routers to the TX Matrix Plus router. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (**re0**), the **re0** Routing Engine on each T1600 router sends messages to the **re1** Routing Engine on its router only. It does not also send messages directly to the **re1** Routing Engine on the TX Matrix Plus router.

Because the configuration on the TX Matrix Plus router applies to the T1600 routers, any T1600 router that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T1600 routers are configured to forward messages to the TX Matrix Plus router (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T1600 router and the other from the TX Matrix Plus router. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see [“Configuring Message Forwarding to the TX Matrix Plus Router” on page 61](#).
- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers in the routing matrix report the same source address in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single routing router.
- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

#### Related Documentation

- [Configuring System Logging for a TX Matrix Plus Router on page 59](#)

## Configuring System Logging Differently on Each T1600 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix Plus router and T1600 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix Plus router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router in the routing matrix is experiencing problems with authentication, a Juniper Networks support representative might instruct you to log messages from the **authorization** facility with severity **debug** on that router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix Plus router:

- To configure settings that apply to the TX Matrix Plus router but not the T1600 routers, include them in the **re0** and **re1** configuration groups.
- To configure settings that apply to particular T1600 routers, include them in the **lccn-re0** and **lccn-re1** configuration groups, where **n** is the line-card chassis (LCC) index number of the router.

When you use configuration groups, do not issue CLI configuration-mode commands to change statements at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T1600 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T1600 routers at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *Junos OS CLI User Guide*.

The following example shows how to configure the **/var/log/messages** files on three routers to include different sets of messages:

- On the TX Matrix Plus router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T1600 routers, because the **host sfc0-master** statement disables message forwarding.
- On the T1600 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T1600 router designated **LCC1**, messages with severity **notice** from all facilities.

```
[edit groups]
re0 {
  system {
    syslog {
      file messages {
        any info;
      }
      host sfc0-master {
        any none;
      }
    }
  }
}
```

```
}
re1 {
  ... same statements as for re0 ...
}
lcc0-re0 {
  system {
    syslog {
      file messages {
        authorization info;
      }
    }
  }
}
lcc0-re1 {
  ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
  system {
    syslog {
      file messages {
        any notice;
      }
    }
  }
}
lcc0-re1 {
  ... same statements as for lcc1-re0 ...
}
```

**Related Documentation**

- [Configuring System Logging for a TX Matrix Plus Router on page 59](#)



## CHAPTER 5

# Examples

- [Examples: Configuring System Logging on page 67](#)
- [Examples: Assigning an Alternative Facility on page 69](#)
- [Examples: Displaying a Log File on page 69](#)
- [Examples: Displaying System Log Message Descriptions on page 70](#)

### Examples: Configuring System Logging

---

The following example shows how to configure the logging of messages about all commands entered by users at the CLI prompt or invoked by client applications such as Junos XML protocol or NETCONF client applications, and all authentication or authorization attempts, both to the file **cli-commands** and to the terminal of any user who is logged in:

```
[edit system]
syslog {
  file cli-commands {
    interactive-commands info;
    authorization info;
  }
  user * {
    interactive-commands info;
    authorization info;
  }
}
```

The following example shows how to configure the logging of all changes in the state of alarms to the file **/var/log/alarms**:

```
[edit system]
syslog {
  file alarms {
    kernel warning;
  }
}
```

The following example shows how to configure the handling of messages of various types, as described in the comments. Information is logged to two files, to the terminal of user **alex**, to a remote machine, and to the console:

```
[edit system]
```

```
syslog {
  /* write all security-related messages to file /var/log/security */
  file security {
    authorization info;
    interactive-commands info;
  }
  /* write messages about potential problems to file /var/log/messages: */
  /* messages from "authorization" facility at level "notice" and above, */
  /* messages from all other facilities at level "warning" and above */
  file messages {
    authorization notice;
    any warning;
  }
  /* write all messages at level "critical" and above to terminal of user "alex" if */
  /* that user is logged in */
  user alex {
    any critical;
  }
  /* write all messages from the "daemon" facility at level "info" and above, and */
  /* messages from all other facilities at level "warning" and above, to the */
  /* machine monitor.mycompany.com */
  host monitor.mycompany.com {
    daemon info;
    any warning;
  }
  /* write all messages at level "error" and above to the system console */
  console {
    any error;
  }
}
```

The following example shows how to configure the handling of messages generated when users issue Junos OS CLI commands, by specifying the **interactive-commands** facility at the following severity levels:

- **info**—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file `/var/log/user-actions`.
- **notice**—Logs a message when users issue the configuration mode commands **rollback** and **commit**. The example writes the messages to the terminal of user **philip**.
- **warning**—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

```
[edit system]
syslog {
  file user-actions {
    interactive-commands info;
  }
  user philip {
    interactive-commands notice;
  }
  console {
    interactive-commands warning;
  }
}
```

```
}
```

**Related  
Documentation**

- [Single-Chassis System Logging Configuration Overview on page 5](#)

## Examples: Assigning an Alternative Facility

Log all messages generated on the local routing platform at the error level or higher to the **local0** facility on the remote machine called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
  any error;
  facility-override local0;
}
```

Configure routing platforms located in California and routing platforms located in New York to send messages to a single remote machine called **central-logger.mycompany.com**. The messages from California are assigned alternative facility **local0** and the messages from New York are assigned to alternative facility **local2**.

- Configure California routing platforms to aggregate messages in the **local0** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
  change-log info;
  facility-override local0;
}
```

- Configure New York routing platforms to aggregate messages in the **local2** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
  change-log info;
  facility-override local2;
}
```

On **central-logger**, you can then configure the system logging utility to write messages from the **local0** facility to the file **california-config** and the messages from the **local2** facility to the file **new-york-config**.

**Related  
Documentation**

- [Junos OS System Log Alternate Facilities for Remote Logging on page 38](#)

## Examples: Displaying a Log File

Display the contents of the **/var/log/messages** file stored on the local Routing Engine. (The **/var/log** directory is the default location for log files, so you do not need to include it in the filename. The **messages** file is a commonly configured destination for system log messages.)

```
user@host> show log messages Apr 11 10:27:25 router1 mgd[3606]:
UI_DATABASE_LOGIN_EVENT: User 'barbara' entering configuration mode
```

```
Apr 11 10:32:22 router1 mgd[3606]: UI_DBASE_LOGOUT_EVENT: User 'barbara' exiting
configuration mode
Apr 11 11:36:15 router1 mgd[3606]: UI_COMMIT: User 'root' performed commit: no comment
Apr 11 11:46:37 router1 mib2d[2905]: SNMP_TRAP_LINK_DOWN: ifIndex 82, ifAdminStatus
up(1), ifOperStatus down(2), ifName at-1/0/0
```

Display the contents of the file `/var/log/processes`, which has been previously configured to include messages from the **daemon** facility. When issuing the **file show** command, you must specify the full pathname of the file:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
Feb 22 20:35:07 router1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 router1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 23 07:38:19 router1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold:
SNMP trap: cold start
```

Display the contents of the file `/var/log/processes` when the **explicit-priority** statement is included at the `[edit system syslog file processes]` hierarchy level:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
start
Feb 22 20:35:07 router1 snmpd[359]:
%DAEMON-6-SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler: cleared
all throttled traps
Feb 23 07:34:56 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
start
Feb 23 07:38:19 router1 snmpd[359]:
%DAEMON-2-SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold start
```

---

## Examples: Displaying System Log Message Descriptions

Display the list of all currently available system log message descriptions:

```
user@host> help syslog ?

Possible completions:
<syslog-tag>   Syslog tag
. . . . .
BOOTPD_ARG_ERR  Command-line option was invalid
BOOTPD_BAD_ID   Request failed because assembly ID was unknown
BOOTPD_BOOTSTRING tnp.bootpd provided boot string
BOOTPD_CONFIG_ERR tnp.bootpd could not parse configuration file;
                  used default settings
BOOTPD_CONF_OPEN tnp.bootpd could not open configuration file
BOOTPD_DUP_REV  Extra boot string definitions for revision were
                  ignored
---(more 4%)---
```

Display the list of all currently available system log message descriptions for tags that begin with the letters **ACCT** (there is no space between **ACCT** and the question mark, and some descriptions are shortened for legibility):

```
user@host> help syslog ACCT?
```

Possible completions:

```
<syslog-tag>      System log tag or regular expression
ACCT_ACCOUNTING_FERROR    Error occurred during file processing
ACCT_ACCOUNTING_FOPEN_ERROR  Open operation failed on file
ACCT_ACCOUNTING_SMALL_FILE_SIZE Maximum file size is smaller than ...
ACCT_BAD_RECORD_FORMAT    Record format does not match accounting profile
ACCT_CU_RTSLIB_ERROR      Error occurred obtaining current class usage ...
ACCT_FORK_ERR             Could not create child process
ACCT_FORK_LIMIT_EXCEEDED  Could not create child process because of limit
ACCT_GETHOSTNAME_ERROR    gethostname function failed
ACCT_MALLOC_FAILURE       Memory allocation failed
ACCT_UNDEFINED_COUNTER_NAME Filter profile used undefined counter name
ACCT_XFER_FAILED          Attempt to transfer file failed
ACCT_XFER_POPEN_FAIL      File transfer failed
```

Display the description of the `UI_CMDLINE_READ_LINE` message:

```
user@host> help syslog UI_CMDLINE_READ_LINE
```

```
Name:      UI_CMDLINE_READ_LINE
Message:    User '<users>', command '<input>'
Help:       User entered command at CLI prompt
Description: The indicated user typed the indicated command at the CLI
              prompt and pressed the Enter key, sending the command string
              to the management process (mgd).
Type:       Event: This message reports an event, not an error
Severity:   info
```



## CHAPTER 6

# Configuration Statements

- [System Management Configuration Statements on page 73](#)

### System Management Configuration Statements

---

This topic lists all the configuration statements that you can include at the **[edit system]** hierarchy level to configure system management features:

```
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
archival {
  configuration {
    archive-sites {
      ftp://<username>:<password>@<host>:<port>/<url-path>;
      ftp://<username>:<password>@<host>:<port>/<url-path>;
    }
    transfer-interval interval;
  }
}
```

```

        transfer-on-commit;
    }
}
allow-v4mapped-packets;
arp {
    aging-timer minutes;
    gratuitous-arp-delay;
    gratuitous-arp-on-ifup;
    interfaces;
    passive-learning;
    purging;
}
authentication-order [ authentication-methods ];
backup-router address <destination destination-address>;
commit synchronize;
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
dump-device (compact-flash | remove-compact | usb);
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
    versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options {
    tcp-mss mss-value;
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
    icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323-paws;
    no-tcp-rfc1323;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
}
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
login {

```



```

announcement text;
class class-name {
    access-end;
    access-start;
    allow-commands "regular-expression";
    ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular
        expression 2";
    allowed-days;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
        expression 2 ";
    idle-timeout minutes;
    login-tip;
    permissions [ permissions ];
}
message text;
password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
}
retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
}
user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
}
login-tip number;
mirror-flash-on-disk;
name-server {
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key key-number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
}

```

```
source-address source-address;  
server address <key key-number> <version value> <prefer>;  
trusted-key [ key-numbers ];  
}  
ports {  
  auxiliary {  
    type terminal-type;  
  }  
  pic-console-authentication {  
    encrypted-password encrypted-password;  
    plain-text-password;  
    console {  
      insecure;  
      log-out-on-disconnect;  
      type terminal-type;  
      disable;  
    }  
  }  
}  
processes {  
  process--name (enable | disable) failover (alternate-media | other-routing-engine);  
  timeout seconds;  
}  
}  
radius-server server-address {  
  accounting-port port-number;  
  port port-number;  
  retry number;  
  secret password;  
  source-address source-address;  
  timeout seconds;  
}  
radius-options {  
  password-protocol mschap-v2;  
}  
attributes {  
  nas-ip-address ip-address;  
}  
root-authentication {  
  (encrypted-password "password" | plain-text-password);  
  ssh-rsa "public-key";  
  ssh-dsa "public-key";  
}  
(saved-core-context | no-saved-core-context);  
saved-core-files saved-core-files;  
scripts {  
  commit {  
    allow-transients;  
    file filename {  
      optional;  
      refresh;  
      refresh-from url;  
      source url;  
    }  
  }  
  traceoptions {  
    file <filename> <files number> <size size> <world-readable | no-world-readable>;  
    flag flag;  
    no-remote-trace;  
  }  
}
```

```

}
op {
  file filename {
    arguments {
      argument-name {
        description descriptive-text;
      }
    }
    command filename-alias;
    description descriptive-text;
    refresh;
    refresh-from url;
    source url;
  }
  refresh;
  refresh-from url;
  traceoptions {
    file <filename> <files number> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
}
services {
  finger {
    connection-limit limit;
    rate-limit limit;
  }
  flow-tap-dtcp {
    ssh {
      connection-limit limit;
      rate-limit limit;
    }
  }
  ftp {
    connection-limit limit;
    rate-limit limit;
  }
  service-deployment {
    servers server-address {
      port port-number;
    }
    source-address source-address;
  }
  ssh {
    root-login (allow | deny | deny-password);
    protocol-version [v1 v2];
    connection-limit limit;
    rate-limit limit;
  }
  telnet {
    connection-limit limit;
    rate-limit limit;
  }
  web-management {
    http {

```

```
    interfaces [ interface-names ];
    port port;
}
https {
    interfaces [ interface-names ];
    local-certificate name;
    port port;
}
session {
    idle-timeout [ minutes ];
    session-limit [ session-limit ];
}
}
xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
}
xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
}
}
static-host-mapping {
    hostname {
        alias [ alias ];
        inet [ address ];
        sysid system-identifier;
    }
}
syslog {
    archive <files number> <size size> <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
            no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
}
host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
        brief;
    }
}
```

```
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
        facility severity;
        match "regular-expression";
    }
}
tacplus-options {
    service-name service-name;
    (no-cmd-attribute-value | exclude-cmd-attribute);
}
tacplus-server server-address {
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
}
time-zone (GMThour-offset | time-zone);
}
tracing {
    destination-override {
        syslog host;
    }
}
use-imported-time-zones;
}
```

## allow-duplicates

---

<b>Syntax</b>	allow-duplicates
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog], [edit logical-systems <i>logical-system-name</i> system syslog file <i>file-name</i> ], [edit logical-systems <i>logical-system-name</i> system syslog host <i>host-name</i> ], [edit logical-systems <i>logical-system-name</i> system syslog user <i>user-name</i> ], [edit system syslog], [edit system syslog file <i>file-name</i> ], [edit system syslog host <i>host-name</i> ], [edit system syslog user <i>user-name</i> ],
<b>Release Information</b>	Statement introduced in Release 11.1 of Junos OS. Logical systems support introduced in Release 11.4 of Junos OS.
<b>Description</b>	Specify whether to allow the repeated messages in the system log output files. This can be set either at global configuration level or for individual file, host, or user. By default, this parameter is set to disable.
<b>Options</b>	<b>file</b> —Name of the file to log messages  <b>host</b> —Host to receive the messages  <b>user</b> —User to receive the notification of the event
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Junos OS Monitoring and Troubleshooting Guide for Security Devices</a></li><li>• Example: Configuring System Logging on Logical Systems</li></ul>

## archive (All System Log Files)

<b>Syntax</b>	<code>archive &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;start-time<i>time</i>&gt; &lt;transfer-interval <i>interval</i>&gt; &lt;world-readable   no-world-readable&gt; ;</code>
<b>Hierarchy Level</b>	[edit system <a href="#">syslog</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Configure archiving properties for all system log files.
<b>Options</b>	<p><b>files <i>number</i></b>—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file <b><i>logfile</i></b>, it closes the file, compresses it, and renames it <b><i>logfile.0.gz</i></b> (the amount of data is determined by the <b>size</b> statement at this hierarchy level). The utility then opens and writes to a new file called <b><i>logfile</i></b>. When the new file reaches the maximum size, the <b><i>logfile.0.gz</i></b> file is renamed to <b><i>logfile.1.gz</i></b>, and the new file is closed, compressed, and renamed <b><i>logfile.0.gz</i></b>. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).</p> <p><b>Range:</b> 1 through 1000</p> <p><b>Default:</b> 10 files</p> <p><b>size <i>size</i></b>—Maximum amount of data that the Junos OS logging utility writes to a log file <b><i>logfile</i></b> before archiving it (closing it, compressing it, and changing its name to <b><i>logfile.0.gz</i></b>). The utility then opens and writes to a new file called <b><i>logfile</i></b>.</p> <p><b>Syntax:</b> <b><i>xk</i></b> to specify the number of kilobytes, <b><i>xm</i></b> for the number of megabytes, or <b><i>xg</i></b> for the number of gigabytes</p> <p><b>Range:</b> 64 KB through 1 GB</p> <p><b>Default:</b> 128 KB for J Series routers; 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers</p> <p><b>world-readable   no-world-readable</b>—Grant all users permission to read archived log files, or restrict the permission only to the <b>root</b> user and users who have the Junos OS <b>maintenance</b> permission.</p> <p><b>Default:</b> no-world-readable</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Specifying Log File Size, Number, and Archiving Properties on page 40</a></li> </ul>

## archive (Individual System Log File)

---

<b>Syntax</b>	<code>archive &lt;archive-sites (ftp-url &lt;password password&gt;)&gt; &lt;files number&gt; &lt;size size&gt; &lt;start-time "YYYY-MM-DD.hh:mm"&gt; &lt;transfer-interval minutes&gt; &lt;world-readable   no-world-readable&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit system syslog file filename]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>start-time</b> and <b>transfer-interval</b> statements introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Configure archiving properties for a specific system log file.
<b>Options</b>	<p><b>archive-sites site-name</b>—FTP URL representing the destination for the archived log file (for information about how to specify valid FTP URLs, see Format for Specifying Filenames and URLs in Junos OS CLI Commands). If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the filename specified at the <code>[edit system syslog]</code> hierarchy level.</p> <p><b>files number</b>—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file <i>logfile</i>, it closes the file, compresses it, and renames it <i>logfile.0.gz</i> (the amount of data is determined by the <b>size</b> statement at this hierarchy level). The utility then opens and writes to a new file called <i>logfile</i>. When the new file reaches the maximum size, the <i>logfile.0.gz</i> file is renamed to <i>logfile.1.gz</i>, and the new file is closed, compressed, and renamed <i>logfile.0.gz</i>. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).</p> <p><b>Range:</b> 1 through 1000</p> <p><b>Default:</b> 10 files</p> <p><b>password password</b>—Password for authenticating with the site specified by the <b>archive-sites</b> statement.</p> <p><b>size size</b>—Maximum amount of data that the Junos OS logging utility writes to a log file <i>logfile</i> before archiving it (closing it, compressing it, and changing its name to <i>logfile.0.gz</i>). The utility then opens and writes to a new file called <i>logfile</i>.</p> <p><b>Syntax:</b> <b>xk</b> to specify the number of kilobytes, <b>xm</b> for the number of megabytes, or <b>xg</b> for the number of gigabytes</p> <p><b>Range:</b> 64 KB through 1 GB</p> <p><b>Default:</b> 128 KB for J Series routers; 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers</p>



**start-time "YYYY-MM-DD.hh:mm"**—Date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

**transfer-interval *interval***—Interval at which to transfer the log file to an archive site.

**Range:** 5 through 2880 minutes

**world-readable | no-world-readable**—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

**Default:** no-world-readable

**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**

- [Specifying Log File Size, Number, and Archiving Properties on page 40](#)

## console (System Logging)

**Syntax** console {  
    *facility severity*;  
}

**Hierarchy Level** [edit system [syslog](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** Configure the logging of system messages to the system console.

**Options** ***facility***—Class of messages to log. To specify multiple classes, include multiple ***facility severity*** statements. For a list of the facilities, see Junos OS System Logging Facilities and Message Severity Levels.

***severity***—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Junos OS System Logging Facilities and Message Severity Levels.

**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**

- [Directing System Log Messages to the Console on page 34](#)
- [Junos OS System Log Messages Reference](#)

## destination-override

---

<b>Syntax</b>	<pre>destination-override {     syslog host <i>ip-address</i>; }</pre>
<b>Hierarchy Level</b>	[edit system tracing]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	This option overrides the system-wide configuration under <b>[edit system tracing]</b> and has no effect if system tracing is not configured.
<b>Options</b>	<p>These options specify the system logs and the host to which remote tracing output is sent:</p> <ul style="list-style-type: none"><li>• <b>syslog</b>—Specify the system process log files to send to the remote tracing host.</li><li>• <b>host <i>ip-address</i></b>—Specify the IP address to which to send tracing information.</li></ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Junos OS Tracing and Logging Operations</li><li>• Understanding Tracing and Logging Operations</li><li>• <a href="#">tracing on page 97</a></li></ul>

## explicit-priority

<b>Syntax</b>	explicit-priority;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i> ], [edit logical-systems <i>logical-system-name</i> system syslog host], [edit system syslog file <i>filename</i> ], [edit system syslog host]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Record the priority (facility and severity level) in each standard-format system log message directed to a file or remote destination.  When the <b>structured-data</b> statement is also included at the [edit system syslog file <i>filename</i> ] hierarchy level, this statement is ignored for the file.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Including Priority Information in System Log Messages on page 41</a></li> <li>• <a href="#">Junos OS System Log Messages Reference</a></li> <li>• <a href="#">structured-data on page 93</a></li> </ul>

## facility-override

<b>Syntax</b>	facility-override <i>facility</i> ;
<b>Hierarchy Level</b>	[edit system syslog host]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Substitute an alternate facility for the default facilities used when messages are directed to a remote destination.
<b>Options</b>	<i>facility</i> —Alternate facility to substitute for the default facilities. For a list of the possible facilities, see <a href="#">Table 20 on page 38</a> .
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Changing the Alternative Facility Name for Remote System Log Messages on page 36</a></li> <li>• <a href="#">Junos OS System Log Messages Reference</a></li> </ul>

## file (System Logging)

---

Syntax	<pre>file <i>filename</i> {     <i>facility severity</i>;     archive {         <i>files number</i>;         <i>size size</i>;         (no-world-readable   world-readable);     }     explicit-priority;     match "<i>regular-expression</i>";     structured-data {         brief;     } }</pre>
Hierarchy Level	[edit system <a href="#">syslog</a> ]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure the logging of system messages to a file.
Options	<p><b>facility</b>—Class of messages to log. To specify multiple classes, include multiple <b>facility severity</b> statements. For a list of the facilities, see Junos OS System Logging Facilities and Message Severity Levels.</p> <p><b>file filename</b>—File in the <code>/var/log</code> directory in which to log messages from the specified facility. To log messages to more than one file, include more than one <b>file</b> statement.</p> <p><b>severity</b>—Severity of the messages that belong to the facility specified by the paired <b>facility</b> name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Junos OS System Logging Facilities and Message Severity Levels.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Directing System Log Messages to a Log File on page 32</a></li><li>• <a href="#">Junos OS System Log Messages Reference</a></li></ul>

## files

<b>Syntax</b>	<code>files <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit system syslog archive], [edit system syslog file <i>filename</i> <a href="#">archive</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for EX Series switches.
<b>Description</b>	Configure the maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file <i>logfile</i> , it closes the file, compresses it, and renames it to <i>logfile.0.gz</i> (for information about the maximum file size, see <a href="#">size</a> ). The utility then opens and writes to a new file called <i>logfile</i> . When the new file reaches the maximum size, the <i>logfile.0.gz</i> file is renamed to <i>logfile.1.gz</i> , and the new file is closed, compressed, and renamed <i>logfile.0.gz</i> . By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).
<b>Options</b>	<i>number</i> —Maximum number of archived files. <b>Range:</b> 1 through 1000 <b>Default:</b> 10 files
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Specifying Log File Size, Number, and Archiving Properties on page 40</a></li> <li>• <a href="#">Junos OS System Log Messages Reference</a></li> <li>• <a href="#">size on page 92</a></li> </ul>

## host

---

<b>Syntax</b>	<pre>host (hostname   other-routing-engine) {     facility severity;     explicit-priority;     facility-override facility;     log-prefix string;     match "regular-expression";     source-address source-address;     structured-data {         brief;     } }</pre>
<b>QFX Series</b>	<pre>host (hostname {     facility severity;     explicit-priority;     facility-override facility;     log-prefix string;     match "regular-expression";     port;     source-address source-address; }</pre>
<b>TX Matrix Router and EX Series Switches</b>	<pre>host (hostname   other-routing-engine   scc-master) {     facility severity;     explicit-priority;     facility-override facility;     log-prefix string;     match "regular-expression";     port;     source-address source-address; }</pre>
<b>TX Matrix Plus Router</b>	<pre>host (hostname   other-routing-engine   sfc0-master) {     facility severity;     explicit-priority;     facility-override facility;     log-prefix string;     match "regular-expression";     port;     source-address source-address; }</pre>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog], [edit system syslog]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Configure the logging of system messages to a remote destination.

**Options** *facility*—Class of messages to log. To specify multiple classes, include multiple *facility severity* statements. For a list of the facilities, see Junos OS System Logging Facilities and Message Severity Levels.

*hostname*—IPv4 address, IPv6 address, or fully qualified hostname of the remote machine to which to direct messages. To direct messages to multiple remote machines, include a **host** statement for each one.

**other-routing-engine**—Direct messages to the other Routing Engine on a router or switch with two Routing Engines installed and operational.



**NOTE:** The **other-routing-engine** option is not applicable to the QFX Series.

**port**—Port number of the remote syslog server that can be modified.

**scc-master**—(TX Matrix routers only) On a T640 router that is part of a routing matrix, direct messages to the TX Matrix router.

*severity*—Severity of the messages that belong to the facility specified by the paired *facility* name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Junos OS System Logging Facilities and Message Severity Levels.

**sfc0-master**—(TX Matrix Plus routers only) On a T1600 router that is part of a routing matrix, direct messages to the TX Matrix Plus router.

The remaining statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

- Related Documentation**
- [Directing System Log Messages to a Remote Machine or the Other Routing Engine on page 34](#)
  - [Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router on page 55](#)
  - [Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router on page 63](#)
  - [Junos OS System Log Messages Reference](#)

## log-prefix

---

<b>Syntax</b>	<code>log-prefix <i>string</i>;</code>
<b>Hierarchy Level</b>	[edit system syslog host]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Include a text string in each message directed to a remote destination.
<b>Options</b>	<i>string</i> —Text string to include in each message.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Adding a Text String to System Log Messages on page 39</a></li><li>• <a href="#">Junos OS System Log Messages Reference</a></li></ul>

## log-rotate-frequency

---

<b>Syntax</b>	<code>log-rotate-frequency <i>frequency</i>;</code>
<b>Hierarchy Level</b>	[set system <a href="#">syslog</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.3.
<b>Description</b>	Configure the system log file rotation frequency by configuring the time interval for checking the log file size.  When the log file size has exceeded the configured limit, the old log file is archived and a new log file is created.
<b>Options</b>	<i>frequency</i> —Frequency of rotation of the system log file. <b>Range:</b> 1 minute through 59 minutes <b>Default:</b> 15 minutes
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Specifying Log File Size, Number, and Archiving Properties on page 40</a></li><li>• <a href="#">syslog on page 94</a></li></ul>



## match

---

<b>Syntax</b>	<code>match "regular-expression";</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i> ], [edit logical-systems <i>logical-system-name</i> system syslog user ( <i>username</i>   *)], [edit system syslog file <i>filename</i> ], [edit system syslog host <i>hostname</i>   other-routing-engine  scc-master)], [edit system syslog user ( <i>username</i>   *)]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Using Regular Expressions to Refine the Set of Logged Messages on page 45</a></li> </ul>

## no-remote-trace

---

See [tracing](#).

## port

---

<b>Syntax</b>	<code>port port number;</code>
<b>Hierarchy Level</b>	[edit system syslog host <i>hostname</i>   other-routing-engine  scc-master)]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.3.
<b>Description</b>	Specify the port number for the remote syslog server.
<b>Options</b>	<i>port number</i> —Port number of the remote syslog server. <b>Range:</b> 0 through 65535 <b>Default:</b> 514
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">syslog on page 94</a></li> <li>• <a href="#">host on page 88</a></li> </ul>

## size

---


<b>Syntax</b>	<code>size size;</code>
<b>Hierarchy Level</b>	[edit system syslog archive], [edit system syslog file <i>filename</i> archive]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Configure the maximum amount of data that the Junos OS logging utility writes to a log file <b>logfile</b> before archiving it (closing it, compressing it, and changing its name to <b>logfile.0.gz</b> ). The utility then opens and writes to a new file called <b>logfile</b> . For information about the number of archive files that the utility creates in this way, see <a href="#">files</a> .
<b>Options</b>	<b>size</b> —Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). <b>Syntax:</b> <b>xk</b> to specify the number of kilobytes, <b>xm</b> for the number of megabytes, or <b>xg</b> for the number of gigabytes <b>Range:</b> 64 KB through 1 GB <b>Default:</b> 1 MB for MX Series routers and the QFX Series
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Specifying Log File Size, Number, and Archiving Properties on page 40</a></li><li>• <a href="#">Junos OS System Log Messages Reference</a></li><li>• <a href="#">files on page 87</a></li></ul>

## system

---

<b>Syntax</b>	<code>system { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure system management properties.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">System Management Configuration Statements on page 73</a></li></ul>

## structured-data

<b>Syntax</b>	structured-data { brief; }
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i> ], [edit system syslog file <i>filename</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Write system log messages to the log file in structured-data format, which complies with Internet draft draft-ietf-syslog-protocol-23, <i>The syslog Protocol</i> ( <a href="http://tools.ietf.org/html/draft-ietf-syslog-protocol-23">http://tools.ietf.org/html/draft-ietf-syslog-protocol-23</a> ).
<div>  <p><b>NOTE:</b> When this statement is included, other statements that specify the format for messages written to the file are ignored (the <code>explicit-priority</code> statement at the [edit system syslog file <i>filename</i>] hierarchy level and the <code>time-format</code> statement at the [edit system syslog] hierarchy level).</p> </div>	
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Logging Messages in Structured-Data Format on page 32</a></li> <li>• <a href="#">Junos OS System Log Messages Reference</a></li> <li>• <a href="#">explicit-priority on page 85</a></li> <li>• <a href="#">time-format on page 96</a></li> </ul>

## syslog

---

**Syntax**    `syslog {`  
              `archive {`  
                  `files` *number*;  
                  `size` *maximum-file-size*;  
                  `start-time` "YYYY-MM-DD.hh:mm";  
                  `transfer-interval` *minutes*;  
                  `(world-readable | no-world-readable)`;  
              `}`  
              `console {`  
                  `facility` *severity*;  
              `}`  
              `file` *filename* {  
                  `facility` *severity*;  
                  `explicit-priority`;  
                  `match` "regular-expression";  
                  `archive {`  
                      `files` *number*;  
                      `size` *maximum-file-size*;  
                      `start-time` "YYYY-MM-DD.hh:mm";  
                      `transfer-interval` *minutes*;  
                      `(world-readable | no-world-readable)`;  
                  `}`  
                  `structured-data` {  
                      `brief`;  
                  `}`  
              `}`  
              `host` (*hostname* | *other-routing-engine* | *scc-master*) {  
                  `facility` *severity*;  
                  `explicit-priority`;  
                  `facility-override` *facility*;  
                  `log-prefix` *string*;  
                  `match` "regular-expression";  
                  `source-address` *source-address*;  
                  `structured-data` {  
                      `brief`;  
                  `}`  
                  `port` *port number*;  
              `}`  
              `log-rotate-frequency` *frequency*;  
              `source-address` *source-address*;  
              `time-format` (*millisecond* | *year* | *year millisecond*);  
              `user` (*username* | *\**) {  
                  `facility` *severity*;  
                  `match` "regular-expression";  
              `}`  
              `}`

**Hierarchy Level**    [edit logical-systems *logical-system-name* system],  
                          [edit system]

**Release Information**    Statement introduced before Junos OS Release 7.4.  
                              Statement introduced in Junos OS Release 9.0 for EX Series switches.

Statement introduced in Junos OS Release 11.1 for the QFX Series.  
Support at the **[edit logical-systems *logical-system-name* system]** hierarchy level introduced in Junos OS Release 11.4.

**Description** Configure the types of system log messages to log to files, a remote destination, user terminals, or the system console.

The remaining statements are explained separately.


**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**

- [Junos OS System Log Configuration Overview on page 3](#)
- [Junos OS System Log Messages Reference](#)
- Overview of Single-Chassis System Logging Configuration

## time-format

---

<b>Syntax</b>	<code>time-format (year   millisecond   year millisecond);</code>
<b>Hierarchy Level</b>	<code>[edit system syslog]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	<p>Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a <b>file</b>, <b>console</b>, or <b>user</b> statement at the <code>[edit system syslog]</code> hierarchy level, but not to destinations configured by a <b>host</b> statement.</p> <p>By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged—for example, <b>Aug 21 12:36:30</b>. However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the <code>[edit system syslog time-format]</code> statement.</p>
	<div><p><b>NOTE:</b> When the <b>structured-data</b> statement is included at the <code>[edit system syslog file <i>filename</i>]</code> hierarchy level, this statement is ignored for the file.</p></div>
<b>Options</b>	<p><b>millisecond</b>—Include the millisecond in the timestamp.</p> <p><b>year</b>—Include the year in the timestamp.</p>
<b>Required Privilege Level</b>	<p><b>system</b>—To view this statement in the configuration.</p> <p><b>system-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Including the Year or Millisecond in Timestamps on page 45</a></li><li>• <a href="#">Junos OS System Log Messages Reference</a></li><li>• <a href="#">structured-data on page 93</a></li></ul>

## tracing

---

<b>Syntax</b>	tracing { destination-override syslog host <i>ip-address</i> ; }
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	<p>Configure the router to enable remote tracing to a specified host IP address. The default setting is disabled.</p> <p>The following processes are supported:</p> <ul style="list-style-type: none"> <li>• <b>chassisd</b>—Chassis-control process</li> <li>• <b>eventd</b>—Event-processing process</li> <li>• <b>cosd</b>—Class-of-service process</li> <li>• <b>spd</b>—Adaptive-services process</li> </ul> <p>You can use the <b>no-remote-trace</b> statement, under the [edit system process-name traceoptions] hierarchy, to disable remote tracing.</p>
<b>Options</b>	<b>destination-override syslog host <i>ip-address</i></b> —Overrides the global config under <b>system tracing</b> and has no effect if <b>system tracing</b> is not configured.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Junos OS Tracing and Logging Operations</li> <li>• <a href="#">destination-override on page 84</a></li> <li>• <a href="#">no-remote-trace on page 91</a></li> </ul>

## user (System Logging)

---

<b>Syntax</b>	<pre>user (username   *) {     facility severity;     match "regular-expression"; }</pre>
<b>Hierarchy Level</b>	[edit system syslog]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Configure the logging of system messages to user terminals.
<b>Options</b>	<p><b>*</b> (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.</p> <p><b>facility</b>—Class of messages to log. To specify multiple classes, include multiple <b>facility severity</b> statements. For a list of the facilities, see Junos OS System Logging Facilities and Message Severity Levels.</p> <p><b>severity</b>—Severity of the messages that belong to the facility specified by the paired <b>facility</b> name. Messages with severities the specified level and higher are logged. For a list of the severities, see Junos OS System Logging Facilities and Message Severity Levels.</p> <p><b>username</b>—Junos OS login name of the user whose terminal session is to receive system log messages. To log messages to more than one user's terminal session, include more than one <b>user</b> statement.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Directing System Log Messages to a User Terminal on page 33</a></li><li>• <a href="#">Junos OS System Logging Facilities and Message Severity Levels</a></li><li>• <a href="#">Junos OS System Log Messages Reference</a></li></ul>



---

## world-readable

---

<b>Syntax</b>	world-readable   no-world-readable;
<b>Hierarchy Level</b>	[edit system <a href="#">syslog archive</a> ], [edit system <a href="#">syslog file filename archive</a> ]
<b>Release Information</b>	Statement introduced before OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Grant all users permission to read log files, or restrict the permission only to the <b>root</b> user and users who have the Junos <b>maintenance</b> permission.
<b>Default</b>	no-world-readable
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Specifying Log File Size, Number, and Archiving Properties on page 40</a></li><li>• <i>Junos System Log Messages Reference</i></li></ul>



## PART 3

# Administration

- [Administrative Commands on page 103](#)
- [Monitoring Commands on page 105](#)



## CHAPTER 7

# Administrative Commands

## clear log

---

<b>Syntax</b>	<code>clear log <i>filename</i></code> <code>&lt;all&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	Remove contents of a log file.
<b>Options</b>	<b><i>filename</i></b> —Name of the specific log file to delete.  <b>all</b> —(Optional) Delete the specified log file and all archived versions of it.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show log on page 109</a></li></ul>
<b>List of Sample Output</b>	<a href="#">clear log on page 104</a>
<b>Output Fields</b>	See file list for an explanation of output fields.

## Sample Output

**clear log** The following sample commands list log file information, clear the contents of a log file, and then display the updated log file information:

```
user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
-----
-rw-r----- 1 root  wheel      26450 Jun 23 18:47 /var/log/sampled
total 1

user@host> clear log lcc0-re0:sampled
lcc0-re0:
-----

user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
-----
-rw-r----- 1 root  wheel      57 Sep 15 03:44 /var/log/sampled
total 1
```

## CHAPTER 8

# Monitoring Commands

## monitor list

<b>Syntax</b>	monitor list
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Display the status of monitored log and trace files.
<b>Options</b>	This command has no options.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are those configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols protocol]</b> hierarchy levels.
<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">monitor start on page 107</a></li> <li>• <a href="#">monitor stop on page 111</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor list on page 106</a>
<b>Output Fields</b>	<a href="#">Table 25 on page 106</a> describes the output fields for the <b>monitor list</b> command. Output fields are listed in the approximate order in which they appear.

**Table 25: monitor list Output Fields**

Field Name	Field Description
<b>monitor start</b>	Indicates the file is being monitored.
<b>"filename"</b>	Name of the file that is being monitored.
<b>Last changed</b>	Date and time at which the file was last modified.

## Sample Output

```

monitor list user@host> monitor list
monitor start "vrrpd" (Last changed Dec 03:11:06 20)
monitor start "cli-commands" (Last changed Nov 07:3)

```



## monitor start

<b>Syntax</b>	<code>monitor start <i>filename</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Start displaying the system log or trace file and additional entries being added to those files.
<b>Options</b>	<i>filename</i> —Specific log or trace file.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols protocol]</b> hierarchy levels.



**NOTE:** To monitor a log file within a logical system, issue the `monitor start logical-system-name/filename` command.

<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">monitor list on page 106</a></li> <li>• <a href="#">monitor stop on page 111</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor start on page 107</a>
<b>Output Fields</b>	<a href="#">Table 26 on page 107</a> describes the output fields for the <b>monitor start</b> command. Output fields are listed in the approximate order in which they appear.

**Table 26: monitor start Output Fields**

Field Name	Field Description
<b>***<i>filename</i>***</b>	Name of the file from which entries are being displayed. This line is displayed initially and when the command switches between log files.
<b><i>Date and time</i></b>	Timestamp for the log entry.

## Sample Output

```
monitor start user@host> monitor start system-log
```

```
*** system-log***
Jul 20 15:07:34 hang sshd[5845]: log: Generating 768 bit RSA key.
Jul 20 15:07:35 hang sshd[5845]: log: RSA key generation complete.
Jul 20 15:07:35 hang sshd[5845]: log: Connection from 204.69.248.180 port 912
Jul 20 15:07:37 hang sshd[5845]: log: RSA authentication for root accepted.
Jul 20 15:07:37 hang sshd[5845]: log: ROOT LOGIN as 'root' from trip.jcmax.com
Jul 20 15:07:37 hang sshd[5845]: log: Closing connection to 204.69.248.180
```

## show log

<b>Syntax</b>	<code>show log</code> <code>&lt;filename   user &lt;username&gt;&gt;</code>
<b>Syntax (TX Matrix Router)</b>	<code>show log</code> <code>&lt;all-lcc   lcc <i>number</i>   scc&gt;</code> <code>&lt;filename   user &lt;username&gt;&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	List log files, display log file contents, or display information about users who have logged in to the router or switch.
<b>Options</b>	<p><b>none</b>—List all log files.</p> <p><b>&lt;all-lcc   lcc <i>number</i>   scc&gt;</b>—(Routing matrix only) (Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace <i>number</i> with a value from 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).</p> <p><b><i>filename</i></b>—(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.</p> <p><b>user &lt;username&gt;</b>—(Optional) Display logging information about users who have recently logged in to the router or switch. If you include <i>username</i>, display logging information about the specified user.</p>
<b>Required Privilege Level</b>	trace
<b>List of Sample Output</b>	<a href="#">show log on page 109</a> <a href="#">show log filename on page 110</a> <a href="#">show log user on page 110</a>

## Sample Output

```

user@host> show log
total 57518
-rw-r--r--  1 root  bin      211663 Oct  1 19:44 dcd
-rw-r--r--  1 root  bin      999947 Oct  1 19:41 dcd.0
-rw-r--r--  1 root  bin      999994 Oct  1 17:48 dcd.1
-rw-r--r--  1 root  bin       238815 Oct  1 19:44 rpd
-rw-r--r--  1 root  bin     1049098 Oct  1 18:00 rpd.0
-rw-r--r--  1 root  bin     1061095 Oct  1 12:13 rpd.1
-rw-r--r--  1 root  bin     1052026 Oct  1 06:08 rpd.2
-rw-r--r--  1 root  bin     1056309 Sep 30 18:21 rpd.3
-rw-r--r--  1 root  bin     1056371 Sep 30 14:36 rpd.4
-rw-r--r--  1 root  bin     1056301 Sep 30 10:50 rpd.5
-rw-r--r--  1 root  bin     1056350 Sep 30 07:04 rpd.6

```

```
-rw-r--r-- 1 root bin      1048876 Sep 30 03:21 rpd.7
-rw-rw-r-- 1 root bin      19656 Oct  1 19:37 wtmp
```

```
show log filename user@host> show log rpd
Oct  1 18:00:18 trace_on: Tracing to ?/var/log/rpd? started
Oct  1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
Oct  1 18:00:18
Oct  1 18:00:19 KRT rcv len 56 V9 seq 148 op add Type route/if af 2 addr
13.13.13.21 nhop type local nhop 13.13.13.21
Oct  1 18:00:19 KRT rcv len 56 V9 seq 149 op add Type route/if af 2 addr
13.13.13.22 nhop type unicast nhop 13.13.13.22
Oct  1 18:00:19 KRT rcv len 48 V9 seq 150 op add Type ifaddr index 24 devindex
43
Oct  1 18:00:19 KRT rcv len 144 V9 seq 151 op chnge Type ifdev devindex 44
Oct  1 18:00:19 KRT rcv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct  1 18:00:19 KRT rcv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct  1 18:00:19 KRT rcv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...
```

```
show log user user@host> show log user
darius mg2546 Thu Oct  1 19:37 still logged in
darius mg2529 Thu Oct  1 19:08 - 19:36 (00:28)
darius mg2518 Thu Oct  1 18:53 - 18:58 (00:04)
root mg1575 Wed Sep 30 18:39 - 18:41 (00:02)
root tty2 jun.site.per Wed Sep 30 18:39 - 18:41 (00:02)
alex tty1 192.168.1.2 Wed Sep 30 01:03 - 01:22 (00:19)
```

## monitor stop

---

<b>Syntax</b>	<code>monitor stop <i>filename</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Stop displaying the system log or trace file.
<b>Options</b>	<i>filename</i> —Specific log or trace file.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are those configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are those configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols <i>protocol</i>]</b> hierarchy levels.
<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">monitor list on page 106</a></li> <li>• <a href="#">monitor start on page 107</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor stop on page 111</a>
<b>Output Fields</b>	This command produces no output.

## Sample Output

```
monitor stop  user@host> monitor stop
```



## PART 4

# Index

- [Index on page 115](#)





# Index

## Symbols

!	
	regular expression operator
	system logging.....46, 48
#	comments in configuration statements.....xii
\$	
	regular expression operator
	system logging.....46, 48
( )	
	regular expression operator
	system logging.....46, 48
( ), in syntax descriptions.....xii	
*	
	regular expression operator
	system logging.....46, 47
+	
	regular expression operator
	system logging.....46, 48
.	
	regular expression operator
	system logging.....46, 47
< >, in syntax descriptions.....xii	
?	
	regular expression operator
	system logging.....46, 48
[ ]	
	regular expression operator
	system logging.....46, 48
[ ], in configuration statements.....xii	
^	
	regular expression operator
	system logging.....46, 48
{ }, in configuration statements.....xii	
	regular expression operator
	system logging.....46, 48
(pipe), in syntax descriptions.....xii	

## A

alert (system logging severity level 1).....44
allow-duplicates statement.....80

archive statement
all system log files.....81
individual system log file.....82
usage guidelines.....40
archive-sites statement
system log files.....82
system logging
usage guidelines.....40
authorization (system logging facility)
option to facility-override statement.....38

## B

braces, in configuration statements.....xii
brackets
angle, in syntax descriptions.....xii
square, in configuration statements.....xii
brief statement
system logging.....93
usage guidelines.....32

## C

clear log command.....104
comments, in configuration statements.....xii
Common Criteria
system logging.....5
console statement
system logging.....83
usage guidelines.....34
conventions
text and syntax.....xi
critical (system logging severity level 2).....44
curly braces, in configuration statements.....xii
customer support.....xiii
contacting JTAC.....xiii

## D

daemon (system logging facility)
option to facility-override statement.....38
debug (system logging severity level 7).....44
documentation
comments on.....xiii

## E

emergency (system logging severity level 0).....44
error (system logging severity level 3).....44
explicit-priority statement.....85
usage guidelines
routing matrix.....54, 63
single-chassis system.....41

**F**

facilities (system logging)	
alternate for remote machine.....	38
default for remote machine.....	38
mapping of codes to names.....	43
facility-override statement.....	85
system logging	
usage guidelines.....	36
file statement	
system logging.....	86
usage guidelines.....	32
files	
log file, clearing.....	104
status of, displaying.....	106
system log messages, archiving.....	40
files statement.....	87
archiving of all system log files.....	81
archiving of individual system log file.....	82
system logging	
usage guidelines.....	40
font conventions.....	xi
ftp (system logging facility)	
option to facility-override statement.....	38

**H**

help syslog command	
usage guidelines.....	12
host statement.....	88
system logging	
usage guidelines for routing	
matrix.....	55, 63
usage guidelines for single-chassis	
system.....	34

**I**

info (system logging severity level 6).....	44
---	----

**J**

Junos-FIPS	
system logging.....	5

**K**

kernel (system logging facility)	
option to facility-override statement.....	38

**L**

local0 - local7 (options to facility-override statement).....	38
---	----

## log files

clearing contents of.....	104
contents, displaying.....	109
display of	
starting.....	107
stopping.....	111
specifying properties.....	40
status, displaying.....	106
log-prefix statement	
system logging.....	90
usage guidelines.....	39
log-rotate-frequency statement.....	90

**M**

manuals	
comments on.....	xiii
match statement.....	91
usage guidelines.....	45
monitor list command.....	106
monitor start command.....	107
monitor stop command.....	111

**N**

no-world-readable statement	
archiving of all system log files.....	81
archiving of individual system log file.....	82
system logging.....	99
usage guidelines.....	40
notice (system logging severity level 5).....	44

**O**

operators, regular expression	
system logging.....	46, 47
other-routing-engine option to host statement.....	88
usage guidelines	
routing matrix.....	55, 63
single-chassis system.....	34

**P**

parentheses, in syntax descriptions.....	xii
port statement.....	91
priorities	
system logging, including in log message	
for routing matrix.....	54, 63
for single-chassis system.....	41

**R**

real-time monitoring	
files.....	106

regular expression operators  
     system logging.....47

## S

scc-master option to host statement.....88  
     usage guidelines.....53  
 severity levels for system logging.....44  
 show log command.....109  
 size statement.....92  
     archiving of all system log files.....81  
     archiving of individual system log file.....82  
     system logging  
         usage guidelines.....40  
 source-address statement  
     system logging  
         usage guidelines for routing  
             matrix.....55, 63  
         usage guidelines for single-chassis  
             system.....35  
 start-time statement  
     system log file archiving.....82  
     system logging  
         usage guidelines.....40  
 structured-data statement.....93  
     usage guidelines.....32  
 support, technical See technical support  
 syntax conventions.....xi  
 syslog statement  
     system processes.....94  
     usage guidelines.....28  
 system logging  
     Common Criteria.....5  
     different on each node in routing matrix.....56  
     disabling.....48  
     examples.....67  
     facilities  
         alternate for remote machine.....38  
         default for remote machine.....38  
         mapping of codes to names.....43  
     files, archiving.....40  
     forwarding messages in TX Matrix router.....53  
     Junos-FIPS.....5  
     message descriptions  
         displaying.....12  
         fields in.....12  
     messages, displaying  
         generated by Junos process.....18  
         generated by service on PIC.....19  
         structured-data format.....14

regular expression filtering.....45  
 regular expression operators.....47  
 severity levels.....44  
 single-chassis system.....5  
 timestamp, modifying.....45  
 system statement.....92  
     usage guidelines.....73

## T

technical support  
     contacting JTAC.....xiii  
 time-format statement.....96  
     usage guidelines.....45  
 trace files  
     display of  
         starting.....107  
         stopping.....111  
     status, displaying.....106  
 tracing.....97  
     destination-override.....97  
 transfer-interval statement  
     system log file archiving.....82  
     system logging  
         usage guidelines.....40

## U

user (system logging facility)  
     option to facility-override statement.....39  
 user statement  
     system logging.....98  
     usage guidelines.....33  
 users  
     logs, displaying.....109

## W

warning (system logging severity level 4).....44  
 world-readable statement  
     archiving of all system log files.....81  
     archiving of individual system log file.....82  
     system logging.....99  
     usage guidelines.....40

