

Chapter 24

Configuring System Log Messages

The JUNOS software generates system log messages (also called syslog messages) to record events that occur on the routing platform, 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 child or peer process

- Emergency or critical conditions, such as routing platform power-down due to excessive temperature

Each system log message identifies the JUNOS software process that generated the message and briefly describes the operation or error that occurred. This manual provides more detailed information about each system log message and, when applicable, describes possible causes of the message and action you can take to correct error conditions.

This chapter discusses the following topics:

- System Logging Configuration Statements on page 402

- Minimum System Logging Configuration on page 403

- Configuring System Logging for a Single-Chassis System on page 403

- Configuring System Logging for a Routing Matrix on page 418

System Logging Configuration Statements

To configure the routing platform 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;
    explicit-priority;
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
  }
  source-address source-address;
  time-format (year | millisecond | year millisecond);
  user (username | *) {
    facility severity;
  }
}
```

Minimum System Logging Configuration

For the JUNOS software processes to generate system log messages, you must include the `syslog` statement at the `[edit system]` hierarchy level. Specify at least one destination for system log messages, as described in Table 17. For more information about the configuration statements, see “Configuring System Logging for a Single-Chassis System” on page 403.

Table 17: Minimum Configuration Statements for System Logging

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

Configuring System Logging for a Single-Chassis System

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 software. For information about configuring system logging for a routing matrix, see “Configuring System Logging for a Routing Matrix” on page 418.

When you configure system logging, you can 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 Messages to a Log File” on page 406.

To the terminal session of one or more specific users (or all users) when they are logged in to the routing platform, by including the `user` statement. See “Directing Messages to a User Terminal” on page 406.

To the routing platform console, by including the `console` statement. See “Directing Messages to the Console” on page 407.

To a remote machine that is running the `syslogd` utility or to the other Routing Engine on the routing platform, by including the `host` statement. See “Directing Messages to a Remote Machine or the Other Routing Engine” on page 407.

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). To log the messages belonging to one or more facilities to a particular destination, specify each facility name as a separate statement within the set of statements for the destination. Table 18 lists the JUNOS system logging facilities that you can specify in the configuration statements at the [edit system syslog] hierarchy level:

Table 18: JUNOS System Logging Facilities

Facility	Type of Event or Error
any	All (messages from all facilities)
authorization	Authentication and authorization attempts
change-log	Changes to the JUNOS configuration
conflict-log	Configuration that is inconsistent with routing platform hardware
daemon	Actions performed or errors encountered by various system processes
firewall	Packet filtering actions performed by a firewall filter
ftp	Actions performed or errors encountered by the FTP process
interactive-commands	Commands issued at the JUNOS command-line interface (CLI) prompt or by a JUNOScript client application
kernel	Actions performed or errors encountered by the JUNOS kernel
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
user	Actions performed or errors encountered by various user-space processes

Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects routing 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.

Unlike the other severity levels, the none level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see “Disabling Logging of a Facility” on page 415.

Table 19 lists the severity levels that you can specify in configuration statements at the [edit system syslog] hierarchy level. The levels from emergency through info are in order from highest severity (greatest effect on functioning) to lowest.

Table 19: System Log Message Severity Levels

Severity Level	Description
any	Includes all severity levels
none	Disables logging of the associated facility to a destination
emergency	System panic or other condition that causes the routing platform to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database
critical	Critical conditions, such as hard drive errors
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or nonerror conditions of interest

A message's facility and severity level are together referred to as its *priority*. By default, the system logging utility does not include priority information in system log messages. To include priority information in messages directed to a file, or to a remote machine or the other Routing Engine, include the explicit-priority statement. For more information, see "Including Priority in System Log Messages" on page 412.

You can modify the timestamp on system log messages to include the year, the millisecond, or both. For more information, see "Including the Year or Millisecond in Timestamps" on page 415.

When directing messages to a remote machine, you can specify the source address to use, and you can configure features that make it easier to separate JUNOS-specific messages or messages generated on particular routing platforms. For more information, see "Directing Messages to a Remote Machine or the Other Routing Engine" on page 407.

For more information about configuring system logging, see the following sections:

Directing Messages to a Log File on page 406

Directing Messages to a User Terminal on page 406

Directing Messages to the Console on page 407

Directing Messages to a Remote Machine or the Other Routing Engine on page 407

Configuring Log File Archiving on page 411

Including Priority in System Log Messages on page 412

Including the Year or Millisecond in Timestamps on page 415

Disabling Logging of a Facility on page 415

Examples: Configuring System Logging on page 416

Directing Messages to a Log File

To direct system log messages to a file on the local disk of the local Routing Engine, include the file statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
file filename {
  facility severity;
  explicit-priority;
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
}
```

The default directory for log files is /var/log; to specify a different directory on the local Routing Engine's local disk, include the complete pathname. For the list of logging facilities and severity levels, see Table 18 on page 404 and Table 19 on page 405.

To prevent log files from growing too large, the JUNOS system logging utility by default writes messages to a sequence of files of a defined size. You can configure the number of files, their maximum size, and who can read them, for either all log files or a certain log file. For more information, see "Configuring Log File Archiving" on page 411.

For information about the explicit-priority statement, see "Including Priority in System Log Messages" on page 412.

Directing 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;
}
```

Specify one or more JUNOS 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 Table 18 on page 404 and Table 19 on page 405.

Directing 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 Table 18 on page 404 and Table 19 on page 405.

Directing 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 routing platform, 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;
}
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 address or fully qualified hostname. The remote machine must be running the standard `syslogd` utility. We do not recommend directing messages to another routing platform. 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 routing platform with two Routing Engines installed and operational, include the host `other-routing-engine` statement. Include the statement in each Routing Engine's configuration if you want them both to direct messages to the other Routing Engine. In each system log message directed to the other Routing Engine, the string `re0` or `re1` appears after the timestamp to indicate that the local Routing Engine is the source for the message.

For the list of logging facilities and severity levels to configure under the host statement, see Table 18 on page 404 and Table 19 on page 405.

To record facility and severity level information in each message, include the `explicit-priority` statement. For more information, see "Including Priority in System Log Messages" on page 412.

When directing messages to remote machines, you can use the `source-address` statement to specify the source address to use. In each host statement, you can also include the `facility-override` statement to assign an alternate facility and the `log-prefix` statement to add a string to each message. For more information, see the following sections:

Specifying an Alternate Source Address on page 408

Changing the Alternate Facility for Remote Messages on page 408

Adding a String to System Log Messages on page 410

Specifying an Alternate Source Address

To specify the source address to use when directing system log messages 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 IP address configured on one of the routing platform interfaces. The address is used only for messages directed to the remote machines specified in all the host `hostname` statements at the `[edit system syslog]` hierarchy level, not for messages directed to the other Routing Engine.

Changing the Alternate Facility for Remote Messages

Some of the facilities for messages logged on a Juniper Networks routing platform (listed in Table 18 on page 404) are JUNOS-specific. Because the remote machine designated at the `[edit system syslog host hostname]` hierarchy level is a regular computer instead of another Juniper Networks routing platform, its `syslogd` utility cannot interpret the JUNOS-specific facilities. When messages are directed to a remote machine, an alternate facility—one that is certain to be available to the standard `syslogd` utility—is used for each JUNOS-specific facility.

Table 20 lists the alternate facility used by default for each JUNOS-specific facility. For facilities that are not listed, the alternate facility is the same as the facility used for local logging.

Table 20: Default Facilities for Messages Directed to a Remote Machine

JUNOS-Specific Local Facility	Facility when Directed to Remote Machine
change-log	local6
conflict-log	local5
firewall	local3
interactive-commands	local7
pfe	local4

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 routing platform or the remote machine itself). For example, you can include the following statements on the routing platform called local-router to direct messages from the authorization facility to a remote machine called monitor.mycompany.com:

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

The default alternate facility for the local authorization facility is also authorization. The logging utility on monitor is configured to write messages belonging to the authorization facility to the file `/var/log/auth-attempts`, so that file contains both 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 change the facility used for 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 alternate 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 assigned to the alternate facility in the desired manner.

Table 21 lists the facilities that you can specify in the facility-override statement.

Table 21: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts
daemon	Actions performed or errors encountered by various system processes
ftp	Actions performed or errors encountered by the FTP process
kernel	Actions performed or errors encountered by the JUNOS 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
local6	Local facility number 6
local7	Local facility number 7
user	Actions performed or errors encountered by various 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 alternate facilities when directing messages to the other Routing Engine, because it runs the JUNOS system logging utility and can interpret the JUNOS-specific facilities.

Examples: Assigning an Alternate 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 direct messages to a single remote machine called central-logger.mycompany.com. The messages from California are aggregated into one facility (local1) and the messages from New York into another facility (local2).

Configure California routing platforms to aggregate messages in the local1 facility:

```
[edit system syslog]
host central-logger.mycompany.com {
  change-log info;
  facility-override local1;
}
```

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 local1 facility to /var/log/california-config and the messages from the local2 facility to /var/log/new-york-config.

Adding a 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 character other than a space, the equal sign (=), or the colon (:). A colon and a space are appended to the string when the system log messages are written to the log. The string is inserted after the hostname of the Routing Engine that generated the message.

Example: Adding a String

Add the string M40e to all messages to indicate that the router is an M40e 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 M40e;
}
```

When these configuration statements are included on an M40e router called origin1, a message in the system logging file on hardware-logger looks like the following:

```
Mar 9 17:33:23 origin1 M40e: mgd[477]: UI_CMDLINE_READ_LINE: user 'root',
command 'run show version'
```

Configuring Log File Archiving

By default, the JUNOS logging utility writes 128 kilobytes (KB) of messages to a log file *logfile*. At that point, *logfile* is closed, compressed, and renamed to *logfile.0.gz*. The logging utility then opens and writes to a new file called *logfile*. When the new file reaches 128 KB in size, *logfile.0.gz* is renamed to *logfile.1.gz* and the new file is closed, compressed, and renamed *logfile.0.gz*. By default, the logging utility creates up to 10 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). The logging utility by default also limits the users who can read log files to the root user and users who have the JUNOS maintenance permission.

You can include the archive statement in the configuration to change the maximum size of each file, how many archive files are created, and who can read log files. To configure different values that apply to all log files, include the archive statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
archive {
  files number;
  size size;
  (world-readable | no-world-readable);
}
```

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

```
[edit system syslog file filename]
facility severity;
archive {
  files number;
  size size;
  (world-readable | no-world-readable);
}
```

The number of files specified with the files statement can range from 1 through 1000. The maximum file size specified with the size statement can range from 64 KB (64k) through 1 gigabyte (1g); to represent megabytes, use the letter m after the integer. To enable all users to read log files, include the world-readable statement. To restore the default permissions, include the no-world-readable statement.

Including Priority in System Log Messages

A message's facility and severity level are together referred to as its *priority*. By default, the system logging utility does not include information about priority in system log messages.

To include the priority in 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;
```

To include the priority 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;
```

When the explicit-priority statement is included, the message string includes the facility name and a numerical code representing the severity level. The name and number appear directly before the message code.

The message string always reports the original, local facility. If a message belongs to a JUNOS-specific facility, the JUNOS system logging utility still uses an alternate facility for the message itself when directing messages to a remote machine. For more information, see "Changing the Alternate Facility for Remote Messages" on page 408.

Table 22 lists the facility codes that can appear in system log messages and maps them to facility names.



NOTE: If Table 22 does not provide the facility name for a code, you cannot include the facility in a statement at the [edit system syslog] hierarchy level. The JUNOS software might use these facilities—and others that are not listed—when reporting on internal operations.

Table 22: Mapping of Facility Codes to Names

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	Configuration that is inconsistent with routing platform hardware
CONSOLE		Messages written to /dev/console by the kernel console output driver
CRON		Actions performed or errors encountered by the cron process
DAEMON	daemon	Actions performed or errors encountered by various system processes
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 CLI prompt or by a JUNOScript client application
KERN	kernel	Actions performed or errors encountered by the JUNOS kernel
NTP		Actions performed or errors encountered by the Network Time Protocol process (ntpd)
PFE	pfe	Actions performed or errors encountered by the Packet Forwarding Engine
SYSLOG		Actions performed or errors encountered by the JUNOS system logging utility
USER	user	Actions performed or errors encountered by various user-space processes

Table 23 lists the numerical severity codes that can appear in system log messages and maps them to severity levels.

Table 23: Mapping of Numerical Codes to Severity Levels

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

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, which has the following format:

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

Including the Year or Millisecond in Timestamps

By default, the timestamp recorded in a 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);
```

The modified timestamp is used for 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 (2003):

```
Aug 21 12:36:30.401 2003
```

Disabling Logging of a Facility

To disable logging of the messages from a 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 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;
}
```

Examples: Configuring System Logging

Log messages about all commands entered by users at the CLI prompt or by JUNOScript 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;
  }
}
```

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" or above to the system console */
  console {
    any error;
  }
}
```

Log all changes in the state of alarms to the file `/var/log/alarms`:

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

Configure the handling of messages generated when users issue JUNOS 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;
  }
}
```

Configuring System Logging for a Routing Matrix

This section explains how to configure system logging for the T640 Internet routing nodes and TX Matrix platform in a routing matrix. It assumes you are familiar with system logging for single-chassis systems, as described in “Configuring System Logging for a Single-Chassis System” on page 403. For more information about routing matrixes, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742 and *TX Matrix Platform Hardware Guide*.

To configure system logging for all platforms in a routing matrix, include the `syslog` statement at the `[edit system]` hierarchy level on the TX Matrix platform. The `syslog` statement applies to every platform in the routing matrix.

```
[edit system]
syslog {
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
  console {
    facility severity;
  }
  file filename {
    facility severity;
    explicit-priority;
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
  }
  source-address source-address;
  time-format (year | millisecond | year millisecond);
  user (username | *) {
    facility severity;
  }
}
```

The following configuration statements have the same effect for a routing matrix as for a single-chassis system, except that they apply to every platform in the routing matrix:

`archive`—Configures the archiving of log files on each platform in the routing matrix. See “Configuring Log File Archiving” on page 411.

`console`—Directs the specified messages to the console of each platform in the routing matrix. See “Directing Messages to the Console” on page 407.

`file`—Directs the specified messages to a file of the same name on each platform in the routing matrix. See “Directing Messages to a Log File” on page 406.

`source-address`—Sets the source address used for messages directed to the remote machines specified in all the `host hostname` statements at the [edit system syslog] hierarchy level for each platform in the routing matrix. The address is not used for messages directed to the other Routing Engine on each platform or to the TX Matrix platform from the T640 routing nodes. See “Specifying an Alternate Source Address” on page 408.

`time-format`—Adds the millisecond, year, or both to the timestamp in each message. See “Including the Year or Millisecond in Timestamps” on page 415.

`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 Messages to a User Terminal” on page 406.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system. For more information, see the following sections:

Configuring Message Forwarding in the Routing Matrix on page 419

Configuring Optional Features for Forwarded Messages on page 422

Directing Messages to a Remote Destination from the Routing Matrix on page 423

Configuring System Logging Differently on Each Platform on page 425

Configuring Message Forwarding in the Routing Matrix

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

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

The setting applies to all T640 routing nodes in the routing matrix.

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

For the TX Matrix platform to record the messages forwarded by the T640 routing nodes (as well as messages generated on the TX Matrix platform itself), you must also configure system logging on the TX Matrix platform. Direct the messages to one or more destinations by including the appropriate statements at the [edit system syslog] hierarchy level on the TX Matrix platform:

To a file, as described in “Directing Messages to a Log File” on page 406.

To the terminal session of one or more specific users (or all users), as described in “Directing Messages to a User Terminal” on page 406.

To the console, as described in “Directing Messages to the Console” on page 407.

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” on page 423.

As previously noted, the configuration statements included on the TX Matrix platform also configure the same destinations on each T640 routing node.

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.)

Messages Logged when Local and Forwarded Severity Level Is the Same on page 420

Messages Logged when Local Severity Level Is Lower on page 421

Messages Logged when Local Severity Level Is Higher on page 421

Messages Logged when Local and Forwarded Severity Level Is the Same

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

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

Table 24 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform.

Table 24: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T640 routing node	Local	info
TX Matrix platform	Local	info
	Forwarded from T640 routing nodes	info

Messages Logged when Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix platform 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, 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 25 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform. The T640 routing nodes forward only those messages with severity critical and higher, so the log on the TX Matrix platform does not include the messages with severity error, warning, or notice that the T640 routing nodes log locally.

Table 25: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T640 routing node	Local	notice
TX Matrix platform	Local	notice
	Forwarded from T640 routing nodes	critical

Messages Logged when Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix platform 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 26 specifies which messages are included in the logs on the T640 routing nodes and the TX Matrix platform. Although the T640 routing nodes forward messages with severity notice and higher, the TX Matrix platform discards any of those messages with severity critical or lower (does not log forwarded messages with severity error, warning, or notice). None of the logs include messages with severity error or lower.

Table 26: Example: Local Severity critical, Forwarded Severity is notice

Log Location	Source of Messages	Lowest Severity Included
T640 routing node	Local	critical
TX Matrix platform	Local	critical
	Forwarded from T640 routing nodes	critical

Configuring Optional Features for Forwarded Messages

You can configure additional optional features when specifying how the T640 routing nodes forward messages to the TX Matrix platform. To insert a string in each forwarded message, include the log-prefix statement 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.

```
[edit system syslog host scc-master]
  facility severity;
  explicit-priority;
  log-prefix string;
}
```



NOTE: 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 alternate facilities for messages forwarded to the TX Matrix platform, because it runs the JUNOS system logging utility and can interpret the JUNOS-specific facilities. For more information about alternate facilities, see “Changing the Alternate Facility for Remote Messages” on page 408.

The string that you define with the `log-prefix` statement appears in every message forwarded to the TX Matrix platform. For more information, see “Adding a String to System Log Messages” on page 410.

When you include the `explicit-priority` statement, the messages forwarded to the TX Matrix platform include priority information. For the information to appear in a log file on the TX Matrix platform, you must also include the `explicit-priority` statement at the [edit system syslog file *filename*] hierarchy level. The log file on each platform in the routing matrix also includes priority information for locally generated messages as a consequence.

To include priority information in messages directed to a remote machine from the routing matrix, also include the `explicit-priority` statement at the [edit system syslog host *hostname*] hierarchy level. For more information, see “Directing Messages to a Remote Destination from the Routing Matrix” on page 423.

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

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

Directing Messages to a Remote Destination from the Routing Matrix

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

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

The TX Matrix platform directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional configuration statements (`facility-override`, `log-prefix`, `explicit-priority`, and `source-address`) also have the same effect as on a single-chassis system. For more information, see “Directing Messages to a Remote Machine or the Other Routing Engine” on page 407.

For the TX Matrix platform to include priority information when it directs messages that originated on a T640 routing node 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 routing nodes to the TX Matrix platform. 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 routing node 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 platform.

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

If the T640 routing nodes are configured to forward messages to the TX Matrix platform (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T640 routing node and the other from the TX Matrix platform. 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 in the Routing Matrix” on page 419.

If the `source-address` statement is configured at the `[edit system syslog]` hierarchy level, all platforms in the routing matrix use the same source address for messages directed to the remote machine. This is appropriate, as the routing matrix is intended to function as a single routing platform.

If the `log-prefix` statement is included, the messages from all platforms in the routing matrix include the same string. You cannot use the string to distinguish between the platforms in the routing matrix.

Configuring System Logging Differently on Each Platform

We recommend that all platforms in a routing matrix use the same configuration, which implies that you include system logging configuration statements on the TX Matrix platform only. In rare circumstances, however, you might choose to log different messages on different platforms. For example, if one platform in the routing matrix is experiencing problems, a Juniper Networks support representative might instruct you to log messages with severity debug on that one platform.

To configure platforms separately, include system logging configuration statements in the appropriate groups at the [edit groups] hierarchy level on the TX Matrix platform:

To configure settings that apply to the TX Matrix platform but not the T640 routing nodes, include them in the re0 and re1 configuration groups.

To configure settings that apply to particular T640 routing nodes, include them in the lccn-re0 and lccn-re1 configuration groups.

When you use configuration groups, do not issue CLI configuration mode commands on the TX Matrix platform that affect the [edit system syslog] hierarchy level. The resulting statements overwrite the statements defined in configuration groups and apply to the T640 routing nodes also. (We further recommend that you do not issue CLI configuration mode commands on the T640 routing nodes at any time.)

For more information about the configuration groups for a routing matrix, see “Creating a Configuration Group” on page 538.

The following sample statements configure the /var/log/messages files on three platforms to include different sets of messages:

On the TX Matrix platform, local messages with severity info and higher from all facilities. The file does not include messages from the T640 routing nodes, because the host scc-master statement disables message forwarding.

On the T640 routing node designated LCC0 (line-card chassis 0), messages with severity debug from all facilities.

On the T640 routing node 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 {
        any debug;
      }
    }
  }
}
lcc0-re1 {
  ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
  system {
    syslog {
      file messages {
        any notice;
      }
    }
  }
}
lcc0-re1 {
  ... same statements as for lcc1-re0 ...
}
}
```