

## Chapter 27

# Summary of System Management Configuration Statements

The following sections explain each of the system management configuration statements. The statements are organized alphabetically.

## accounting

---

<b>Syntax</b>	<pre>accounting {   events [ login change-log interactive-commands ];   destination {     tacplus {       server {         server-address {           port <i>port-number</i>;           secret <i>password</i>;           single-connection;           timeout <i>seconds</i>;         }       }     }   } }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure audit of TACACS+ authentication events, configuration changes, and interactive commands.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring TACACS+ System Accounting” on page 438.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## allow-commands

---

<b>Syntax</b>	allow-commands " <i>regular-expression</i> ";
<b>Hierarchy Level</b>	[edit system login class <i>class-name</i> ]
<b>Description</b>	Specify the operational mode commands that members of a login class can use.
<b>Default</b>	If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
<b>Options</b>	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
<b>Usage Guidelines</b>	See “Specifying Operational Mode Commands” on page 379.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	deny-commands on page 486, user on page 529

## allow-configuration

---

<b>Syntax</b>	allow-configuration " <i>regular-expression</i> ";
<b>Hierarchy Level</b>	[edit system login class <i>class-name</i> ]
<b>Description</b>	Specify the configuration mode commands that members of a login class can use.
<b>Default</b>	If you omit this statement and the deny-configuration statement, users can issue only those commands for which they have access privileges through the permissions statement.
<b>Options</b>	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
<b>Usage Guidelines</b>	See “Specifying Operational Mode Commands” on page 379.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	deny-commands on page 486, user on page 529

## archival

---

**Syntax** archival {  
     configuration {  
         transfer-interval *interval*;  
         transfer-on-commit;  
         archive-sites {  
             ftp://<username>:<password>@<host>:<port>/<url-path>;  
         }  
     }  
 }

**Hierarchy Level** [edit system]

**Description** Configure copying of the currently active configuration to an archive site.  
 The remaining statements are described separately.

**Usage Guidelines** See “Configuring a Router to Transfer its Configuration to an Archive Site” on page 436.

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

## archive

---

**Syntax** archive {  
     files *number*;  
     size *size*;  
     (world-readable | no-world-readable);  
 }

**Hierarchy Level** [edit system syslog],  
 [edit system syslog file *filename*]

**Description** Configure how to archive system log files.  
 The remaining statements are described separately.

**Usage Guidelines** See “Configuring System Log Messages” on page 401.

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

## archive-sites

---

<b>Syntax</b>	archive-sites { ftp://username@host:<port>url-path password password; }
<b>Hierarchy Level</b>	[edit system archival configuration]
<b>Description</b>	Specifies where to transfer the current configuration files. If you specify more than one archive site, the router attempts to transfer to the first archive site in the list, moving to the next only if the transfer fails. The format for the destination file name is < router-name> _juniper.conf[.gz]_YYYYMMDD_HHMMSS.
<b>Usage Guidelines</b>	See “Configuring Archive Sites” on page 437.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	transfer-on-commit on page 528, transfer-on-commit on page 528, and configuration on page 483.

## authentication

---

<b>Syntax</b>	authentication { (encrypted-password "password"   plain-text-password); ssh-rsa "public-key"; ssh-dsa "public-key"; }
<b>Hierarchy Level</b>	[edit system login user username]
<b>Description</b>	Authentication methods that a user can use to log in to the router. You can assign multiple authentication methods to a single user.
<b>Options</b>	encrypted-password "password"—Use Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.  plain-text-password—Use a plain-text password. The command-line interface (CLI) prompts you for the password and then encrypts it. For information about how to create plain-text passwords, see “Specifying Plain-Text Passwords” on page 17.  ssh-rsa "public-key"—Secure shell (SSH version 1) authentication. Specify the SSH public key. You can specify one or more public keys for each user.  ssh-dsa "public-key"—Secure shell (SSH version 2) authentication. Specify the SSH public key. You can specify one or more public keys for each user.
<b>Usage Guidelines</b>	See “Configuring User Accounts” on page 387.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

**See Also** root-authentication on page 512

## authentication-key

---

**Syntax** authentication-key *key-number* *type* *type* *value* *password*;

**Hierarchy Level** [edit system ntp]

**Description** Configure Network Time Protocol (NTP) authentication keys so that the router can send authenticated packets. If you configure the router to operate in authenticated mode, you must configure a key.

Both the keys and the authentication schemes (DES or MD5) must be identical between a set of peers sharing the same key number.

**Options** *key-number*—Positive integer that identifies the key.

*type type*—Authentication type. It can be either md5 or des.

*value password*—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.

**Usage Guidelines** See “Configuring NTP Authentication Keys” on page 399.

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

**See Also** broadcast on page 480, peer on page 505, server on page 515, trusted-key on page 529

## authentication-order

---

<b>Syntax</b>	authentication-order [ <i>authentication-methods</i> ];
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.
<b>Default</b>	If you do not include the authentication-order statement, users are verified based on their configured passwords.
<b>Options</b>	<p><i>authentication-methods</i>—One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following:</p> <p>password—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.</p> <p>radius—Verify the user using RADIUS authentication services.</p> <p>tacplus—Verify the user using TACACS+ authentication services.</p>
<b>Usage Guidelines</b>	See “Configuring the Authentication Order” on page 369.
<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>

## auxiliary

---

<b>Syntax</b>	<pre>auxiliary {     type <i>terminal-type</i>; }</pre>
<b>Hierarchy Level</b>	[edit system ports]
<b>Description</b>	Configure the characteristics of the auxiliary port, which is on the router's craft interface.
<b>Default</b>	The auxiliary port is disabled.
<b>Options</b>	<p><i>type terminal-type</i>—Type of terminal that is connected to the port.</p> <p><b>Values:</b> ansi, vt100, small-xterm, xterm</p> <p><b>Default:</b> The terminal type is unknown, and the user is prompted for the terminal type.</p>
<b>Usage Guidelines</b>	See “Configuring Console and Auxiliary Port Properties” on page 428.
<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>

## autoinstallation

---

**Syntax**

```

autoinstallation {
  interfaces {
    interface-name {
      bootp;
      rarp;
      slarp;
    }
  }
  configuration-servers {
    url;
  }
}

```

**Hierarchy Level** [edit system]

**Description** For J-series Services Routers only, enables you to download a configuration file automatically from an FTP, Hypertext Transfer Protocol (HTTP), or Trivial FTP (TFTP) server. When you power on a J-series Services Router configured for autoinstallation, it requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server. Once the Router has an address, it sends a request to a configuration server and downloads and installs a configuration.

The remaining statements are explained separately in this chapter.

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

**See Also** configuration-servers on page 483, idle-timeout on page 496

## backup-router

---

**Syntax** backup-router *address* <destination *destination-address*>;

**Hierarchy Level** [edit system]

**Description** Set a default router (running IP version 4 [IPv4]) to use while the local router (running IPv4) is booting and if the routing protocol processes fail to start. The JUNOS software removes the route to this router as soon as the software starts.

**Options** *address*—Address of the default router.

*destination destination-address*—(Optional) Destination address that is reachable through the backup router. Include this option to achieve network reachability while loading, configuring, and recovering the router, but without the risk of installing a default route in the forwarding table.

**Default:** All hosts (default route) are reachable through the backup router.

**Usage Guidelines** See “Configuring a Backup Router” on page 352.

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

## boot-server

---

<b>Syntax</b>	<code>boot-server address;</code>
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	<p>Configure the server that NTP queries when the router boots to determine the local date and time.</p> <p>When you boot the router, it issues an <code>ntpdate</code> request, which polls a network server to determine the local date and time. You need to configure a server that the router uses to determine the time when the router boots. Otherwise, NTP will not be able to synchronize to a time server if the server's time appears to be very far off of the local router's time.</p>
<b>Options</b>	<code>address</code> —Address of an NTP server. You must specify an address, not a hostname.
<b>Usage Guidelines</b>	See “Configuring the NTP Boot Server” on page 394.
<b>Required Privilege Level</b>	<p><code>system</code>—To view this statement in the configuration.</p> <p><code>system-control</code>—To add this statement to the configuration.</p>

## broadcast

---

<b>Syntax</b>	<code>broadcast address &lt;key key-number&gt; &lt;version value&gt; &lt;ttl value&gt;;</code>
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	<p>Configure the local router to operate in broadcast mode with the remote system at the specified <code>address</code>. In this mode, the local router sends periodic broadcast messages to a client population at the specified broadcast or multicast <code>address</code>. Normally, you include this statement only when the local router is operating as a transmitter.</p>
<b>Options</b>	<p><code>address</code>—Address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. Currently, the multicast address must be 224.0.1.1.</p> <p><code>key key-number</code>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.  <b>Values:</b> Any unsigned 32-bit integer</p> <p><code>ttl value</code>—(Optional) Time-to-live (TTL) value to use.  <b>Range:</b> 1 through 255  <b>Default:</b> 1</p> <p><code>version value</code>—(Optional) Specify the version number to be used in outgoing NTP packets.  <b>Values:</b> 1, 2, 3  <b>Default:</b> 3</p>

**Usage Guidelines** See “Configuring the NTP Time Server and Time Services” on page 395.

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

## broadcast-client

---

**Syntax** broadcast-client;

**Hierarchy Level** [edit system ntp]

**Description** Configure the local router to listen for broadcast messages on the local network to discover other servers on the same subnet.

**Usage Guidelines** See “Configuring the Router to Listen for Broadcast Messages” on page 399.

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

## class

---

See the following sections:

class (Assign a Class to an Individual User) on page 481

class (Define Login Classes) on page 482

### ***class (Assign a Class to an Individual User)***

**Syntax** class *class-name*;

**Hierarchy Level** [edit system login user *username*]

**Description** Configure a user’s login class. You must configure one class for each user.

**Options** *class-name*—One of the classes defined at the [edit system login class] hierarchy level.

**Usage Guidelines** See “Configuring User Accounts” on page 387.


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

**class (Define Login Classes)**

<b>Syntax</b>	<pre>class <i>class-name</i> {     allow-commands "<i>regular-expression</i>";     allow-configuration "<i>regular-expression</i>";     deny-commands "<i>regular-expression</i>";     deny-configuration "<i>regular-expression</i>";     idle-timeout <i>minutes</i>;     no-tip;     permissions [ <i>permissions</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit system login]
<b>Description</b>	Define login classes.
<b>Options</b>	<p><i>class-name</i>—A name you choose for the login class.</p> <p>The remaining statements are explained separately in this chapter.</p>
<b>Usage Guidelines</b>	See “Defining Login Classes” on page 375.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>See Also</b>	user on page 529

**compress-configuration-files**


---

<b>Syntax</b>	compress-configuration-files;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Compress the current operational configuration file. By default, the current operational configuration file is uncompressed, and is stored in the file juniper.conf, in the /config file system, along with the last three committed versions of the configuration. However, with large networks, the current configuration file might exceed the available space in the /config file system. Compressing the current configuration file allows the file to fit in the file system, typically reducing the size of the file by 90 percent. The current configuration file is compressed on the second commit of the configuration after the first commit is made to include the compress-configuration-files statement.
	<b>NOTE:</b> Juniper Networks recommends that you enable compression of the router configuration files to minimize the amount of disk space that they require.
<b>Default</b>	The current operational configuration file is uncompressed.
<b>Usage Guidelines</b>	See “Compressing the Current Configuration File” on page 357.
<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>

## configuration

---

<b>Syntax</b>	<pre>configuration {   transfer-interval <i>interval</i>;   transfer-on-commit;   archive-sites {     ftp://&lt;username&gt;:&lt;password&gt;@&lt;host&gt;:&lt;port&gt;/&lt;url-path&gt;;   } }</pre>
<b>Hierarchy Level</b>	[edit system archival]
<b>Description</b>	Configure the router to transfer its currently active configuration by means of FTP periodically or after each commit. The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring a Router to Transfer its Configuration to an Archive Site” on page 436.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	transfer-interval on page 528, transfer-on-commit on page 528, and archive on page 475.

## configuration-servers

---

<b>Syntax</b>	<pre>configuration-servers {   <i>url</i>; } }</pre>
<b>Hierarchy Level</b>	[edit system autoinstallation]
<b>Description</b>	For J-series Services Routers only, configure the URL address of a server from which to obtain configuration files. <b>Example URLs:</b> tftp://tftpconfig.sp.com/config.conf; ftp://user:password@sftpconfig.sp.com/path/file-name
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	autoinstallation on page 479, idle-timeout on page 496.

## connection-limit

---

<b>Syntax</b>	connection-limit <i>limit</i> ;
<b>Hierarchy Level</b>	[edit system services finger], [edit system services ssh], [edit system services telnet], [edit system services xnm-clear-text], [edit system services xnm-ssl]
<b>Options</b>	<i>limit</i> —(Optional) Maximum number of established connections. <b>Range:</b> 1 through 250 <b>Default:</b> 75
<b>Usage Guidelines</b>	See “Configuring System Services” on page 430.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## console

---

See the following sections:

console (Physical Port) on page 484

console (System Logging) on page 485

### *console (Physical Port)*

<b>Syntax</b>	console { insecure; log-out-on-disconnect; type <i>terminal-type</i> ; }
<b>Hierarchy Level</b>	[edit system ports]
<b>Description</b>	Configure the characteristics of the console port, which is on the router’s craft interface.
<b>Default</b>	The console port is enabled and its speed is 9600 baud.
<b>Options</b>	<b>insecure</b> —Disable root login connections to the console and auxiliary ports.  <b>log-out-on-disconnect</b> —Logs out the session when the data carrier on the console port is lost.  <b>type <i>terminal-type</i></b> —Type of terminal that is connected to the port. <b>Values:</b> ansi, vt100, small-xterm, xterm <b>Default:</b> The terminal type is unknown, and the user is prompted for the terminal type.

**Usage Guidelines** See “Configuring Console and Auxiliary Port Properties” on page 428.

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

### ***console (System Logging)***

**Syntax** console {  
    *facility level*;  
}

**Hierarchy Level** [edit system syslog]

**Description** Configure the types of messages to log to the system console.

**Options** *facility*—Class of messages to log. To specify multiple classes, include multiple *facility level* statements. For a list of the facilities, see Table 18 on page 404.

*level*—Severity of the messages that belong to the facility specified by the paired *facility* name. For a list of the severities, see Table 19 on page 405.

**Usage Guidelines** See “Configuring System Log Messages” on page 401.

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

**See Also** *JUNOS System Log Messages Reference*

### **default-address-selection**

---

**Syntax** default-address-selection;

**Hierarchy Level** [edit system]

**Description** Use the loopback interface, lo0, as the source address for all locally generated IP packets. The lo0 interface is the interface to the router’s Routing Engine.

**Default** The outgoing interface is used as the source address.

**Usage Guidelines** See “Configuring the Source Address for Locally Generated TCP/IP Packets” on page 429 and the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

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

deny-commands

---

<b>Syntax</b>	deny-commands " <i>regular-expression</i> ";
<b>Hierarchy Level</b>	[edit system login class]
<b>Description</b>	Specify the operational mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.
<b>Default</b>	If you omit this statement and the allow-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
<b>Options</b>	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
<b>Usage Guidelines</b>	See “Specifying Operational Mode Commands” on page 379.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	allow-commands on page 474, user on page 529

deny-configuration

---

<b>Syntax</b>	deny-configuration " <i>regular-expression</i> ";
<b>Hierarchy Level</b>	[edit system login class]
<b>Description</b>	Specify the configuration mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.
<b>Default</b>	If you omit this statement and the allow-configuration statement, users can issue only those commands for which they have access privileges through the permissions statement.
<b>Options</b>	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
<b>Usage Guidelines</b>	See “Specifying Operational Mode Commands” on page 379.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	allow-configuration on page 474, user on page 529

## destination

---

**Syntax** destination {  
     tacplus {  
         server {  
             server-address {  
                 secret *password*;  
                 single-connection;  
                 timeout *seconds*;  
                 port *port-number*;  
             }  
         }  
     }  
 }

**Hierarchy Level** [edit system accounting]

**Description** Configure the authentication server.

**Options** The remaining statements are explained separately.

**Usage Guidelines** See “Configuring TACACS+ System Accounting” on page 438.

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

## diag-port-authentication

---

**Syntax** diag-port-authentication (encrypted-password “*password*” | plain-text-password);

**Hierarchy Level** [edit system]

**Description** Configure a password for performing diagnostics on the router’s System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), or Forwarding Engine Board (FEB) port.

For routers that have more than one SSB, the same password is used for both SSBs.



**NOTE:** Do not run diagnostics on the SCB, SSB, SFM, or FEB unless you have been instructed to do so by Customer Support personnel.

---

**Default** No password is configured on the diagnostics port.

**Options** encrypted-password “*password*”—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password for each user. For information about how to create plain-text passwords, see “Specifying Plain-Text Passwords” on page 17.

**Usage Guidelines** See “Configuring the Password on the Diagnostics Port” on page 435.

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

## domain-name

---

**Syntax** domain-name *domain-name*;

**Hierarchy Level** [edit system]

**Description** Configure the name of the domain in which the router is located. This is the default domain name that is appended to hostnames that are not fully qualified.

**Options** *domain-name*—Name of the domain.

**Usage Guidelines** See “Configuring the Router’s Domain Name” on page 350.

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

## domain-search

---

**Syntax** domain-search [*domain-list*];

**Hierarchy Level** [edit system]

**Description** Configure a list of domains to be searched.

**Options** *domain-list*—A list of domain names to search. The list can contain up to 6 domain names, with a total of up to 256 characters.

**Usage Guidelines** See “Configuring Which Domains to Search” on page 350.

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

## dump-device

---

<b>Syntax</b>	<pre>dump-device {     compact-flash;     removable-compact-flash;     usb; }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	<p>For J-series Services Routers only. Configure the medium used for storing memory snapshots of system failure. When you specify the storage and an operating system fails, the operating system writes a snapshot of the state of the router when it failed to the storage medium. When the operating system is rebooted, the storage device is checked for a snapshot. If found, the snapshot of memory is written to the /var/crash directory on the router and can be examined by Juniper Networks customer support to help determine the cause of failure.</p> <p>If the swap partition on the device medium is not large enough for the system memory snapshot, the snapshot not successfully written to the directory. Use the request system snapshot command to specify the swap partition.</p>
<b>Options</b>	<p>compact-flash—The primary compact flash.</p> <p>removable-compact-flash—The compact flash device on the front of the router (J4300 and J6300 only) as the system software failure memory snapshot device.</p> <p>usb—The device attached to the universal serial bus (USB) port.</p>
<b>Usage Guidelines</b>	See the <i>J-series Services Router User Guide</i> .
<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>

## events

---

<b>Syntax</b>	events [events];
<b>Hierarchy Level</b>	[edit system accounting]
<b>Description</b>	Configure the types of events to track and log.
<b>Options</b>	<p>events—Event types; can be one or more of the following:</p> <p>login—Audit logins.</p> <p>change-log—Audit configuration changes.</p> <p>interactive-commands—Audit interactive commands (any command-line input).</p>
<b>Usage Guidelines</b>	See “Specifying Events” on page 439.
<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>

## explicit-priority

---

<b>Syntax</b>	explicit-priority;
<b>Hierarchy Level</b>	[edit system syslog file <i>filename</i> ], [edit system syslog host]
<b>Description</b>	Record the priority (facility and severity level) in each message logged to a system log file or directed to a remote destination.
<b>Usage Guidelines</b>	See “Configuring System Log Messages” on page 401.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	<i>JUNOS System Log Messages Reference</i>

## facility-override

---

<b>Syntax</b>	facility-override <i>facility</i> ;
<b>Hierarchy Level</b>	[edit system syslog host]
<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 Table 21 on page 409.
<b>Usage Guidelines</b>	See “Configuring System Log Messages” on page 401.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	<i>JUNOS System Log Messages Reference</i>

## file

---

<b>Syntax</b>	file <i>filename</i> { <i>facility level</i> ; explicit-priority; archive { files <i>number</i> ; size <i>size</i> ; (world-readable   no-world-readable); } }
<b>Hierarchy Level</b>	[edit system syslog]
<b>Description</b>	Configure the types of system logging messages to log to a file.
<b>Options</b>	<p><i>facility</i>—Class of messages to log. To specify multiple classes, include multiple <i>facility level</i> statements. For a list of the facilities, see Table 18 on page 404.</p> <p><i>filename</i>—File in the /var/log directory in which to log messages from the specified facility. To log messages to more than one file, include more than one file statement.</p> <p><i>level</i>—Severity of the messages that belong to the facility specified by the paired <i>facility</i> name. For a list of the severities, see Table 19 on page 405.</p> <p>The remaining statements are explained separately.</p>
<b>Usage Guidelines</b>	See “Configuring System Log Messages” on page 401.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	<i>JUNOS System Log Messages Reference</i>

## files

---

<b>Syntax</b>	files <i>number</i> ;
<b>Hierarchy Level</b>	[edit system syslog archive], [edit system syslog file <i>filename</i> archive]
<b>Description</b>	Configure the maximum number of archived log files to retain. When the JUNOS 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 <i>size</i> on page 519). 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 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).
<b>Options</b>	<i>number</i> —Maximum number of archived files. <b>Range:</b> 1 through 1000 <b>Default:</b> 10 files
<b>Usage Guidelines</b>	See “Configuring System Log Messages” on page 401.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	<i>size</i> on page 519, <i>JUNOS System Log Messages Reference</i>

## finger

---

<b>Syntax</b>	finger { <connection-limit <i>limit</i> >; <rate-limit <i>limit</i> >; }
<b>Hierarchy Level</b>	[edit system services]
<b>Description</b>	Allow finger requests from remote systems to the local router.  The remaining statements are explained separately/
<b>Usage Guidelines</b>	See “Configuring System Services” on page 430.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## ftp

---

<b>Syntax</b>	ftp { <connection-limit <i>limit</i> >; <rate-limit <i>limit</i> >; }
<b>Hierarchy Level</b>	[edit system services]
<b>Description</b>	Allow FTP requests from remote systems to the local router.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring System Services” on page 430.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## full-name

---

<b>Syntax</b>	full-name <i>complete-name</i> ;
<b>Hierarchy Level</b>	[edit system login user]
<b>Description</b>	Configure the complete name of a user.
<b>Options</b>	<i>complete-name</i> —Full name of the user. If the name contains spaces, enclose it in quotation marks.
<b>Usage Guidelines</b>	See “Configuring User Accounts” on page 387.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## host

---

**Syntax** host (*hostname* | other-routing-engine| scc-master) {  
     *facility level*;  
     explicit-priority;  
     facility-override *facility*;  
     log-prefix *string*;  
 }

**Hierarchy Level** [edit system syslog]

**Description** Configure the types of system log messages to log to a remote destination.

**Options** *facility*—Class of messages to log. To specify multiple classes, include multiple *facility level* statements. For a list of the facilities, see Table 18 on page 404.

*hostname*—IP 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.

*level*—Severity of the messages that belong to the facility specified by the paired *facility* name. For a list of the severities, see Table 19 on page 405.

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

scc-master—On a T640 routing node that is part of a routing matrix, direct messages to the TX Matrix platform.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring System Log Messages” on page 401.

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

**See Also** *JUNOS System Log Messages Reference*

## host-name

---

**Syntax** host-name *host-name*;

**Hierarchy Level** [edit system]

**Description** Set the hostname of the router.

**Options** *host-name*—Name of the router.

**Usage Guidelines** See “Configuring the Router’s Name and Addresses” on page 348.

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

## http

---

**Syntax** http {  
     port *port*;  
 }

**Hierarchy Level** [edit system services web-management]

**Description** For J-series Services Routers only, configure port for HTTP service, which is unencrypted.

**Options** The remaining statement is explained separately in this chapter.

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

**See Also** https on page 495, port (HTTP/HTTPS) on page 507, web-management on page 531

## https

---

**Syntax** https {  
     local-certificate *name*;  
     port *port*;  
 }

**Hierarchy Level** [edit system services web-management]

**Description** For J-series Services Routers only, configure for the secure version of HTTP (HTTPS) service, which is encrypted.

**Options** local-certificate *name*—Name of the X.509 certificate for a secure sockets layer (SSL) connection. An SSL connection is configured at the [edit security certificates local] hierarchy.

The remaining statement is explained separately in this chapter.

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

**See Also** http on page 495, port (HTTP/HTTPS) on page 507, web-management on page 531

## idle-timeout

---

<b>Syntax</b>	<code>idle-timeout <i>minutes</i>;</code>
<b>Hierarchy Level</b>	[edit system login class <i>class-name</i> ]
<b>Description</b>	For a login class, configure the maximum time that a session can be idle before the user is logged off the router. The session times out after remaining at the CLI operational mode prompt for the specified time.
<b>Default</b>	If you omit this statement, a user is never forced off the system after extended idle times.
<b>Options</b>	<i>minutes</i> —Maximum idle time. <b>Range:</b> 0 through 100,000 minutes
<b>Usage Guidelines</b>	See “Configuring the Timeout Value for Idle Login Sessions” on page 386.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	user on page 529

## inet6-backup-router

---

<b>Syntax</b>	<code>inet6-backup-router <i>address</i> &lt;destination <i>destination-address</i>&gt;;</code>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Set a default router (running IP version 6 [IPv6]) to use while the local router (running IPv6) is booting and if the routing protocol processes fail to start. The JUNOS software removes the route to this router as soon as the software starts.
<b>Options</b>	<i>address</i> —Address of the default router.  <i>destination destination-address</i> —(Optional) Destination address that is reachable through the backup router. Include this option to achieve network reachability while loading, configuring, and recovering the router, but without the risk of installing a default route in the forwarding table. <b>Default:</b> All hosts (default route) are reachable through the backup router.
<b>Usage Guidelines</b>	See “Configuring a Backup Router” on page 352.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## interfaces

---

**Syntax** interfaces {  
     *interface-name* {  
         bootp;  
         rarp;  
         slarp;  
     }  
 }

**Hierarchy Level** [edit system autoinstallation]

**Description** For J-series Services Routers only, configure the interface on which to perform autoinstallation. A request for an IP address is sent from the interface. Specify the IP address procurement protocol.

**Options** bootp—Sends requests over all available interfaces.

rarp—Sends requests over Ethernet interfaces.

slarp—Sends requests over serial interfaces.

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

**See Also** autoinstallation on page 479

## internet-options

---

**Syntax** internet-options {  
     path-mtu-discovery;  
     source-port upper-limit *upper-limit*;  
     source-quench;  
 }

**Hierarchy Level** [edit system]

**Description** Configure path maximum transmission rate (MTU) discover, source quench, and port range.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring the Path MTU Discovery” on page 440, “Configuring Source Quench” on page 440, and “Configuring the Range of Port Addresses” on page 441.

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

## load-key-file

---

<b>Syntax</b>	load-key-file;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Load RSA (SSH version 1) and DSA (SSH version 2) public keys from a file. The file is a URL containing one or more SSH keys.
<b>Usage Guidelines</b>	See “Configuring the Root Password” on page 355 and “Configuring User Accounts” on page 387.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## local-certificate

---

<b>Syntax</b>	local-certificate;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Import or reference a SSL certificate.
<b>Usage Guidelines</b>	See “Configure JUNOScript SSL Service” on page 431 and “Using JUNOScript SSL Service” on page 663.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## location

<b>Syntax</b>	<pre>location {     altitude <i>feet</i>;     building <i>name</i>;     country-code <i>code</i>;     floor <i>number</i>;     hcoord <i>horizontal-coordinate</i>;     lata <i>service-area</i>;     latitude <i>degrees</i>;     longitude <i>degrees</i>;     npa-nxx <i>number</i>;     postal-code <i>postal-code</i>;     rack <i>number</i>;     vcoord <i>vertical-coordinate</i>; }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the system location in various formats.
<b>Options</b>	<p>altitude <i>feet</i>—Number of feet above sea level.</p> <p>building <i>name</i>—Name of building. The name of the building can be 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" ").</p> <p>country-code <i>code</i>—Two-letter country code.</p> <p>floor <i>number</i>—Floor in the building.</p> <p>hcoord <i>horizontal-coordinate</i>—Bellcore Horizontal Coordinate.</p> <p>lata <i>service-area</i>—Long-distance service area.</p> <p>latitude <i>degrees</i>—Latitude in degree format.</p> <p>longitude <i>degrees</i>—Longitude in degree format.</p> <p>npa-nxx <i>number</i>—First six digits of the phone number (area code and exchange).</p> <p>postal-code <i>postal-code</i>—Postal code.</p> <p>rack <i>number</i>—Rack number.</p> <p>vcoord <i>vertical-coordinate</i>—Bellcore Vertical Coordinate.</p>
<b>Usage Guidelines</b>	See “Configuring the System Location” on page 354.
<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>

## log-prefix

---

<b>Syntax</b>	<code>log-prefix <i>string</i>;</code>
<b>Hierarchy Level</b>	[edit system syslog host]
<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>Usage Guidelines</b>	See “Configuring System Log Messages” on page 401.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	<i>JUNOS System Log Messages Reference</i>

## login

---

<b>Syntax</b>	<pre>login {   message <i>text</i>;   class <i>class-name</i> {     allow-commands "<i>regular-expression</i>";     allow-configuration "<i>regular-expression</i>";     deny-commands "<i>regular-expression</i>";     deny-configuration "<i>regular-expression</i>";     idle-timeout <i>minutes</i>;     no-tip;     permissions [ <i>permissions</i> ];   }   user <i>username</i> {     full-name <i>complete-name</i>;     uid <i>uid-value</i>;     class <i>class-name</i>;     authentication <i>authentication</i>;     (encrypted-password "<i>password</i>"   plain-text-password);     ssh-rsa "<i>public-key</i>";     ssh-dsa "<i>public-key</i>";   } }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure user access to the router.
<b>Options</b>	The remaining statements are explained separately in this chapter.
<b>Usage Guidelines</b>	See “Configuring User Access” on page 375.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## max-configurations-on-flash

---

<b>Syntax</b>	max-configurations-on-flash <i>number</i> ;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Specify the number of configurations stored on the the flash drive.
<b>Options</b>	<i>number</i> — The number of configurations stored on the flash drive. <b>Range:</b> 0 through 49. The most recently saved configuration is number 0, and the oldest saved configuration is number 49.
<b>Usage Guidelines</b>	See “Specifying the Number of Configurations Stored on the Flash Drive” on page 438.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration

## message

---

<b>Syntax</b>	message <i>text</i> ;
<b>Hierarchy Level</b>	[edit system login]
<b>Description</b>	Configure a system login message.
<b>Options</b>	<i>text</i> —Text of the message.
<b>Usage Guidelines</b>	See “Configuring a System Login Message” on page 434.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration

## mirror-flash-on-disk

---

<b>Syntax</b>	mirror-flash-on-disk;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the hard disk to automatically mirror the contents of the compact flash. The hard disk maintains a synchronized mirror copy of the compact-flash contents. Data written to the compact flash is simultaneously updated in the mirrored copy of the hard disk. If the flash drive fails to read data, the hard disk automatically retrieves its mirrored copy of the flash disk.



**CAUTION:** We recommend that you disable flash disk mirroring when you upgrade or downgrade the router.

You cannot issue the request system snapshot command while flash disk mirroring is enabled.

---



**NOTE:** After you have enabled or disabled the `mirror-flash-on-disk` statement, you must reboot the router for your changes to take effect. To reboot, issue the request `system reboot` command.

---

**Usage Guidelines** See “Configuring Flash Disk Mirroring” on page 353.

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

---

## multicast-client

---

**Syntax** `multicast-client <address>;`

**Hierarchy Level** [edit system ntp]

**Description** For NTP, configure the local router to listen for multicast messages on the local network to discover other servers on the same subnet.

**Options** `address`—(Optional) One or more IP addresses. If you specify addresses, the router joins those multicast groups.  
**Default:** 224.0.1.1.

**Usage Guidelines** See “Configuring the Router to Listen for Multicast Messages” on page 400.

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

---

## name-server

---

**Syntax** `name-server {  
     address;  
>}`

**Hierarchy Level** [edit system]

**Description** Configure one or more Domain Name System (DNS) name servers.

**Options** `address`—Address of the name server. To configure multiple name servers, include multiple `address` options.

**Usage Guidelines** See “Configuring a DNS Name Server” on page 351.

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

## no-compression-configuration-files

---

<b>Syntax</b>	no-compress-configuration-files;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the router so that it does not compress the current operational configuration.
<b>Usage Guidelines</b>	See “Compressing the Current Configuration File” on page 357.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## no-redirects

---

<b>Syntax</b>	no-redirects;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Disable the sending of protocol redirect messages by the router.  To disable the sending of redirect messages on a per-interface basis, include the no-redirects statement at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> ] hierarchy level.
<b>Default</b>	The router sends redirect messages.
<b>Usage Guidelines</b>	See “Disabling the Sending of Redirect Messages on the Router” on page 428.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	The no-redirects statement in the <i>JUNOS Network Interfaces and Class of Service Configuration Guide</i> .

## no-saved-core-context

---

<b>Syntax</b>	no-saved-core-context;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Disable core files generated by internal JUNOS processes.
<b>Default</b>	Core files generated by internal JUNOS processes are now saved along with contextual information in compressed tar files stored under /var/tmp/process-name.core.core-number.tgz for debugging purposes.
<b>Usage Guidelines</b>	See “Core Dump Files” on page 436.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## no-tip

---

<b>Syntax</b>	no-tip;
<b>Hierarchy Level</b>	[edit system login class <i>class-name</i> ]
<b>Description</b>	Disable CLI tips.
<b>Default</b>	Enabled.
<b>Usage Guidelines</b>	See “Configuring Tips” on page 386.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	“Displaying Tips About CLI Commands” on page 165.

## no-world-readable

---

**See** world-readable on page 531

## ntp

---

<b>Syntax</b>	ntp { authentication-key <i>number</i> type <i>type</i> value <i>password</i> ; boot-server <i>address</i> ; broadcast < <i>address</i> > < <i>key key-number</i> > < <i>version value</i> > < <i>tll value</i> >; broadcast-client; multicast-client < <i>address</i> >; peer <i>address</i> < <i>key key-number</i> > < <i>version value</i> > < <i>prefer</i> >; server <i>address</i> < <i>key key-number</i> > < <i>version value</i> > < <i>prefer</i> >; source-address <i>source-address</i> ; trusted-key [ <i>key-numbers</i> ]; }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure NTP on the router.
<b>Options</b>	The remaining statements are explained separately in this chapter.
<b>Usage Guidelines</b>	See “Configuring the Network Time Protocol” on page 393.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## path-mtu-discovery

---

<b>Syntax</b>	path-mtu-discovery
<b>Hierarchy Level</b>	[edit system internet-options]
<b>Description</b>	Configure path MTU discovery on outgoing Transmission Control Protocol (TCP) connections.
<b>Usage Guidelines</b>	See “Configuring the Path MTU Discovery” on page 440.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## peer

---

<b>Syntax</b>	peer <i>address</i> <key <i>key-number</i> > <version <i>value</i> > <prefer>;
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	For NTP, configure the local router to operate in symmetric active mode with the remote system at the specified <i>address</i> . In this mode, the local router and the remote system can synchronize each other. This configuration is useful in a network in which either the local router or the remote system might be a better source of time.
<b>Options</b>	<p><i>address</i>—Address of the remote system. You must specify an address, not a hostname.</p> <p>key <i>key-number</i>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number. <b>Values:</b> Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as the preferred host, which means that, if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>version <i>value</i>—(Optional) Specify the NTP version number to be used in outgoing NTP packets. <b>Values:</b> 1, 2, 3 <b>Default:</b> 3</p>
<b>Usage Guidelines</b>	See “Configuring the NTP Time Server and Time Services” on page 395.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## permissions

---

<b>Syntax</b>	<code>permissions [ <i>permissions</i> ];</code>
<b>Hierarchy Level</b>	[edit system login class]
<b>Description</b>	Configure the login access privileges to be provided on the router.
<b>Options</b>	<i>permissions</i> —Privilege type. For a list of types, see Table 13 on page 377.
<b>Usage Guidelines</b>	See “Configuring Access Privilege Levels” on page 376.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	user on page 529

## pic-console-authentication

---

<b>Syntax</b>	<code>pic-console authentication {     (encrypted-password "<i>password</i>"   plain-text-password); }</code>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure console access to Physical Interface Cards (PICs).
<b>Default</b>	Disabled. By default, there is no password setting for console access.
<b>Options</b>	<code>encrypted-password "<i>password</i>"</code> —Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.  <code>plain-text-password</code> —Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password. For information about how to create plain-text passwords, see “Specifying Plain-Text Passwords” on page 17.
<b>Usage Guidelines</b>	See “Specifying Plain-Text Passwords” on page 17 and “Configuring Console Access to PICs” on page 434.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	“Configuring Console and Auxiliary Port Properties” on page 428.

## port

---

See the following sections:

port (HTTP/HTTPS) on page 507

port (RADIUS Server) on page 507

port (SDX Server) on page 508

port (TACACS+ Server) on page 508

### *port (HTTP/HTTPS)*

<b>Syntax</b>	<code>port port;</code>
<b>Hierarchy Level</b>	[edit system services web-management]
<b>Description</b>	For J-series Services Routers only, configure the port on which the HTTP or HTTPS service is connected.
<b>Options</b>	<i>port</i> —The TCP port number on which the specified service listens.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	web-management on page 531, http on page 495, https on page 495

### *port (RADIUS Server)*

<b>Syntax</b>	<code>port port-number;</code>
<b>Hierarchy Level</b>	[edit system radius-server <i>address</i> ]
<b>Description</b>	Configure the port number on which to contact the RADIUS server.
<b>Options</b>	<i>number</i> —Port number on which to contact the RADIUS server. <b>Default:</b> 1812 (as specified in RFC 2138)
<b>Usage Guidelines</b>	See “Configuring RADIUS Authentication” on page 360.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

**port (SDX Server)**

<b>Syntax</b>	<code>port port-number;</code>
<b>Hierarchy Level</b>	[edit system services service-deployment servers <i>server-address</i> ]
<b>Description</b>	Configure the port number on which to contact the SDX server.
<b>Options</b>	<i>port-number</i> —(Optional) The TCP port number for the SDX server. <b>Default:</b> 3333
<b>Usage Guidelines</b>	See “Enabling the SDX Software” on page 440.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

**port (TACACS+ Server)**

<b>Syntax</b>	<code>port number;</code>
<b>Hierarchy Level</b>	[edit system accounting destination tacplus server <i>server-address</i> ]
<b>Description</b>	Configure the port number on which to contact the TACACS+ server.
<b>Options</b>	<i>number</i> —Port number on which to contact the TACACS+ server. <b>Default:</b> 49
<b>Usage Guidelines</b>	See “Configuring TACACS+ System Accounting” on page 438.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

**ports**


---

<b>Syntax</b>	<pre>ports {   auxiliary {     type <i>terminal-type</i>;   }   console {     type <i>terminal-type</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the properties of the console and auxiliary ports, which are located on the router’s craft interface.
<b>Options</b>	The remaining statements are explained separately in this chapter.
<b>Usage Guidelines</b>	See “Configuring Console and Auxiliary Port Properties” on page 428.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## processes

**Syntax** processes {  
 disk-monitoring (enable | disable);  
 inet-process (enable | disable) failover (alternate-media | other-routing-engine);  
 interface-control (enable | disable) failover (alternate-media | other-routing-engine);  
 mib-process (enable | disable) failover (alternate-media | other-routing-engine);  
 ntp (enable | disable) failover (alternate-media | other-routing-engine);  
 routing (enable | disable) failover (alternate-media | other-routing-engine);  
 snmp (enable | disable) failover (alternate-media | other-routing-engine);  
 watchdog (enable | disable) failover (alternate-media | other-routing-engine);  
 web-management (enable | disable) failover (alternate-media | other-routing-engine);  
 timeout *seconds*;  
 }

**Hierarchy Level** [edit system]

**Description** Configure which JUNOS software processes are running on the router.

**Default** All processes are enabled by default



**CAUTION:** Never disable any of the software processes unless instructed to do so by a Customer Support engineer.

**Options** failover (alternate-media | other-routing-engine)—(Optional) For routers with redundant Routing Engines only, switch to backup media if a process fails repeatedly. If a process fails three times in quick succession, the router reboots from the alternate media or the other Routing Engine.

timeout *seconds*—(Optional) How often the system checks the watchdog timer, in seconds. If the watchdog timer has not been checked in the specified number of seconds, the system reloads. If you set the time value too low, it is possible for the system to reboot immediately after it loads.

**Values:** 15, 60, 180

**Default:** 180 seconds (rounded up to 291 seconds by the JUNOS kernel)

**Usage Guidelines** See “Disabling JUNOS Software Processes” on page 435.

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

## protocol-version

---

<b>Syntax</b>	protocol-version;
<b>Hierarchy Level</b>	[edit system services ssh]
<b>Description</b>	Specify the secure shell (ssh) protocol version.
<b>Options</b>	protocol version—v1, v2, or [v1 v2] <b>Default:</b> [v2]
<b>Usage Guidelines</b>	See “Configuring the SSH Protocol Version” on page 433.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## radius-server

---

<b>Syntax</b>	radius-server <i>server-address</i> { port <i>number</i> ; retry <i>number</i> ; secret <i>password</i> ; source-address <i>source-address</i> ; timeout <i>seconds</i> ; }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the Remote Authentication Dial-In User Service (RADIUS) for Point-to-Point Protocol (PPP).  To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.
<b>Options</b>	<i>server-address</i> —Address of the RADIUS authentication server.  The remaining statements are explained separately in this chapter.
<b>Usage Guidelines</b>	See “Configuring RADIUS Authentication” on page 360.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

rate-limit

---

<b>Syntax</b>	<code>rate-limit limit;</code>
<b>Hierarchy Level</b>	[edit system services finger], [edit system services rlogin], [edit system services ssh], [edit system services telnet], [edit system services xnm-clear-text], [edit system services xnm-ssl]
<b>Description</b>	Maximum number of connection attempts on an access service.
<b>Options</b>	<code>rate-limit limit</code> —(Optional) Maximum number of connection attempts allowed per minute. <b>Range:</b> 1 through 250 <b>Default:</b> 150
<b>Usage Guidelines</b>	See “Configuring System Services” on page 430.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

retry

---

<b>Syntax</b>	<code>retry number;</code>
<b>Hierarchy Level</b>	[edit system radius-server <i>server-address</i> ]
<b>Description</b>	Number of times that the router attempts to contact a RADIUS authentication server.
<b>Options</b>	<code>number</code> —Number of times to retry contacting a RADIUS server. <b>Range:</b> 1 through 10 <b>Default:</b> 3
<b>Usage Guidelines</b>	See “Configuring RADIUS Authentication” on page 360.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	timeout on page 525

## root-authentication

---

<b>Syntax</b>	<pre> root-authentication {     (encrypted-password "<i>password</i>"   plain-text-password);     ssh-rsa "<i>public-key</i>";     ssh-dsa "<i>public-key</i>"; } </pre>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the authentication methods for the root-level user, whose username is "root."
<b>Options</b>	<p>encrypted-password "<i>password</i>"—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.</p> <p>plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password. For information about how to create plain-text passwords, see "Specifying Plain-Text Passwords" on page 17.</p> <p>ssh-rsa "<i>public-key</i>"—secure shell (SSH 1) authentication. Specify the SSH public key. You can specify one or more public keys.</p> <p>ssh-rsa "<i>public-key</i>"—secure shell (SSH 2) authentication. Specify the SSH public key. You can specify one or more public keys.</p>
<b>Usage Guidelines</b>	See "Configuring the Root Password" on page 355.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	authentication on page 476

## root-login

---

<b>Syntax</b>	root-login (allow   deny   deny-password);
<b>Hierarchy Level</b>	[edit system services ssh]
<b>Description</b>	Control user access through SSH.
<b>Options</b>	<p>allow—Allows users to log in to the router as root through SSH.  <b>Default:</b> allow</p> <p>deny—Disable users from logging in to the router as root through SSH.</p> <p>deny-password—Allows users to log in to the router as root through SSH when the authentication method (for example, RSA authentication) does not require a password.</p>
<b>Usage Guidelines</b>	See “Configuring the Root Login” on page 432.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>See Also</b>	“Configuring SSH Service” on page 432.

## saved-core-context

---

<b>Syntax</b>	saved-cored-context;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Save contextual information for core files generated by internal JUNOS processes. The contextual information contains the configuration and log messages file.
<b>Usage Guidelines</b>	See “Core Dump Files” on page 436.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>See Also</b>	no-saved-core-context on page 503

## saved-core-files

---

<b>Syntax</b>	<code>save-core-files <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the amount of core values to save.
<b>Options</b>	<i>number</i> —Number of core file to save and can be a value from 1 through 64.
<b>Usage Guidelines</b>	See “Core Dump Files” on page 436.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	saved-core-context on page 513.

## secret

---

<b>Syntax</b>	<code>secret <i>password</i>;</code>
<b>Hierarchy Level</b>	[edit system radius-server <i>server-address</i> ], [edit system tacplus-server <i>server-address</i> ], [edit system accounting destination tacplus server <i>server-address</i> ]
<b>Description</b>	Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router must match that used by the server.
<b>Options</b>	<i>password</i> —Password to use; can include spaces.
<b>Usage Guidelines</b>	See “Configuring RADIUS Authentication” on page 360, “Configuring TACACS+ Authentication” on page 362, and “Configuring TACACS+ System Accounting” on page 438.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## server

See the following sections:

server (Accounting) on page 515

server (NTP) on page 515

**server (Accounting)**

```
Syntax  server {
          server-address {
            port port-number;
            secret password;
            single-connection;
            timeout seconds;
          }
        }
```

**Hierarchy Level** [edit system accounting destination tacplus]

**Description** Configure TACACS+ logging.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring TACACS+ System Accounting” on page 438.

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

**server (NTP)**

```
Syntax  server address <key key-number> <version value> <prefer>;
```

**Hierarchy Level** [edit system ntp]

**Description** For NTP, configure the local router to operate in client mode with the remote system at the specified *address*. In this mode, the local router can be synchronized to the remote system, but the remote system never can be synchronized to the local router.

**Options** *address*—Address of the remote system. You must specify an address, not a hostname.

*key key-number*—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

**Values:** Any unsigned 32-bit integer

**prefer**—(Optional) Mark the remote system as preferred host, which means that, if all other are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

**version *value***—(Optional) Specify the version number to be used in outgoing NTP packets.

**Values:** 1, 2, 3

**Default:** 3

**Usage Guidelines** See “Configuring the NTP Time Server and Time Services” on page 395.

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

## servers

---

**Syntax** `servers server-address {  
 port port-number;  
}`

**Hierarchy Level** [edit system services service-deployment]

**Description** Configure an IPv4 address for the Service Deployment System (SDX) server.

**Options** **server-address**—The TCP port number.  
**Default:** 3333

The remaining statement is explained separately in this chapter.

**Usage Guidelines** See “Enabling the SDX Software” on page 440.

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

## service-deployment

---

**Syntax** `service-deployment {  
 servers server-address {  
 port port-number;  
 }  
 source-address source-address;  
}`

**Hierarchy Level** [edit system services]

**Description** Enable JUNOS software to work with the SDX software.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Enabling the SDX Software” on page 440.

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

## services

```

Syntax  services {
            finger {
              <connection-limit limit>;
              <rate-limit limit>;
            }
            ftp {
              <connection-limit limit>;
              <rate-limit limit>;
            }
            ssh {
              root-login (allow | deny | deny-password);
              protocol-version [v1 v2];
              <connection-limit limit>;
              <rate-limit limit >;
            }
            service-deployment {
              servers server-address {
                port-number port-number;
              }
              source-address source-address;
            }
            telnet {
              <connection-limit limit>;
              <rate-limit limit>;
            }
            xnm-clear-text {
              <connection-limit limit>;
              <rate-limit limit>;
            }
            xnm-ssl {
              <connection-limit limit>;
              <rate-limit limit>;
              <local-certificate name>
            }
          }

```

**Hierarchy Level** [edit system]

**Description** Configure the router so that users on remote systems can access the local router through the finger, rlogin, SSH, and Telnet, JUNOScript clear-text, JUNOScript SSL, and network utilities or enable JUNOS software to work with the SDX software.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring System Services” on page 430 and “Enabling the SDX Software” on page 440

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

ssh

---

<b>Syntax</b>	ssh { <connection-limit <i>limit</i> >; <rate-limit <i>limit</i> >; }
<b>Hierarchy Level</b>	[edit system services]
<b>Description</b>	Allow ssh requests from remote systems to the local router.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring SSH Service” on page 432.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

single-connection

---

<b>Syntax</b>	single-connection;
<b>Hierarchy Level</b>	[edit system tacplus-server <i>server-address</i> ], [edit system accounting destination tacplus-server <i>server-address</i> ]
<b>Description</b>	Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt.
<b>Usage Guidelines</b>	See “Configuring TACACS+ Authentication” on page 362 and “Configuring TACACS+ System Accounting” on page 438.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## 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>Description</b>	Configure the maximum amount of data that the JUNOS 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> . For information about the number of archive files that the utility creates in this way, see files on page 492.
<b>Options</b>	<i>size</i> —Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). <b>Syntax:</b> <i>xk</i> to specify the number of kilobytes, <i>xm</i> for the number of megabytes, or <i>xg</i> for the number of gigabytes <b>Range:</b> 64 KB through 1 GB
<b>Usage Guidelines</b>	See “Configuring System Log Messages” on page 401.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	files on page 492, <i>JUNOS System Log Messages Reference</i>

## source-address

---

source-address (NTP, RADIUS, System Logging, or TACACS+ ) on page 520

source-address (SDX Software) on page 520

### ***source-address (NTP, RADIUS, System Logging, or TACACS+)***

<b>Syntax</b>	source-address <i>source-address</i> ;
<b>Hierarchy Level</b>	[edit system accounting destination tacplus server <i>server-address</i> ], [edit system ntp], [edit system radius-server <i>server-address</i> ], [edit system syslog], [edit system tacplus-server <i>server-address</i> ]
<b>Description</b>	Specify a source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to use when directing system log messages to a remote machine.
<b>Options</b>	<i>source-address</i> —A valid IP address configured on one of the router interfaces. For system logging, the address is used for messages sent to the remote machines specified in all the host <i>hostname</i> statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine or to the TX Matrix platform in a routing matrix.
<b>Usage Guidelines</b>	See “Specifying a Source Address for RADIUS and TACACS+ Servers” on page 364, “Specifying a Source Address for an NTP Server” on page 394, and “Specifying an Alternate Source Address” on page 408.
<b>See Also</b>	set date ntp source-address on page 269
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

### ***source-address (SDX Software)***

<b>Syntax</b>	source-address <i>source-address</i> ;
<b>Hierarchy Level</b>	[edit system services service-deployment]
<b>Description</b>	Enable JUNOS software to work with the SDX software.
<b>Options</b>	<i>source-address</i> —(Optional) The local IPv4 address to be used as source address for traffic to the SDX server. The source address restricts traffic within the out-of-band network.
<b>Usage Guidelines</b>	See “Enabling the SDX Software” on page 440.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## source-port

---

<b>Syntax</b>	source-port upper-limit < <i>upper-limit</i> >;
<b>Hierarchy Level</b>	[edit system internet-options]
<b>Description</b>	Configure the range of port addresses.
<b>Options</b>	upper-limit <i>upper-limit</i> —(Optional) The range of port addresses and can be a value from 5000 through 65,355.
<b>Usage Guidelines</b>	See “Configuring the Range of Port Addresses” on page 441.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## source-quench

---

<b>Syntax</b>	source-quench
<b>Hierarchy Level</b>	[edit system internet-options]
<b>Description</b>	Configure the JUNOS software to ignore Internet Control Message Protocol (ICMP) source quench messages.
<b>Usage Guidelines</b>	See “Configuring Source Quench” on page 440.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## static-host-mapping

---

<b>Syntax</b>	static-host-mapping { <i>host-name</i> { inet [ <i>address</i> ]; sysid <i>system-identifier</i> ; alias [ <i>alias</i> ]; } }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Map a hostname to one or more IP addresses and aliases, and configure an International Organization for Standardization (ISO) system identifier (system ID).
<b>Options</b>	alias <i>alias</i> —(Optional) Alias for the hostname.  <i>host-name</i> —Fully qualified hostname.

*inet address*—IP address. You can specify one or more IP addresses for the host.

*sysid system-identifier*—ISO system identifier (system ID). This is the 6-byte portion of the Intermediate System-to-Intermediate System (IS-IS) network service access point (NSAP). We recommend that you use the host's IP address represented in binary-coded decimal (BCD) format. For example, the IP address 208.197.169.18 is 2081.9716.9018 in BCD.

**Usage Guidelines** See “Configuring the Router’s Name and Addresses” on page 348.

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

## syslog

---

```
Syntax  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;
           }
         }
```

**Hierarchy Level** [edit system]

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

The statements are explained separately.

**Usage Guidelines** See “Configuring System Log Messages” on page 401.

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

**See Also** *JUNOS System Log Messages Reference*

## system

---

**Syntax** system { ... }

**Hierarchy Level** [edit]

**Description** Configure system management properties.

**Usage Guidelines** See “System Management Configuration Statements” on page 341.

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

## tacplus

---

```
Syntax tacplus {
    server {
        server-address {
            secret password;
            single-connection;
            timeout seconds;
            port port-number;
        }
    }
}
```

**Description** Configure the Terminal Access Controller Access Control System Plus (TACACS+ ).

**Hierarchy Level** [edit system accounting destination]

**Options** *server-address*—Address of the TACACS+ authentication server.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring TACACS+ System Accounting” on page 438.

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

## tacplus-options

---

<b>Syntax</b>	tacplus-options service-name <i>service-name</i> ;
<b>Description</b>	Configure the multiple TACACS+ servers to use the same authentication service.
<b>Hierarchy Level</b>	[edit system]
<b>Options</b>	service-name <i>service-name</i> —The name of the authentication service. <b>Default:</b> junos-exec
<b>Usage Guidelines</b>	See “Configuring the Same Authentication Service for Multiple TACACS+ Servers” on page 365.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## tacplus-server

---

<b>Syntax</b>	tacplus-server <i>server-address</i> { secret <i>password</i> ; single-connection; source-address <i>source-address</i> ; timeout <i>seconds</i> ; }
<b>Description</b>	Configure the TACACS+ server.
<b>Hierarchy Level</b>	[edit system]
<b>Options</b>	<i>server-address</i> —Address of the TACACS+ authentication server.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring TACACS+ Authentication” on page 362.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## telnet

---

<b>Syntax</b>	rlogin { <connection-limit <i>limit</i> >; <rate-limit <i>limit</i> >; }
<b>Hierarchy Level</b>	[edit system services]
<b>Description</b>	Allow rlogin requests from remote systems to the local router.  The remaining statements are explained separately.

**Usage Guidelines** See “Configuring System Services” on page 430.

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

## time-format

---

**Syntax** time-format (year | millisecond | year millisecond);

**Hierarchy Level** [edit system]

**Description** Include the year, the millisecond, or both, in the timestamp on every system log message. The additional information is included 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.

By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged, for example, Aug 21 12:36:30.

**Options** millisecond—Include the millisecond in the timestamp.  
year—Include the year in the timestamp.

**Usage Guidelines** See “Configuring System Log Messages” on page 401.

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

**See Also** *JUNOS System Log Messages Reference*

## timeout

---

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit system radius-server *server-address*],  
[edit system tacplus-server *server-address*],  
[edit system accounting destination tacplus server *server-address*]

**Description** Configure the amount of time that the local router waits to receive a response from a RADIUS or TACACS+ server.

**Options** *seconds*—Amount of time to wait.  
**Range:** 1 through 90 seconds  
**Default:** 3 seconds

**Usage Guidelines** See “Configuring RADIUS Authentication” on page 360 and “Configuring TACACS+ Authentication” on page 362.

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

**See Also** retry on page 511

## time-zone

---

<b>Syntax</b>	<code>time-zone <i>time-zone</i>;</code>
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Set the local time zone.
<b>Default</b>	UTC
<b>Options</b>	<p><i>time-zone</i>—Time zone. To have the time zone change take effect for all processes running on the router, you must reboot the router. Specify the time zone either as UTC, which is the default time zone, or use one of the following continent and major city:</p> <p>Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek</p> <p>America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Aruba, America/Asuncion, America/Barbados, America/Belize, America/Bogota, America/Boise, America/Buenos_Aires, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Cordoba, America/Costa_Rica, America/Cuiaba, America/Curacao, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/El_Salvador, America/Ensenada, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Vevay, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Mexico_City, America/Miquelon, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Regina, America/Rosario, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Tortola, America/Vancouver, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife</p>

Antarctica/Casey, Antarctica/DumontDUrville, Antarctica/Mawson,  
Antarctica/McMurdo, Antarctica/Palmer, Antarctica/South\_Pole

Arctic/Longyearbyen

Asia/Aden, Asia/Alma-Ata, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe,  
Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok,  
Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chungking,  
Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dubai, Asia/Dushanbe,  
Asia/Gaza, Asia/Harbin, Asia/Hong\_Kong, Asia/Irkutsk, Asia/Ishigaki,  
Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka,  
Asia/Karachi, Asia/Kashgar, Asia/Katmandu, Asia/Krasnoyarsk,  
Asia/Kuala\_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Magadan,  
Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novosibirsk, Asia/Omsk,  
Asia/Phnom\_Penh, Asia/Pyongyang, Asia/Qatar, Asia/Rangoon, Asia/Riyadh,  
Asia/Saigon, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Taipei,  
Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Thimbu, Asia/Tokyo,  
Asia/Ujung\_Pandang, Asia/Ulan\_Bator, Asia/Urumqi, Asia/Vientiane,  
Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan

Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape\_Verde,  
Atlantic/Faeroe, Atlantic/Jan\_Mayen, Atlantic/Madeira, Atlantic/Reykjavik,  
Atlantic/South\_Georgia, Atlantic/St\_Helena, Atlantic/Stanley

Australia/Adelaide, Australia/Brisbane, Australia/Broken\_Hill, Australia/Darwin,  
Australia/Hobart, Australia/Lindeman, Australia/Lord\_Howe,  
Australia/Melbourne, Australia/Perth, Australia/Sydney

Europe/Amsterdam, Europe/Andorra, Europe/Athens, Europe/Belfast,  
Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels,  
Europe/Bucharest, Europe/Budapest, Europe/Chisinau, Europe/Copenhagen,  
Europe/Dublin, Europe/Gibraltar, Europe/Helsinki, Europe/Istanbul,  
Europe/Kaliningrad, Europe/Kiev, Europe/Lisbon, Europe/Ljubljana,  
Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta,  
Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Oslo, Europe/Paris,  
Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara,  
Europe/San\_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje,  
Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Vaduz,  
Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Warsaw, Europe/Zagreb,  
Europe/Zurich

Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos,  
Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives,  
Indian/Mauritius, Indian/Mayotte, Indian/Reunion

Pacific/Apia, Pacific/Auckland, Pacific/Chatham, Pacific/Easter, Pacific/Efate,  
Pacific/Enderbury, Pacific/Fakaofu, Pacific/Fiji, Pacific/Funafuti,  
Pacific/Galapagos, Pacific/Gambier, Pacific/Guadacanal, Pacific/Guam,  
Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae,  
Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway,  
Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago\_Pago,  
Pacific/Palau, Pacific/Pitcairn, Pacific/Ponape, Pacific/Port\_Moresby,  
Pacific/Rarotonga, Pacific/Saipan, Pacific/Tahiti, Pacific/Tarawa,  
Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap

**Usage Guidelines** See “Setting the Time Zone” on page 392.

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

## transfer-interval

---

**Syntax** transfer-interval *interval*;

**Hierarchy Level** [edit system archival configuration]

**Description** Configure the router to periodically transfer its currently active configuration to an archive site.

**Option** *interval*—Time interval to transfer the current configuration to an archive site.  
**Range:** 15 through 2880 minutes

**Usage Guidelines** See “Configuring the Transfer Interval” on page 437.

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

**See Also** configuration on page 483, transfer-on-commit on page 528, archive on page 475

## transfer-on-commit

---

**Syntax** transfer-on-commit;

**Hierarchy Level** [edit system archival configuration]

**Description** Configure the router to transfer its currently active configuration to an archive site each time you commit a candidate configuration.

**Usage Guidelines** See “Configuring Transfer on Commit” on page 437.

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

**See Also** configuration on page 483, transfer-interval on page 528, archive on page 475

## trusted-key

---

<b>Syntax</b>	trusted-key [ <i>key-numbers</i> ];
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	For NTP, configure the keys you are allowed to use when you configure the local router to synchronize its time with other systems on the network.
<b>Options</b>	<i>key-numbers</i> —One or more key numbers. Each key can be any 32-bit unsigned integer except 0.
<b>Usage Guidelines</b>	See “Configuring NTP Authentication Keys” on page 399.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	authentication-key on page 477, broadcast on page 480, peer on page 505, server on page 515

## uid

---

<b>Syntax</b>	uid <i>uid-value</i> ;
<b>Hierarchy Level</b>	[edit system login user]
<b>Description</b>	Configure a user identifier for a login account.
<b>Options</b>	<i>uid-value</i> —Number associated with the login account. This value must be unique on the router. <b>Range:</b> 100 through 64,000
<b>Usage Guidelines</b>	See “Configuring User Access” on page 375.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## user

---

See the following sections:

user (Access) on page 530

user (System Logging) on page 530

**user (Access)**

**Syntax** `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";  
     }  
}`

**Hierarchy Level** [edit system login]

**Description** Configure access permission for individual users.

**Options** The remaining statements are explained separately in this chapter.

**Usage Guidelines** See “Configuring User Access” on page 375.

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

**See Also** class on page 481

**user (System Logging)**

**Syntax** `user (username | *) {  
     facility level;  
}`

**Hierarchy Level** [edit system syslog]

**Description** Configure the types of system log messages to log to user terminals.

**Options** \* (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.

*username*—JUNOS 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 user statement.

**Usage Guidelines** See “Configuring System Log Messages” on page 401.

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

**See Also** *JUNOS System Log Messages Reference*

## web-management

---

**Syntax** web-management {  
     http {  
         port *port*;  
     }  
     https {  
         local-certificate *name*;  
         port *port*;  
     }  
 }

**Hierarchy Level** [edit system services]

**Description** For J-series Services Routers only, configure settings for HTTP or HTTPS.

**Options** The remaining statements are explained separately in this chapter.

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

**See Also** http on page 495, https on page 495, port (HTTP/HTTPS) on page 507

## world-readable

---

**Syntax** world-readable | no-world-readable;

**Hierarchy Level** [edit system syslog]

**Description** Grant all users permission to read log files, or restrict the permission only to the root user and users who have the JUNOS maintenance permission.

**Default** no-world-readable

**Usage Guidelines** See “Configuring System Log Messages” on page 401.

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

**See Also** *JUNOS System Log Messages Reference*

## xnm-clear-text

---

<b>Syntax</b>	xnm-clear-text { <connection-limit <i>limit</i> >; <rate-limit <i>limit</i> >; }
<b>Hierarchy Level</b>	[edit system services]
<b>Description</b>	Allow JUNOScript clear-text requests from remote systems to the local router.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring Finger Service” on page 430.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## xnm-ssl

---

<b>Syntax</b>	xnm-clear-text { <connection-limit <i>limit</i> >; <rate-limit <i>limit</i> >; }
<b>Hierarchy Level</b>	[edit system services]
<b>Description</b>	Allow JUNOScript SSL requests from remote systems to the local router.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configure JUNOScript SSL Service” on page 431.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.