JUNIPER NETWORKS | Engineering Simplicity

J-Web User Guide for SRX Series Firewalls

Published
2024-07-01

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

J-Web User Guide for SRX Series Firewalls

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

4

Monitor

About This Guide

Use this guide to understand the Junos Web Device Manager, its capabilities, and features.

1

PART

Juniper Web Device Manager

CHAPTER 1

Getting Started

IN THIS CHAPTER

Juniper Web Device Manager Overview

IN THIS SECTION

What is J-Web?

Juniper Networks SRX Series Services Gateways are shipped with the Juniper Networks Junos operating system (Junos OS) preinstalled.

Junos OS has the following primary user interfaces:

- Juniper Web Device Manager (J-Web) GUI
- Junos OS CLI

The J-Web interface allows you to monitor, configure, troubleshoot, and manage your device by means of a Web browser enabled with HTTP over Secure Sockets Layer (HTTPS) by default.

Benefits of J-Web

- Provides a simple user interface that enables new users to quickly become proficient.
- Enables effective threat management while producing detailed data access and user activity reports. An action-oriented design enables the network administrator to detect threats across the network as they occur, quickly block the traffic going to or coming from a specific region, and apply immediate remedial action with a single click.
- Enables administrators to assess the effectiveness of each firewall rule and quickly identify the unused rules, which results in better management of the firewall environment.

RELATED DOCUMENTATION

Access the J-Web User Interface | 3

Explore J-Web | 39

Access the J-Web User Interface

IN THIS SECTION

Prerequisites for Using J-Web

To access the J-Web interface for all SRX Series devices, your management device requires the following software:

- Supported browsers—Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer.

  NOTE: By default, you establish a J-Web session through an HTTPS-enabled Web browser.

- Language support— English-version browsers.

Log in to J-Web

NOTE: This document assumes that you are accessing the device to launch J-Web for the first time using a factory default configuration. If your SRX Series device is already configured with a management IP address, you simply point your browser to the device's management address to access J-Web.

The factory default settings vary between SRX Series devices. In addition, some SRX Series devices have interface while others use a revenue (network interface) port for Ethernet based management. When running a factory default configuration SRX 300 and 500 Series devices typically provide DHCP services on specific network interface ports that are enabled for host management access.

On SRX Series devices with a dedicated management interface, DHCP services may or may not be present in the factory default. Some devices provide DHCP server functions on the dedicated management interface (fxp0). When using a device that does not offer DHCP services, for example an SRX5400, you must ensure the management device has a compatible IP address. This address can be manually assigned or be allocated by an external DHCP server on the management network.

Table 1 on page 4 provides the factory defaults relating to J-Web access for SRX Series devices. If your SRX Series device is not listed, refer to the corresponding hardware guide for details on the factory defaults.

Table 1: SRX Series Firewall Factory Defaults Relating to J-Web Access

SRX Series Firewall	Management Interface	DHCP Server Ports	DHCP Subnet	J-Web Server IP
SRX300, SRX320	ge-0/0/1 through ge-0/0/6	ge-0/0/1 through ge-0/0/6	192.168.1.0/24	192.168.1.1
SRX340, SRX345	MGMT/fxp0	fxp0	192.168.1.0/24	192.168.1.1
		ge-0/0/1 through ge-0/0/14	192.168.2.0/24	192.168.2.1
SRX380	MGMT/fxp0	fxp0	192.168.1.0/24	192.168.1.1
		ge-0/0/1 through ge-0/0/18	192.168.2.0/24	192.168.2.1

Table 1: SRX Series Firewall Factory Defaults Relating to J-Web Access *(Continued)*

SRX Series Firewall	Management Interface	DHCP Server Ports	DHCP Subnet	J-Web Server IP
SRX550 HM	ge-0/0/1 through ge-0/0/5	ge-0/0/1 through ge-0/0/5	192.168.1.0/24 through 192.168.5.0/24	192.168.1.1 through 192.168.5.1
SRX1500	MGMT/fxp0	ge-0/0/1	192.168.2.0/24	192.168.2.1
SRX4100, SRX4200	MGMT/fxp0	NA	NA	192.168.1.1
SRX4600	MGMT/fxp0	xe-1/1/1	NA (no DHCP address pool in the default configuration)	192.168.1.1
SRX5400, SRX5600, SRX5800	MGMT/fxp0	NA	NA	192.168.1.1
vSRX	fxp0	NA	NA	NA

To log into the J-Web interface on a new device:

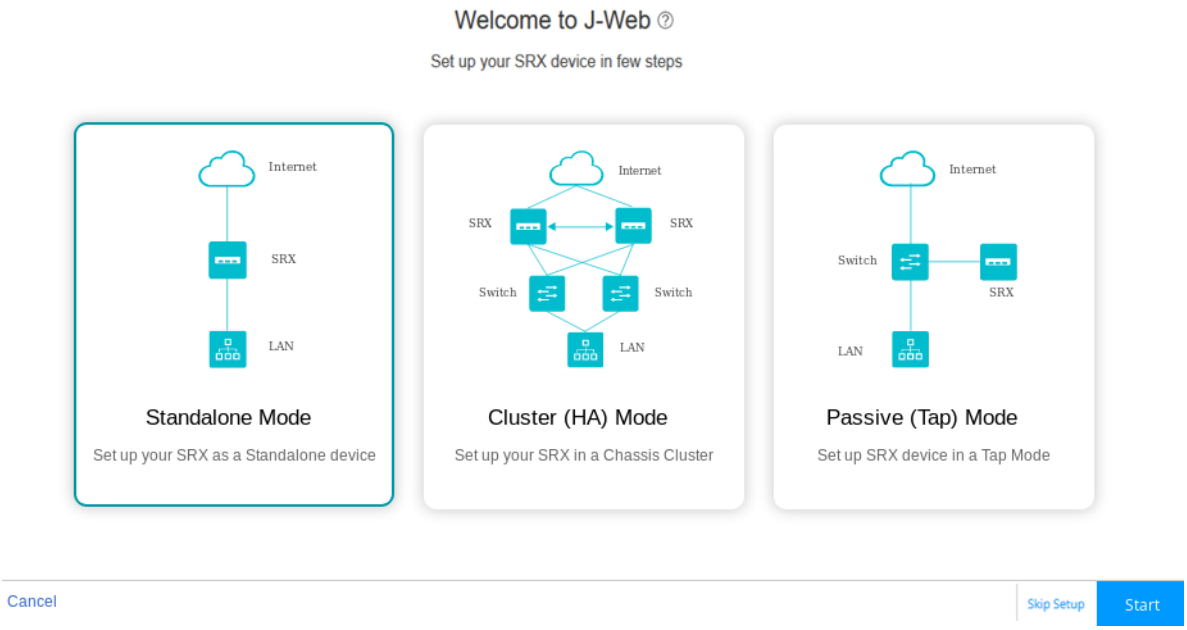
1. Connect the appropriate Ethernet network port on your device to the Ethernet port on the management device (laptop or PC), using an RJ-45 cable. See Table 1 on page 4.
2. If you are using an SRX Series device that provides DHCP services for the management device, confirm that the management device successfully acquires an IP address from the SRX Series device. When using an SRX Series device that does not provide DHCP services for the management device, you must manually configure the management device with a compatible IP address. See Table 1 on page 4.
3. Open a browser and enter **https:// *<IP address>*** in the address bar.

   Where, *<IP address>* is the IP address of the SRX Series device.

> **NOTE**: In a factory default configuration, a self-signed certificate is used to support the HTTPS connection. You can safely accept the security exception to perform initial configuration.

As the device is running a factory default configuration, the J-Web Setup Wizard screen opens. See Figure 1 on page 6.

Figure 1: J-Web Setup Wizard Page



Two examples are given to better illustrate the use of the information in Table 1 on page 4:

a. You have an SRX380 device:

   i. You connect your management PC, which is configured for DHCP address assignment, to the **fxp0** port, or to port **ge-0/0/1** through **ge-0/0/18**.

   ii. If connected to the fxp0 port, you access J-Web at **https://192.168.1.1**.

   iii. If connected to ge-0/0/1 through ge-0/0/18, you access J-Web at **https://192.168.2.1**.

b. You have an SRX5400 device:

   i. You connect your management PC, which is statically configured with an IP address from 192.168.1.0/24 subnet, to the **fxp0** port.

> **NOTE**: The static IP address assignment cannot use 192.168.1.1 for fxp0 on the management subnet as the SRX Series device uses this IP address.

   ii. You access J-Web at **https://192.168.1.1**.

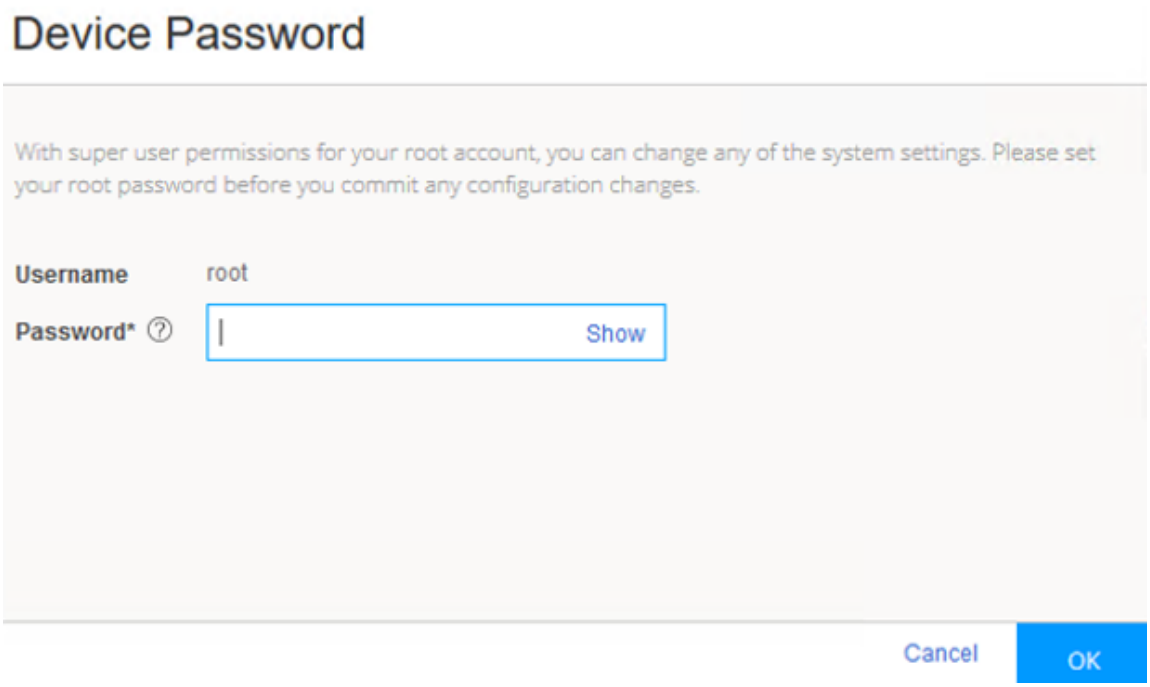
After a successful user login, J-Web opens the **Basic settings** page.

4. Optional. If you do not want to perform the initial configuration, then:

   a. Click **Skip Setup**.

      The J-Web Device Password screen appears. See Figure 2 on page 7.

      Figure 2: Device Password

   b. Enter the root password.

   c. Click **OK**.

      The password is committed to the device and the J-Web login page appears.

   d. Enter the username and password again and click **Log In**.

      The J-Web application window appears.

      NOTE: You can choose **Device Administration** > **Reset Configuration** through the J-Web menu to reset and reconfigure the SRX Series device.

Congratulations! Now that you have access to the J-Web interface, you are ready to use J-Web to configure, manage, and monitor your SRX Series Firewall.

- Get a quick overview of the J-Web user interface: "Explore J-Web" on page 39
- Use the setup wizard for initial configuration: "The J-Web Setup Wizard" on page 8
- Access the device dashboard: "Dashboard Overview" on page 53
- Monitor device traffic: "Monitor Traffic Map" on page 96
- Configure your device: "Configure Basic Settings" on page 132
- Watch a Learning Bytes video showing J-Web usage on a vSRX: SRX J-Web Access

The J-Web Setup Wizard

IN THIS SECTION

Configure SRX Series Firewalls Using the J-Web Setup Wizard

Using the Setup wizard, you can perform step-by-step configuration of a services gateway that can securely pass traffic.

For information on how to start and access the J-Web user interface, see "Access the J-Web User Interface" on page 3.

You can choose one of the following setup modes to configure the services gateway:

- Standalone mode—Configure your SRX Series device to operate in a standalone mode. In this mode, you can configure basic settings such as device credentials, time, management interface, zones and interfaces, and DNS servers and default gateways.
- Cluster (HA) mode—Configure your SRX Series device to operate in a cluster (HA) mode. In the cluster mode, a pair of devices are connected together and configured to operate like a single node, providing device, interface, and service level redundancy.

> **NOTE**: You cannot configure Standalone or Passive mode when your device is in the HA mode.

- Passive (Tap) mode—Configure your SRX Series device to operate in a TAP mode. TAP mode allows you to passively monitor traffic flows across a network. If IPS is enabled, then the TAP mode inspects the incoming and outgoing traffic to detect the number of threats.

> **NOTE**: SRX5000 line of devices, SRX4600, and vSRX devices do not support the passive mode configuration.

To help guide you through the process, the wizard:

- Determines which configuration tasks to present to you based on your selections.
- Flags any missing required configuration when you attempt to leave a page.

To configure SRX Series devices using the J-Web Setup wizard:

1. Select the configuration mode that you want to setup and click **Start**.

   The Setup Wizard page appears.

2. For standalone and passive (Tap) modes, complete the configuration according to the guidelines provided in Table 3 on page 22.

   If you select Cluster (HA) Mode, for the configuration information see "Configure Cluster (HA) Setup" on page 151.

   > **NOTE**: The root password is mandatory in the setup wizard. All other options are optional. In the passive mode, configuration of the management interface, Tap interface, and services are mandatory.

3. Review the configuration details. If you want to change the configuration, click **Edit Configuration**, else click **Finish**.

   Wait till the configuration is committed. A successful message is displayed once the entire configuration is committed to the device.

   > **NOTE**:

- If the commit fails, J-Web displays you the error message received from CLI and you remain on the wizard's last page. Check over your configuration and make changes as necessary so that the commit succeeds.
- For SRX300 line of devices and SRX550M devices in passive mode, an additional message is displayed about the device reboot if you have enabled Juniper ATP Cloud or Security Intelligence services. For other SRX Series Firewalls, the device will not reboot.

4. Read if any instructions are available and then click **Open J-Web Login Page**.

   The J-Web Login page appears.

5. Enter the root username and password and click **Log In**.

   Launch Pad screen appears until the J-Web UI is loaded. See "J-Web: A First Look" on page 40.

Example: J-Web Wizard for Standalone Mode

In this section, we'll show you a typical J-Web setup wizard workflow for standalone mode operation. The J-Web interface is updated and modified over time. The below example is representative of the typical workflow. This specific example is based on the Junos 21.3R1 release.

Table 2 on page 10 provide details on the configuration parameters used for initial setup.

Table 2: Standalone Setup Wizard Parameters

Configuration Parameter	Example Value
Root Password	*"Sample_psswd_for_doc-only!"*
Hostname	SRX-300
Management interface	ge-0/0/1
Management IP and CIDR	10.102.70.79/24
Access Protocols	HTTPS, SSH, Ping
Static route for management	10.0.0.0/8, next hop 10.102.70.254

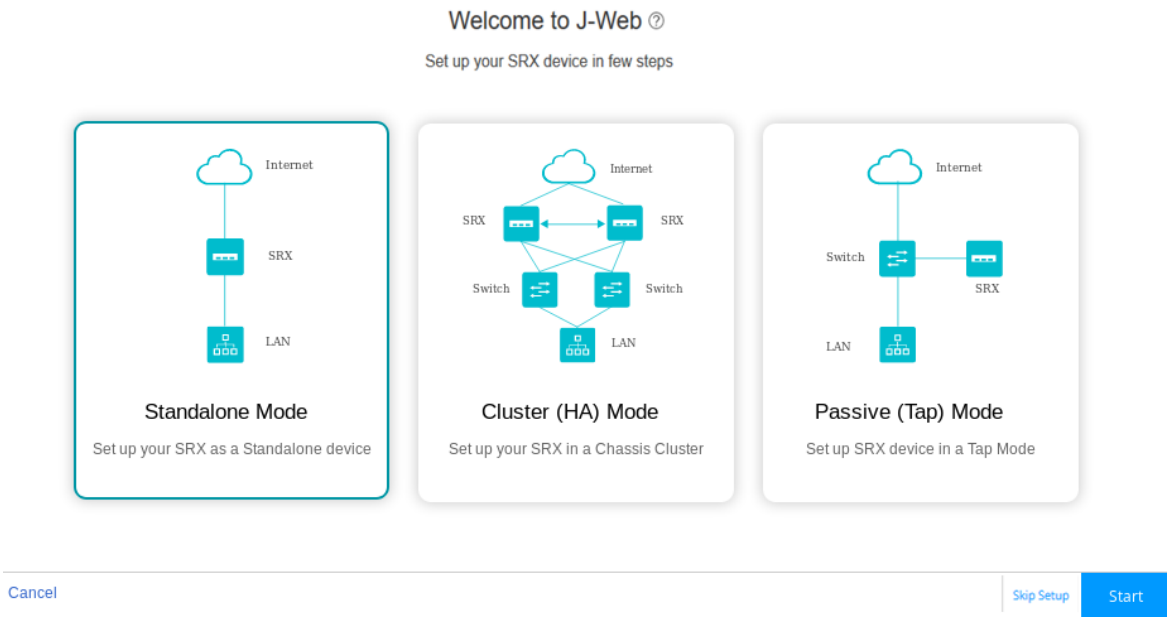
Table 2: Standalone Setup Wizard Parameters *(Continued)*

Configuration Parameter	Example Value
NTP and DNS	• NTP: north-america.pool.ntp.org • DNS: 8.8.8.8 and 8.8.4.4 • Time zone: PST/Los Angeles
Remote access	SSH with root login allowed
Non root user (Admin/super user account)	user "lab", password *"Sample_psswd_for_doc-only!"*
Security Policy	Default

Refer to "Access the J-Web User Interface" on page 3 for information on how to access the J-Web interface. This example is based on an SRX300. Based on the information in Table 1 on page 4, the management device is set for DHCP is and is attached to the ge-0/0/1 interface. When running a factory default configuration, the ge-0/0/1 interface is configured as a DCHP server and assigns an address to the PC from the 192.168.1.0/24 subnet. To access J-Web in this scenario, you point the browser to https://192.168.1.1.

1. We begin at the J-Web setup wizard screen. You click on the option for **Standalone Mode** and then on the **Start button**.

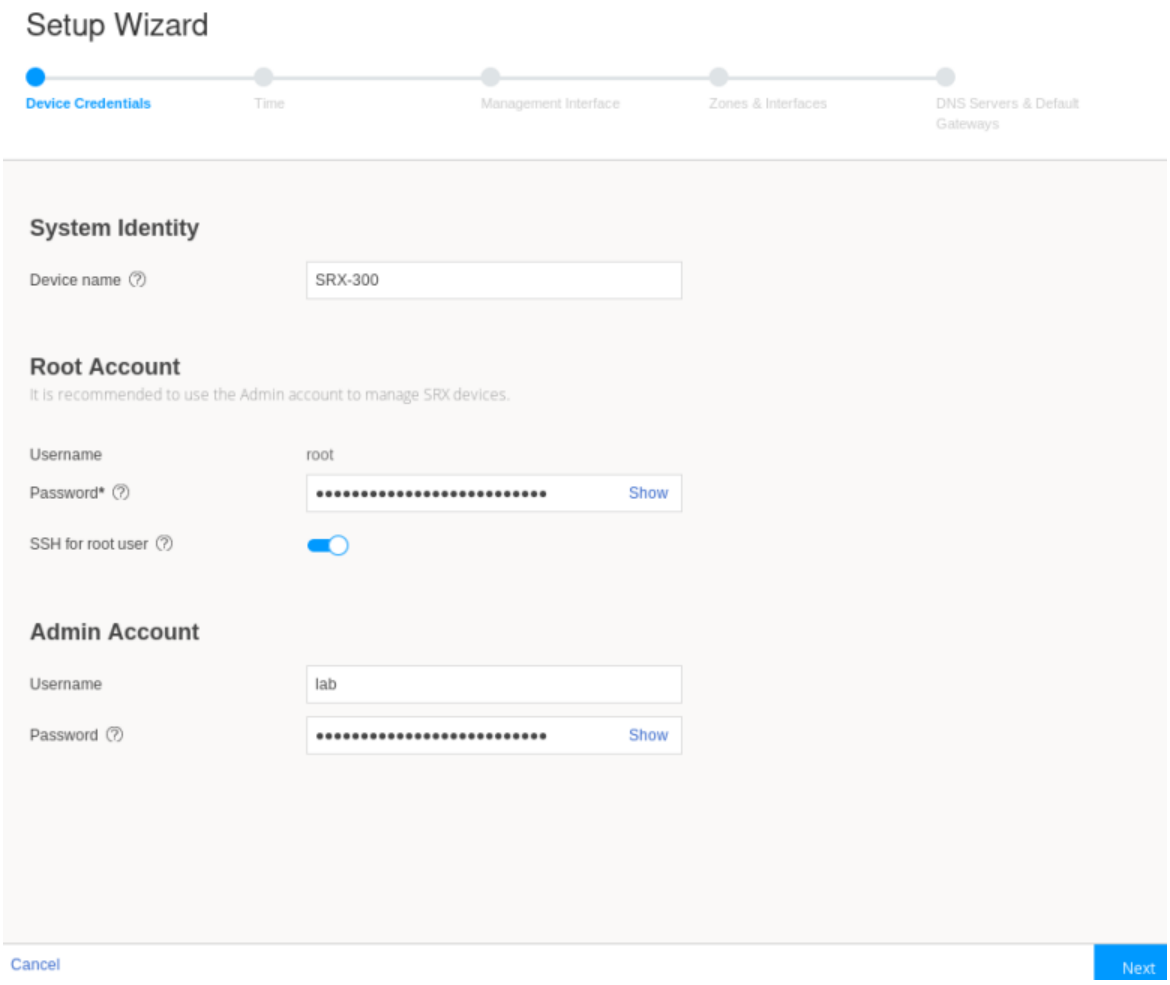
Figure 3: J-Web Setup Wizard Modes



2. Configure the device name, root user, and non-root (administrator) user login information on the Device Credentials page.

> **NOTE**: Enable **SSH for root user**.

Figure 4: J-Web Setup Wizard Device Credentials

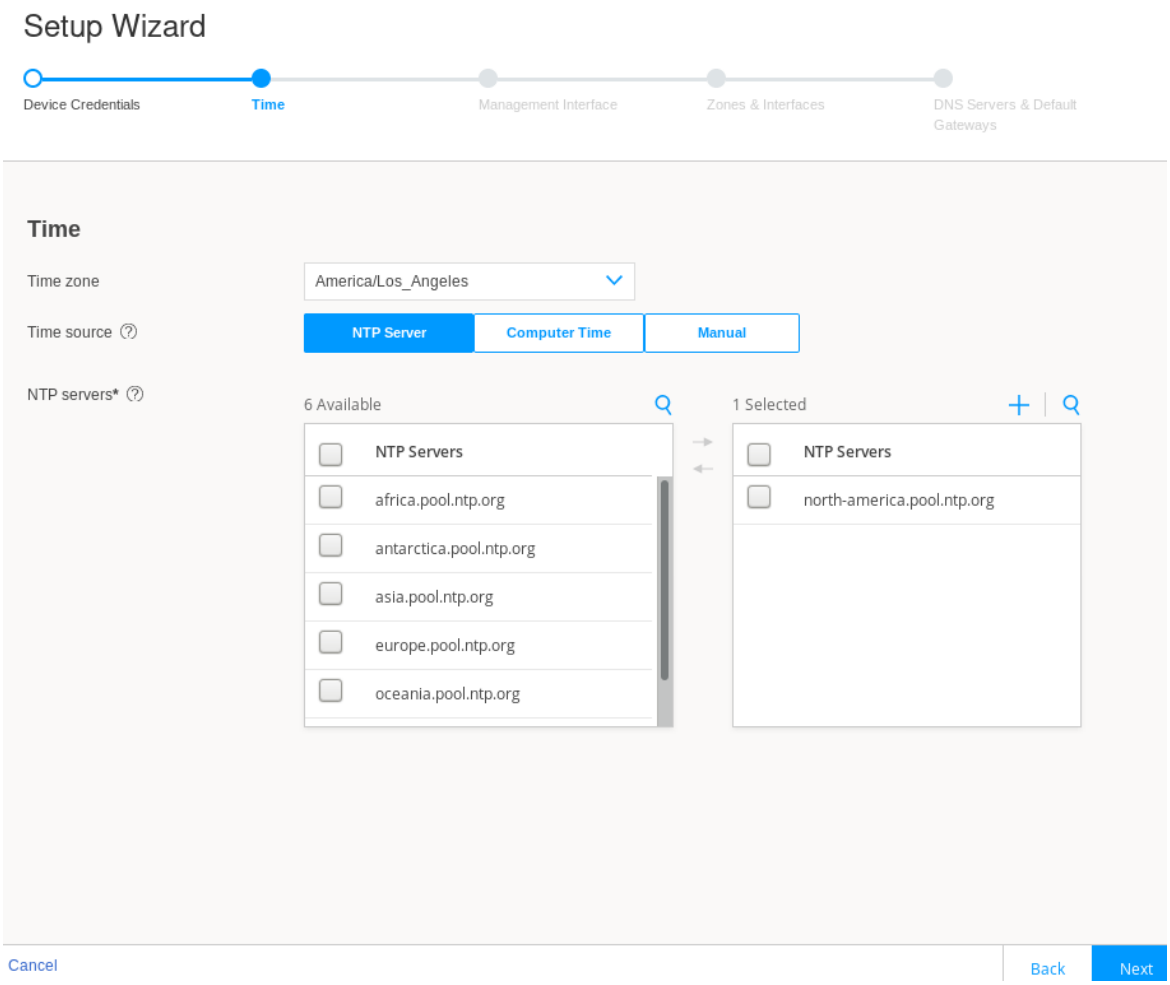


3. Click **Next**.

   The **Time** page opens.

4. Configure the timezone, time source, and in the case of NTP, the desired server(s).

Figure 5: J-Web Setup Wizard Time Servers

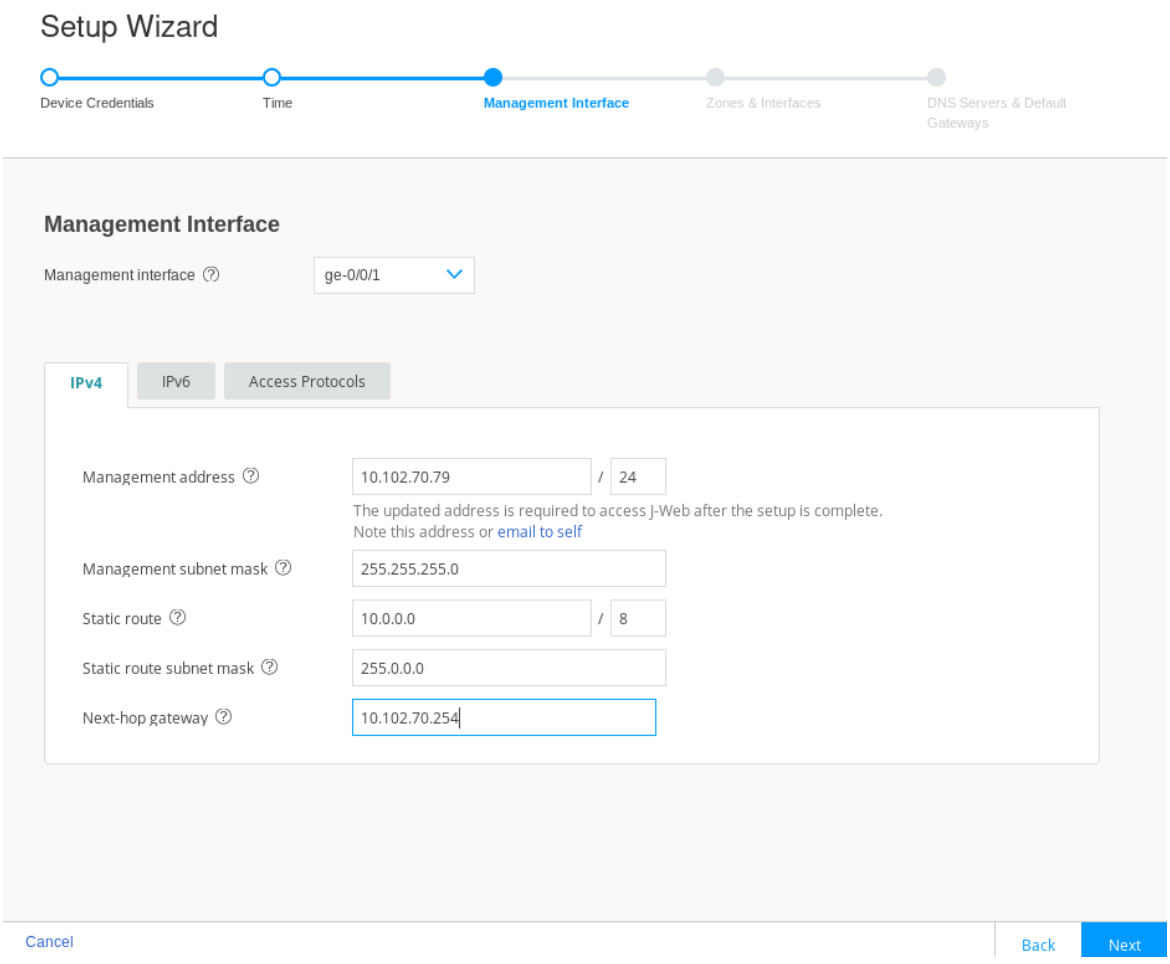


5. Click **Next**.

   The **Management Interface** page opens.

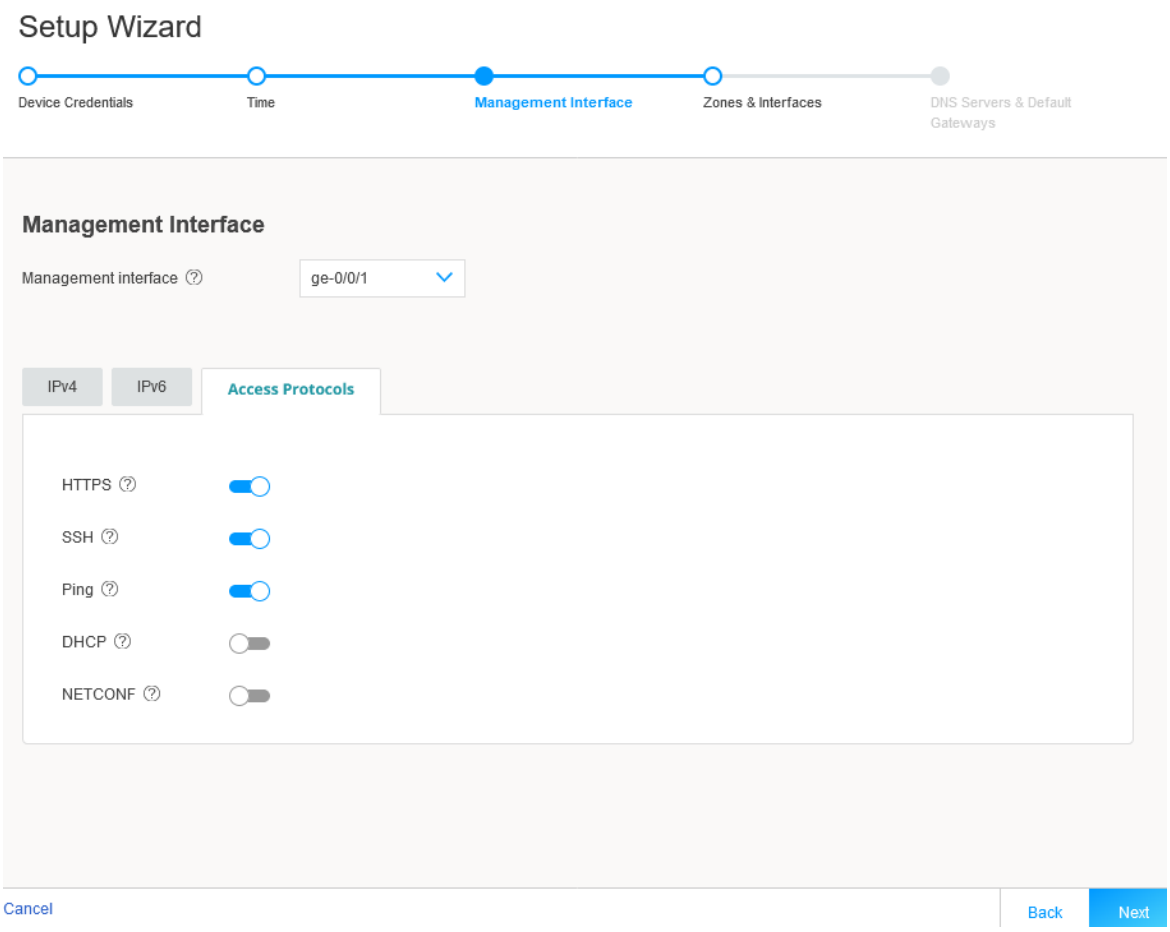
6. Again, this setup example is based on a SRX 300 series device. This SRX Series Firewall does not have a dedicated management interface. In many cases, their role in branch offices results in their being managed remotely through the WAN interface (ge-0/0/0). On larger SRX Series Firewalls, a dedicated management interface (fxp0) is provided for attachment to an out-of-band (OOB) management network. In this example, you configure the ge-0/0/1 interface as a dedicated OOB management interface.

Figure 6: J-Web Setup Wizard Management Interface



Before continuing, you click on the **Access Protocols** tab to confirm that HTTPS, SSH, and Ping (ICMP echo) are permitted on the management interface.

Figure 7: J-Web Setup Wizard Access Protocols

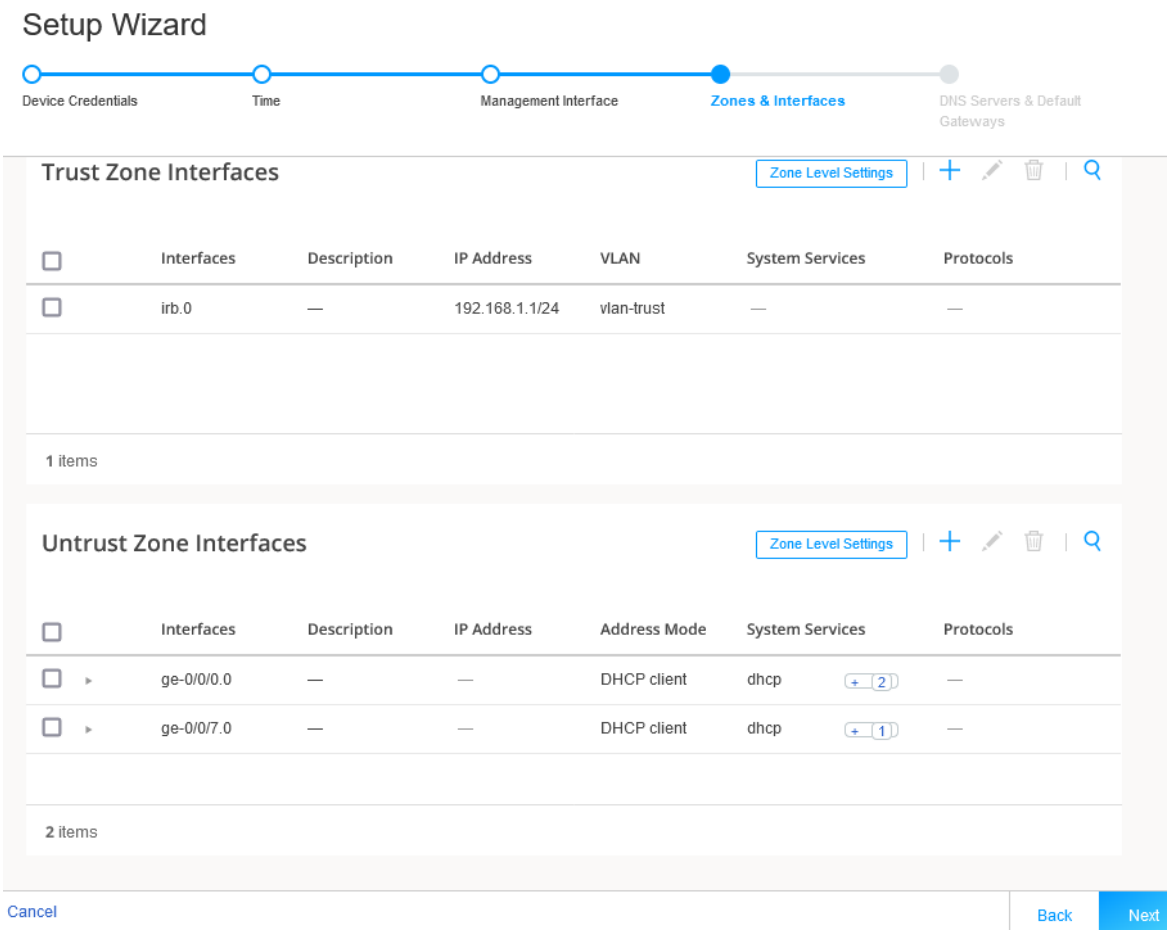


7. Click **Next**.

   The **Zones & Interfaces** page opens.

8. In this example you maintain the factory default security policy. Recall, you can always use J-Web to later modify all aspects of the configuration, to include security, after you complete the initial setup.

Figure 8: J-Web Setup Wizard Security Zones

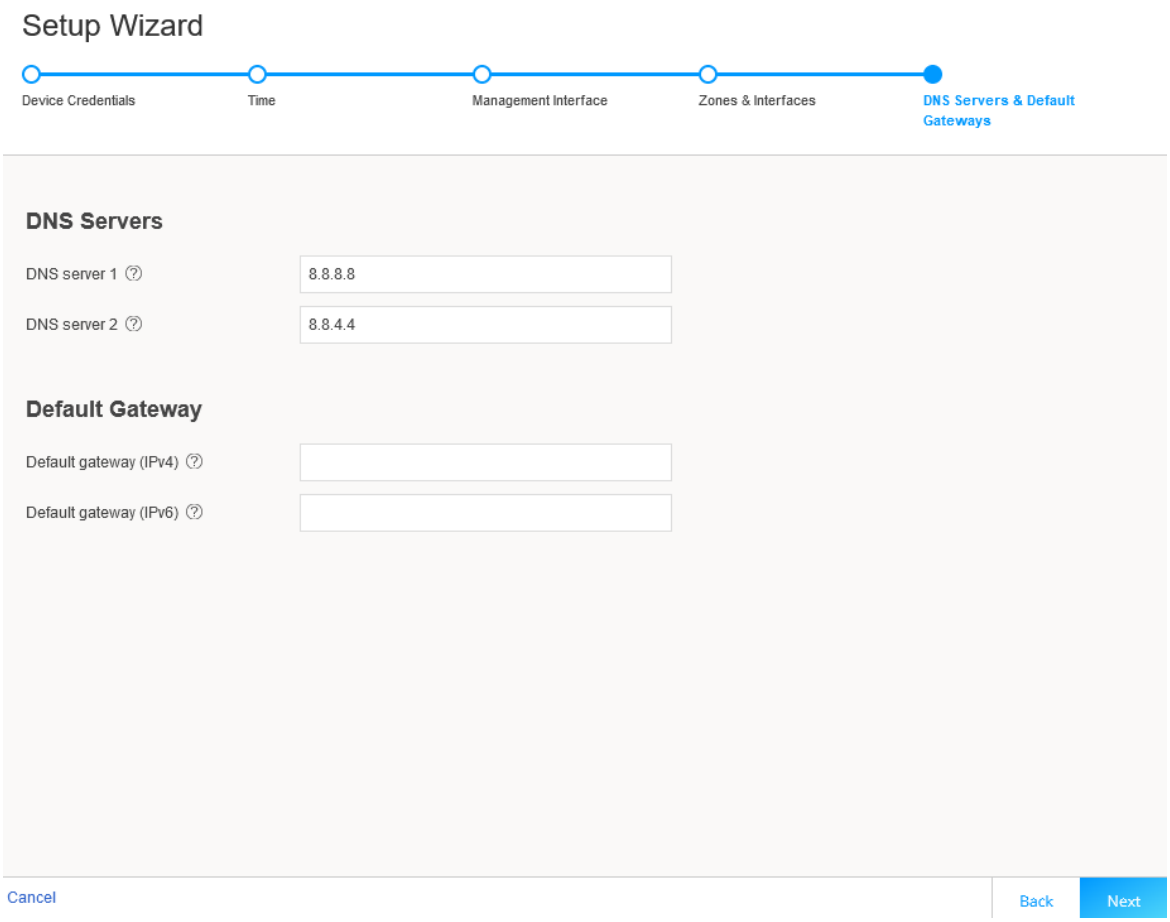


9. Click **Next**.

   The **DNS Servers & Default Gateways** page opens.

10. Configure a public DNS server IP and leave the default gateway fields blank. If desired, you can add default routes to access other networks that should be reachable over the management interface.

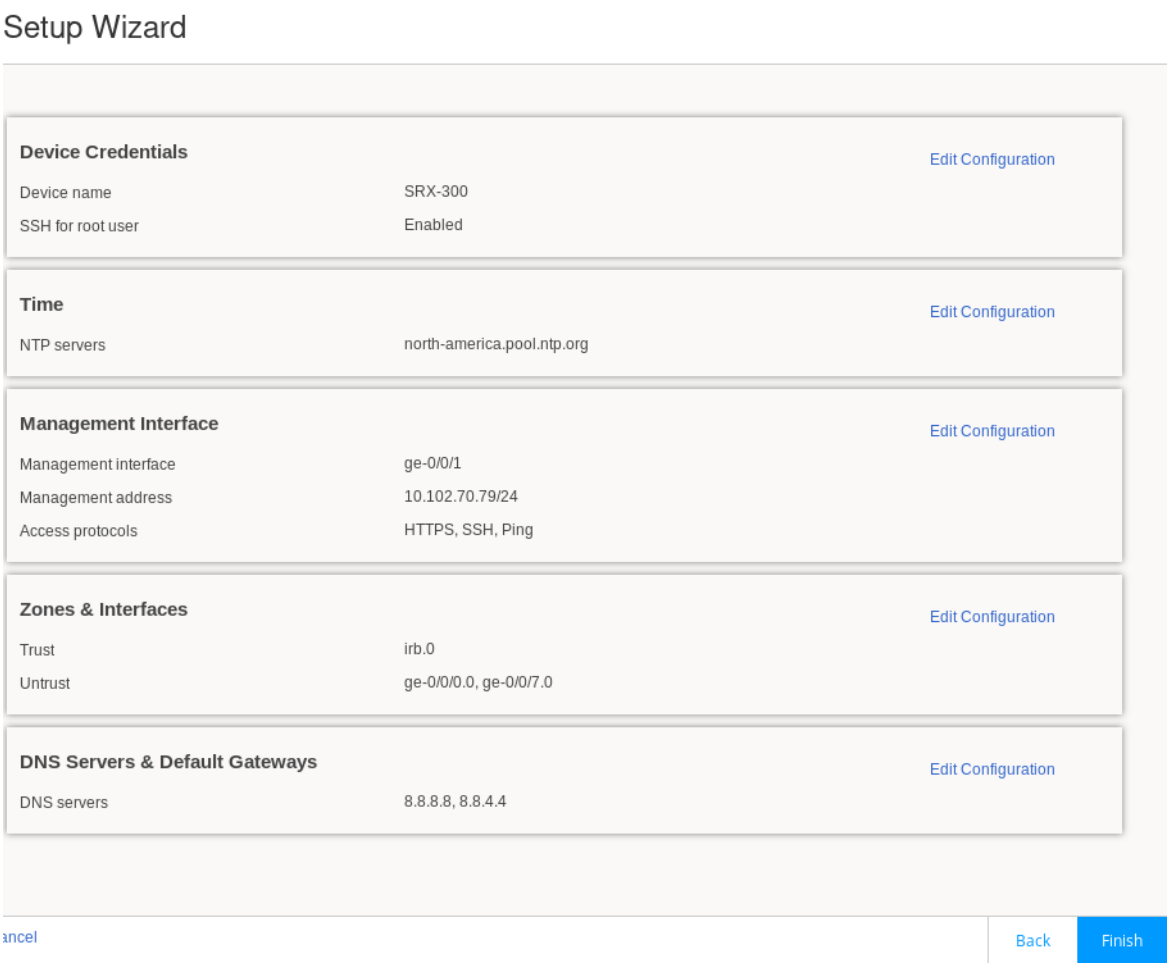
Figure 9: J-Web Setup Wizard DNS and Default Gateways



11. Click **Next**.

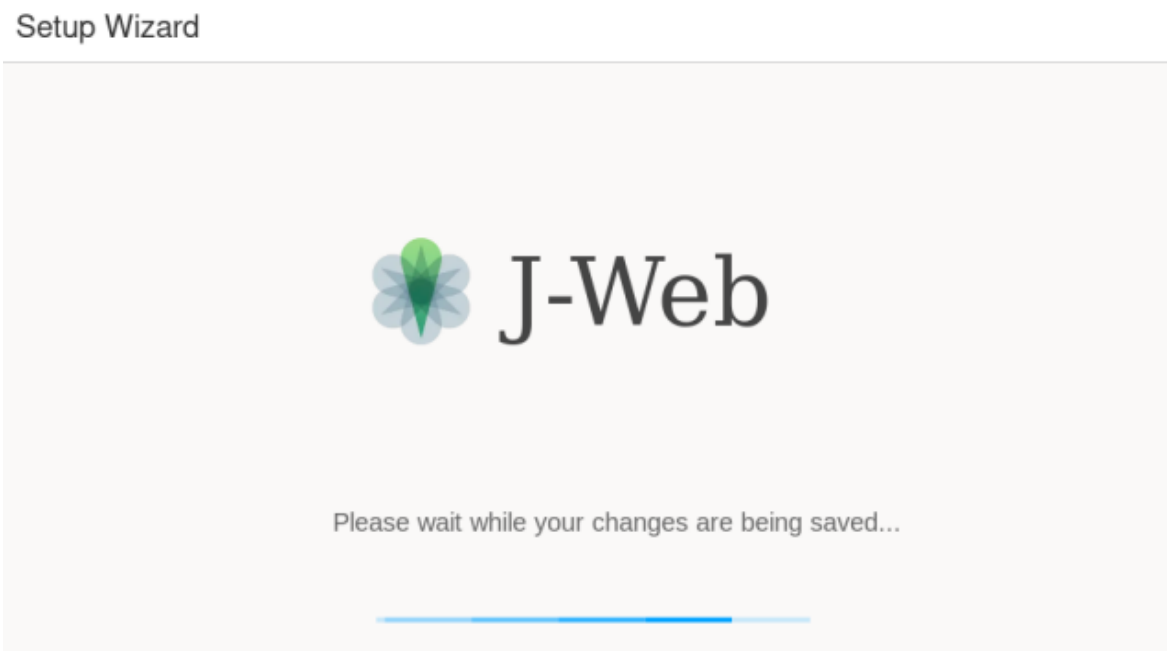
The **Setup Wizard** opens. This page summarizes your configuration. If desired, you use the **Edit Configuration** option to make changes.

Figure 10: J-Web Setup Wizard Summary



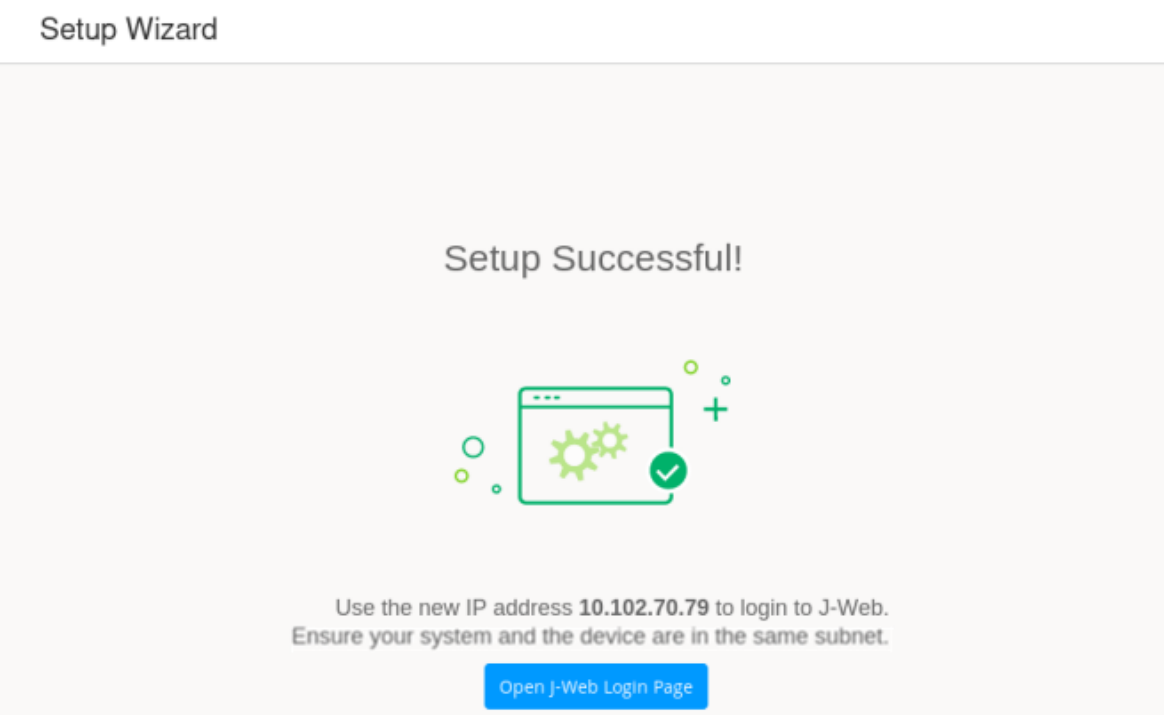
12. When satisfied with the configuration, click on **Finish**. The Setup Wizard displays a status page to indicate the initial configuration is being pushed to the SRX Series Firewall.

Figure 11: J-Web Setup Wizard Configuration Push



In a few moments, the **Setup Successful** page is displayed. Congratulations! Your SRX Series Firewall is remotely accessible and is ready for ongoing management using the J-Web interface.

Figure 12: J-Web Setup Wizard Successful



NOTE: Recall that in this SRX-300 based example the management device is directly connected to the SRX on the ge-0/0/1 port. You performed initial configuration using a 192.168.1.0/24 address that was assigned by the SRX Series device using DHCP.

Using the setup wizard, you configured the ge-0/0/1 interface as a dedicated management interface and assigned a static IP address of 10.102.70.89/24. As a result, the ge-0/0/1 interface no longer functions as a DHCP server.

Once the new configuration is activated, you must ensure the management device is configured with a compatible IP address if it remains directly connected to the ge-0/0/1 interface. You log in back into J-Web using https://10.102.70.89.

Congratulations! You have completed initial setup using J-Web. Keep going by visiting the below links:

- Get a quick overview of the J-Web user interface: "Explore J-Web" on page 39
- Access the device dashboard: "Dashboard Overview" on page 53
- Monitor device traffic: "Monitor Traffic Map" on page 96
- Configure your device: "Configure Basic Settings" on page 132
- Use the Getting Started panel: Security J-Web Getting Started

J-Web Setup Wizard Parameters

This section serves as a reference for the mode specific parameters that you can configure using the J-Web Setup Wizard. Table 3 on page 22 provide details of the parameters that can be configured in the standalone and passive (Tap) modes. For details on parameters supported in cluster (HA) mode, see "Configure Cluster (HA) Setup" on page 151.

Table 3: Setup Wizard Configuration

Field	Action
Device Credentials	
System Identity	
Device name	Enter a hostname. You can use alphanumeric characters, special characters such as the underscore (_), the hyphen (-), or the period (.); the maximum length is 255 characters.
Root Account	
Username	Displays the root user. **NOTE**: We recommend that you do not use root user account as a best practice to manage your devices.
Password	Enter a password. You can use alphanumeric characters and special characters; the minimum length is six characters.
SSH for root user	Enable this option to allow the root login (to the device) using SSH.
Admin Account	
Username	Enter the admin username to manage the device.
Password	Enter the admin password.

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
Time Configuration	
Time	
Time zone	Select a time zone from the list.
Time source	Select either NTP server, computer time, or Manual to configure the system time: • **NTP Server > NTP servers**—Select the NTP server in the Available column and move to the selected column using the right arrow. Once the system is connected to the network, the system time is synced with the NTP server time. In addition, to add a new NTP server, click **+** and enter a hostname or IP address of the NTP server and click **OK**. **NOTE**: If you want to add more NTP servers, go to Device Administration > Basic Settings > Date & Time Details through the J-Web menu. • **Computer Time** > **Computer time**—Device automatically synchronizes with your computer time only during the setup. • **Manual** > **Date and time**—Select the date and time (in MM-DD-YYYY and HH:MM:SS 24-hour format) to configure the system time manually.
Management Interface Configuration	
Management Interface **NOTE**: If you change the management IP address and click **Next**, a warning message appears on the Management Interface page that you need to use the new management IP address to log in to J-Web because you may lose the connectivity to J-Web.	

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
Management interface	Select an interface from the list. If fxp0 port is your device's management port, then the fxp0 port is displayed. You can change it as required or you can select **None** and proceed to the next page. **NOTE**: • You can choose the revenue port as management port if your device does not support the fxp0 port. Revenue ports are all ports except fxp0 and em0. • If you are in the Standalone mode, you can choose **None** for the management interface and click **Next** to proceed to the next screen. • If you are in the Passive (Tap) mode, it is mandatory to configure a management port. J-Web needs a management port for viewing generated report.
IPv4 **NOTE**: Click **email to self** to get the newly configured IPv4 or IPv6 address to your inbox. This is useful if you lose connectivity when you change the management IP address to another network.	
Management address	Enter a valid IPv4 address for the management interface. **NOTE**: If fxp0 port is your device's management port, then the fxp0 port's default IP address is displayed. You can change it if required.
Management subnet mask	Enter a subnet mask for the IPv4 address. If you have changed the management address, use the new IP address to access J-Web.
Static route	Enter an IPv4 address for the static route to route to the other network devices.
Static route subnet mask	Enter a subnet mask for the static route IPv4 address.

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
Next hop gateway	Enter a valid IPv4 address for the next hop.
IPv6	
Management access	Enter a valid IPv6 address for the management interface.
Management subnet prefix	Enter a subnet prefix length for the IPv6 address.
Static route	Enter an IPv6 address for the static route if required to reach the device through the management interface.
Static route subnet prefix	Enter a subnet prefix length for the static route IPv6 address.
Next hop gateway	Enter a valid IPv6 address for the next hop.
Access Protocols **NOTE**: This option is available for all the ports except fxp0.	
HTTPS	This option is enabled by default.
SSH	This option is enabled by default.
Ping	Enable this option for ping service.
DHCP	Enable this option for DHCP service.
NETCONF	Enable this option for NETCONF service.
Zones & Interfaces	

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
Security Policy **NOTE**: This option is available only for the Standalone mode. For the Passive (Tap) mode, this option is available under Tap Settings.	
From Zone	Name of the source zone. In the standalone mode, permits all traffic from the trust zone.
To Zone	Name of the destination zone. In standalone mode, permits all traffic from the trust zone to the untrust zone.
Source	Name of the source address (not the IP address) of a policy.
Destination	Name of the destination address.
Application	Name of a preconfigured or custom application of the policy match.
Action	Action taken when a match occurs as specified in the policy.
Zones —Displays the available trust and untrust zones configuration.	
Trust Zone Interfaces **NOTE**: This option is available only for the Standalone mode.	
Add Trust Zone Interface	Click **+** to add trust zone interface. For more information on the fields, see Table 4 on page 32.
Edit Trust Zone Interface	Select an interface and click the pencil icon at the right corner of the table to modify the configuration.

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
Delete Trust Zone Interface	Select an interface and click the delete icon at the top right corner of the table. A confirmation window appears. Click **Yes** to delete the selected interface or click **No** to discard.
Search Trust Zone Interface	Click the search icon at the right corner of the table to quickly locate a zone or an interface.
Detailed View Trust Zone Interface	Hover over the interface name and click the Detailed View icon to view the zone and interface details.
Trust Zone Interfaces—Zone Level Settings	
Zone name	View the trust zone name populated from your device factory default settings. **NOTE**: For standalone mode, trust and untrust zones are created by default even if these zones are not available in the factory default settings.
Description	Enter the description for trust zone.
System services	Enable this option for the types of traffic that can reach the device on a particular interface. By default, this option is enabled. You can disable if required.
Protocols	Enable this option to configure the device to perform stateful network traffic filtering on network packets using network traffic protocols (for example, TCP and UDP). By default, this option is enabled. You can disable if required.
Application tracking	Enable this option to collect byte, packet, and duration statistics for application flows in the specified zone.

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
Source identity log	Enable this option for the device to log the user identity information based on the source zone configured in the security policy.
Untrust Zone Interfaces	
Add Untrust Zone Interface	Click **+** to add untrust zone interface. For more information on the fields, see Table 5 on page 38.
Edit Untrust Zone Interface	Select an interface and click the pencil icon at the right corner of the table to modify the configuration.
Delete Untrust Zone Interface	Select an interface and click the delete icon at the top right corner of the table. A confirmation window appears. Click **Yes** to delete the selected interface or click **No** to discard.
Search Untrust Zone Interface	Click the search icon at the right corner of the table to quickly locate a zone or an interface.
Detailed View Untrust Zone Interface	Hover over the interface name and click the Detailed View icon to view the zone and interface details.
Untrust Zone Interfaces—Zone Level Settings	
Zone name	View the untrust zone name populated from your device factory default settings. **NOTE**: For standalone mode, trust and untrust zones are created by default even if these zones are not available in the factory default settings.
Description	Enter the description for untrust zone.

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
Application tracking	Enable this option to collect byte, packet, and duration statistics for application flows in the specified zone.
Source identity log	Enable this option for the device to log the user identity information based on the source zone configured in the security policy.
DNS Servers & Default Gateways	
DNS Servers	
DNS server 1	Enter the IPv4 or IPv6 address of the primary DNS.
DNS server 2	Enter the IPv4 or IPv6 address of the secondary DNS.
Default Gateway	
Default gateway (IPv4)	Enter the IPv4 address of the next possible destination for any network.
Default gateway (IPv6)	Enter the IPv6 address of the next possible destination for any network.
Tap Settings **NOTE**: This option is available only for the Passive (Tap) mode.	
Tap Settings	
Tap interface	Select the interface from the list.
IP-IP tunnel inspection	Enable this option for the SRX Series device to inspect pass through traffic over an IP-IP tunnel.

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
GRE tunnel inspection	Enable this option for the SRX Series device to inspect pass through traffic over a GRE tunnel.
Security Policy & Advanced Services **NOTE**: Your device must have internet connectivity to use IPS, Web filtering, Juniper ATP Cloud, and Security threat intelligence services.	
From Zone	Name of the source zone. In the Tap mode, permits all traffic from the tap zone.
To Zone	Name of the destination zone. In the Tap mode, permits all traffic from the TAP zone to the TAP zone.
Source	Name of the source address (not the IP address) of a policy.
Destination	Name of the destination address.
Application	Name of a preconfigured or custom application of the policy match.
Action	Action taken when a match occurs as specified in the policy.
UTM	
UTM	Enable this option for configuring UTM services.
License	Enter UTM license key and click **Install License** to add a new license. **NOTE**: • Use a blank line to separate multiple license keys. • To use UTM services, your device must have internet connectivity from a revenue interface.

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
UTM type	Select an option to configure UTM features: • Web Filtering • Antivirus • Antispam
Web filtering type	Select an option: • Enhanced—Specifies that the Juniper Enhanced Web filtering intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). • Local—Specifies the local profile type.
IPS	
IPS	Enable this option to install the IPS signatures.
License	Enter the license key and click **Install License** to add a new license. **NOTE**: The installation process may take few minutes.
IPS signature	Click **Browse** to navigate to the IPS signature package folder and select it. Click **Install** to install the selected IPS signature package. **NOTE**: You can download the IPS signature offline package at https://support.juniper.net/support/downloads/.
ATP Cloud	

Table 3: Setup Wizard Configuration *(Continued)*

Field	Action
ATP Cloud	Enable this option to use Juniper ATP Cloud services. **NOTE**: After the Juniper ATP Cloud configuration is pushed, only the SRX300 line of devices and SRX550M devices are rebooted. Your device must have internet connectivity to enable Juniper ATP Cloud enrollment process through J-Web.
Security Intelligence	
Security intelligence	Enable this option to use Security intelligence services. **NOTE**: After the Security Intelligence configuration is pushed, only the SRX300 line of devices and SRX550M devices are rebooted. Your device must have internet connectivity to enable Juniper ATP Cloud enrollment process through J-Web.
User Firewall	
User Firewall	Enable this option to use user firewall services.
Domain name	Enter a domain name for Active Directory.
Domain controller	Enter domain controller IP address.
Username	Enter a username for administrator privilege.
Password	Enter a password for administrator privilege.

Table 4: Add Trust Zone

Field	Action
General	

Table 4: Add Trust Zone *(Continued)*

Field	Action
Type (family)	• Select **Switching**. Fields for switching interface are: **NOTE**: This option will be available for only SRX300 line of devices, SRX550M, and SRX1500 devices. For SRX5000 line of devices, SRX4100, SRX4200, SRX4600, and vSRX devices, the Type (family) field is not available. • **IRB interface Unit**—Enter the IRB unit. • **Description**—Enter the description for the interface. • Select **Routing**. Fields for routing interface are: For SRX5000 line of devices, SRX4100, SRX4200, SRX4600, and vSRX devices, the Type (family) field is not available. • **Interface**—Select an option from list. • **Interface unit**—Enter the Inet unit. **NOTE**: VLAN tagging is enabled automatically if the interface unit is higher than zero. • **Description**—Enter the description for the interface. • **VLAN ID**—Enter the VLAN ID. **NOTE**: VLAN ID is mandatory if the interface unit is higher than zero.
Interfaces	Select an interface from the Available column and move it to the Selected column. **NOTE**: This option is available only for the Switching family type.
VLAN **NOTE**: This option is available only for the Switching family type.	
Name	Enter a unique name for the VLAN.
VLAN ID	Enter the VLAN ID.

Table 4: Add Trust Zone *(Continued)*

Field	Action
IPv4	
IPv4 address	Enter a valid IPv4 address for the switching or the routing interface.
Subnet mask	Enter a subnet mask for the IPv4 address.
IPv6	
IPv6 address	Enter a valid IPv6 address for the switching or the routing interface.
Subnet prefix	Enter a subnet prefix for the IPv6 address.
DHCP Local Server	
DHCP local server	Enable this option to configure the switch to function as an extended DHCP local server.
Pool name	Enter the DHCP pool name.
Pool start address	Enter the starting IPv4 address of the DHCP server pool address range. This address must be within the IPv4 network.
Pool end address	Enter the ending IPv4 address of the DHCP server pool address range. This address must be within the IPv4 network. **NOTE**: This address must be greater than the address specified in Pool start address.
Propagate settings from	Select an option from the list. Propagation of TCP/IP settings (such as, DNS and gateway address) received on the device interface acting as DHCP client.
Services & Protocols	

Table 4: Add Trust Zone *(Continued)*

Field	Action
System Services	Select system services from the list in the Available column and then click the right arrow to move it to the Selected column. The available options are: • all—Specify all system services. • any-service—Specify services on entire port range. • appqoe—Specify the APPQOE active probe service. • bootp—Specify the Bootp and dhcp relay agent service. • dhcp—Specify the Dynamic Host Configuration Protocol. • dhcpv6—Enable Dynamic Host Configuration Protocol for IPV6. • dns—Specify the DNS service. • finger—Specify the finger service. • ftp—Specify the FTP protocol. • http—Specify the Web management using HTTP. • https—Specify the Web management using HTTP secured by SSL. • ident-reset—Specify the send back TCP RST IDENT request for port 113. • ike—Specify the Internet key exchange. • lsping—Specify the Label Switched Path ping service. • netconf—Specify the NETCONF Service. • ntp—Specify the network time protocol. • ping—Specify the internet control message protocol. • r2cp—Enable Radio-Router Control Protocol. • reverse-ssh—Specify the reverse SSH Service.

Table 4: Add Trust Zone *(Continued)*

Field	Action
	• reverse-telnet—Specify the reverse telnet Service. • rlogin—Specify the Rlogin service • rpm—Specify the Real-time performance monitoring. • rsh—Specify the Rsh service. • snmp—Specify the Simple Network Management Protocol. • snmp-trap—Specify the Simple Network Management Protocol trap. • ssh—Specify the SSH service. • tcp—encap-Specify the TCP encapsulation service. • telnet—Specify the Telnet service. • tftp—Specify the TFTP • traceroute—Specify the traceroute service. • webapi-clear-text—Specify the Webapi service using http. • webapi-ssl—Specify the Webapi service using HTTP secured by SSL. • xnm-clear-text—Specify the JUNOScript API for unencrypted traffic over TCP. • xnm-ssl—Specify the JUNOScript API Service over SSL.

Table 4: Add Trust Zone *(Continued)*

Field	Action
Protocols	Select protocols from the list in the Available column and then click the right arrow to move it to the Selected column. The available options are: • all—Specifies all protocol. • bfd—Bidirectional Forwarding Detection. • bgp—Border Gateway Protocol. • dvmrp—Distance Vector Multicast Routing Protocol. • igmp—Internet Group Management Protocol. • ldp—Label Distribution Protocol. • msdp—Multicast Source Discovery Protocol. • nhrp- Next Hop Resolution Protocol. • ospf—Open shortest path first. • ospf3—Open shortest path first version 3. • pgm—Pragmatic General Multicast. • pim—Protocol Independent Multicast. • rip—Routing Information Protocol. • ripng—Routing Information Protocol next generation. • router-discovery—Router Discovery. • rsvp—Resource Reservation Protocol. • sap—Session Announcement Protocol. • vrrp—Virtual Router Redundancy Protocol.

Table 5: Add Untrust Zone

Field	Action
General	
Interface	Select an interface from the list.
Interface unit	Enter the interface unit value.
VLAN ID	Enter the VLAN ID. **NOTE**: VLAN ID is mandatory if the interface unit is higher than zero.
Description	Enter the description for the interface.
Address Mode	Select an address mode for the interface. The available options are DHCP Client, PPPoE (PAP), PPPoE (CHAP) and Static IP. **NOTE**: PPPoE (PAP) and PPPoE (CHAP) are not supported for SRX5000 line of devices and if any of the devices are in passive mode.
Username	Enter a username for PPPoE (PAP) or PPPoE (CHAP) authentication.
Password	Enter a password for PPPoE (PAP) or PPPoE (CHAP) authentication.
IPv4 **NOTE**: This option is available only for the Static IP address mode.	
IPv4 Address	Enter a valid IPv4 address for the interface.
Subnet Mask	Enter a subnet mask for the IPv4 address.

Table 5: Add Untrust Zone *(Continued)*

Field	Action
IPv6 **NOTE**: This option is available only for the Static IP address mode.	
IPv6 Address	Enter a valid IPv6 address for the interface.
Subnet Prefix	Enter a subnet prefix for the IPv6 address.
Services & Protocols	
System Services	Select system services from the list in the Available column and then click the right arrow to move it to the Selected column.
Protocols	Select protocols from the list in the Available column and then click the right arrow to move it to the Selected column.

SEE ALSO

Explore J-Web | 39

Explore J-Web

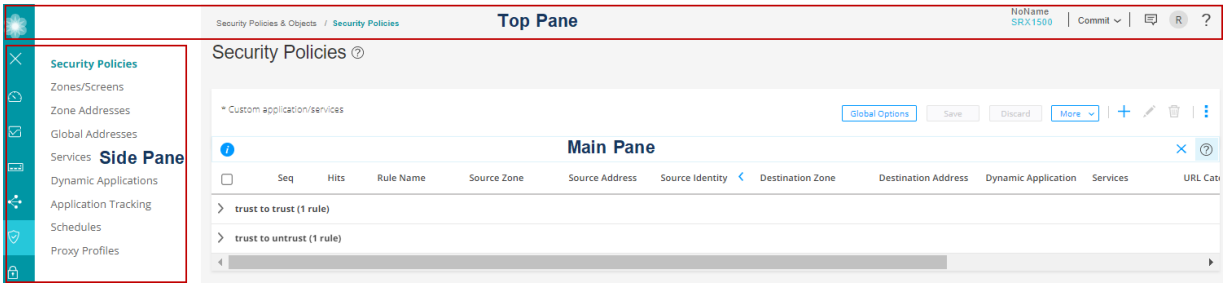
IN THIS SECTION

J-Web: A First Look

Each page of the J-Web interface is divided into the following panes (see Figure 13 on page 40):

- Launch pad—Displays high level details of the system identification, active users, and interface status. See Figure 14 on page 41.
- Top pane—Displays identifying information and links.
- Side pane—Displays subtasks of the Dashboard, Monitor, Device Administration, Network, Security Policies and Objects, and Security Services tasks currently displayed in the main pane. Click an item to access it in the main pane.
- Main pane—Location where you monitor, configure, view or generate reports, and administrate the Juniper Networks device by entering information in text boxes, making selections, and clicking buttons.

Figure 13: J-Web First Look



J-Web Launch Pad

After you successfully login to J-Web GUI, J-Web launch pad appears.

The launch pad provides a quick view of:

- Device information such as model number, serial number, hostname, software version, system time, and system up time.
- Number of active users using the device.

- State of the device physical interfaces: Up or Down.

The launch pad closes automatically once the application is loaded in the background. You do not have the option to manually close or refresh the launch pad.

NOTE:

- Launch pad is not displayed in the factory default settings.
- Launch pad is displayed for all users.

Figure 14 on page 41 shows the launch pad screen and its elements.

Figure 14: J-Web launch Pad Screen

J-Web Top Pane

For a more personal, helpful, and user experience, Juniper Networks has provided some aids within the J-Web GUI. Table 6 on page 42 provides the details of the J-Web top pane elements.

Table 6: J-Web Top Pane Elements

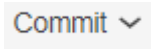
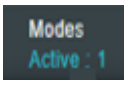
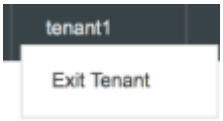
Element	Description
Banner 	Location—The gray bar at the top of the screen. You can access device details, feedback button, commit options, a profile management access menu, and a help button.
Device details 	Location—To the upper right of the banner. Provides details of the device you have accessed.
Feedback Button 	Location—To the right of the device details. You can provide feedback (mailto:jweb-feedback@juniper.net) if you are having an issue with the product.
Commit Configuration Menu 	Location—To the right of the Feedback button. Provides options to commit, compare, confirm, discard, or commit the changes in your preferred way.
User Functions Menu 	Location—To the right of the Commit Configuration button. A head-and-shoulders icon and a field showing the logged in user type. Clicking your username or the down arrow button, logs you out of J-Web interface.

Table 6: J-Web Top Pane Elements *(Continued)*

Element	Description
Help Button 	Location—To the right of the User Functions menu. Access to the online Help center and the Getting Started Guide are available by clicking the right-most icon on the banner, shaped like a question mark. The help center includes access to a list of supported web browsers, user interface assistance, as well as links to technical support and full J-Web documentation.
Mode 	Location—To the right of the device details. Provides the setup mode details whether your device is in the standard, chassis cluster (HA), or passive mode.
Tenant or Logical System Username 	Location—To the left of the device details. Displays the name of the tenant user or logical system user when root user enters as a Tenant or a logical systems. Click on the username and select **Exit** to go back to the root user role.

J-Web Side Pane

J-Web presents you a security-focused administrator with a tabbed interface.

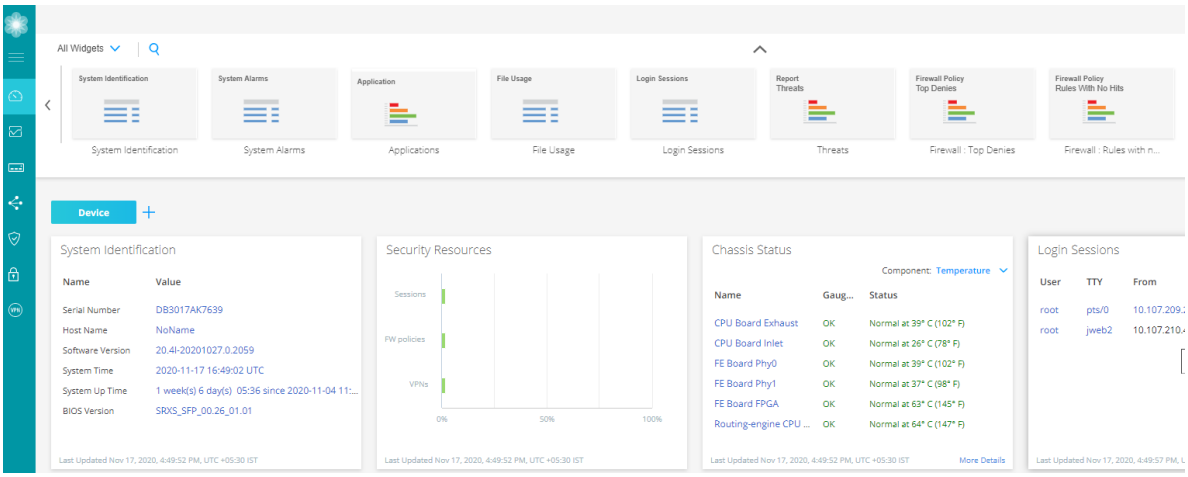
The following tabs across the side pane of the J-Web GUI provide workspaces in which an administrator can perform specific tasks:

- Dashboard—The Dashboard is the main page for J-Web. You can customize the workspace in your Dashboard by adding widgets from the carousel. The placement of, and settings within, widgets are saved so that anything from device information to firewall event information or from top blocked viruses to live threat maps can be unique for each user. Once you decide on the widgets that you want to see, you can minimize the carousel to regain some screen space.

NOTE: By default, the selected widgets are displayed every time you login to J-Web.

Figure 15 on page 44 shows an example of the J-Web Dashboard tab.

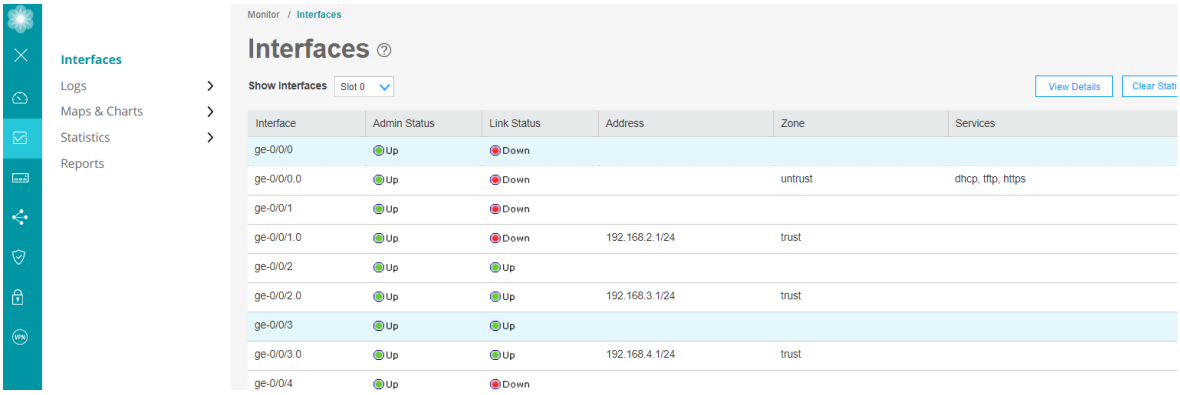
Figure 15: J-Web Dashboard Tab



- Monitor—The Monitor tab provides a workspace in which graphical representations of network traffic, firewall events, live threats, and network user data are available. There is also detailed data for alerts and alarms information. In this workspace, you can review the detailed information needed to understand what is happening to the managed security devices and traffic in your network.

  Figure 16 on page 44 shows an example of the J-Web Monitor tab.

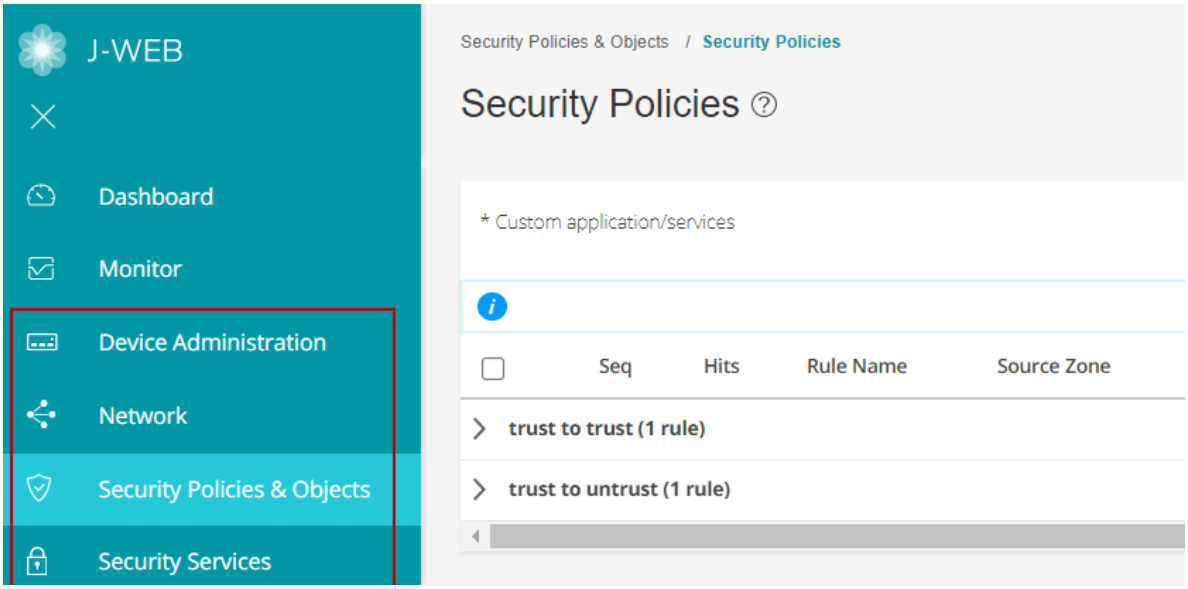
Figure 16: J-Web Monitor Tab



- Configure—The highlighted workspace in Figure 17 on page 45 is where all of the SRX Series device configuration happens. You can configure the following features for managing your network security:
  - Device Administration—Such as basic settings, user management, certificate management, license management, security package management, ATP management, operations, software management, configuration management, alarm management, RPM, tools, and reset configuration.
  - Network—Such as connectivity, DHCP, firewall filters, NAT, routing, Class of Services (CoS), Application QoS, IPsec VPN, manual key VPN, and dynamic VPN.
  - Security policies and objects—Such as security policies, zones/screens, zone and global addresses, services, dynamic applications, application tracking, schedules, and proxy profiles.
  - Security services—Such as UTM, IPS, ALG, ATP, SSL profiles, firewall authentication, and ICAP redirect.

  Figure 17 on page 45 shows an example of the J-Web configuration menus.

Figure 17: J-Web Configure Menus



J-Web Main Pane

The main workspace of J-Web takes up the remainder of the browser window just below the Banner and next to the side pane. Table 7 on page 46 shows a sample of navigation, customization, and help icons in the main pane of the J-Web GUI.

Table 7: J-Web Main Pane Elements

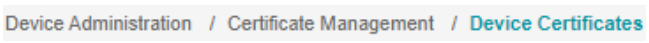
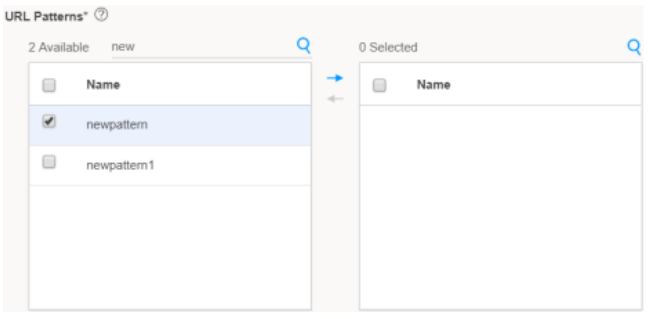
Element	Description
Breadcrumbs 	Location—Upper left part of main screen. Not visible on the Dashboard. Trace your location in the GUI. The breadcrumbs provide a path back to one of the five tabs: Dashboard, Monitor, Configure, Reports, and Administration.
Info Tips 	Location—Various places around the GUI. Hover your mouse over any available question mark icon for quick pop-up guidance.
Show/Hide Columns 	Location—Upper right corner of some tabular display windows such as the Address Pools tab, Rules tab, and so on. In tabular displays, you can choose which columns are visible by clicking the icon and then selecting the check boxes on the menu.
Table Search 	Location—Upper right corner of tabular views. You can click the magnifying glass icon, within large tabular views, to search for specific text within any of the visible fields in the display.
Item Selector Search 	Location—Within the fields. You can use a search text box to select items for inclusion in a rule or policy.

Table 7: J-Web Main Pane Elements *(Continued)*

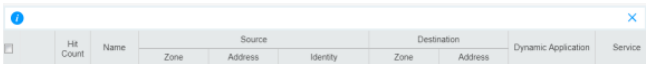
Element	Description
Advanced Search 	Location—Above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. **NOTE**: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.
Filter 	Location—Upper right corner of tabular views. You can click the filter icon to select any value from a list for category and subcategory columns. The grid is reloaded with the filtered category and subcategory.
Success message 	Location—At the top of the main pane. A message is displayed with this icon to state that your task is successful.
Information message 	Location—At the top of the main pane. A message is displayed with this icon to state you have some pending actions, but you can continue with the task.
Alert message 	Location—At the top of the main pane. A message is displayed with this icon to state you have some pending actions which you must complete to proceed with the required task.

Table 7: J-Web Main Pane Elements *(Continued)*

Element	Description
Warning message 	Location—At the top of the main pane. A message is displayed with this icon to state you have some pending actions which you must complete else you cannot proceed with the required task.

J-Web Workflow Wizards

J-Web contains assisting workflow wizards that guide you through some of its security functions. These include Setup wizard, Chassis Cluster wizard, PPPoE wizard, and NAT wizard. These wizards help you with a guided setup and helps you in performing step-by-step configuration of a services gateway that can securely pass traffic.

NOTE: PPPoE and NAT Wizards are available only in the SRX300 line of devices and SRX550M devices.

Summary

J-Web is a GUI approach that aims to provide a graphical framework to help you visualize and manage your SRX Series devices more easily.

SEE ALSO

Add an SRX Series Firewall to Juniper Security Director Cloud | 50

2

PART

Add SRX Series Firewall to Security Director Cloud

Add an SRX Series Firewall to Juniper Security Director Cloud

You can add your SRX Series device to Juniper Security Director Cloud from J-Web. After you add the SRX Series device to the Juniper Security Director Cloud, you can manage your network security using these devices.

In order for your device to be managed by Juniper Security Director Cloud, ensure the following:

- Your device must have Internet connectivity and access to the Juniper Security Director Cloud portal.
- Before adding, you must open the following ports of your device so that it communicates with Juniper Security Director Cloud:
  - TCP/443 (HTTPS) for Juniper Security Director Cloud portal and Redirect server
  - TCP/7804 (NETCONF) for SRX Series device outbound access to Juniper Security Director Cloud portal
  - TCP/6514 (TLS syslog)
  - TCP/53 (DNS) - (IP: 8.8.8.8)
  - UDP/53 (DNS) - (IP: 8.8.4.4)

Here's how you can add your device to Juniper Security Director Cloud from J-Web:

1. Login to J-Web.
2. Click **Add Device to Juniper Security Director Cloud** located on the top-right corner of the J-Web GUI to open the Add Device to Juniper Security Director Cloud page.
3. Select your location from the list and then enter your Juniper Security Director Cloud account email and password. Then, click **Next**.
4. Select your organization account name (with administrator permissions) and click **Proceed**.
   The status progress bar is shown until your device is successfully added. During this process, your device gets added to the Juniper Security Director Cloud and commits the received configuration from the Cloud API.

A success message is displayed and your device is added to Juniper Security Director Cloud. The label next to the icon changes from **Add Device to Juniper Security Director Cloud** to **Manged by Juniper Security Director Cloud** and the changed label is grayed out.

NOTE:

- When you have logged into the J-Web and remove your device from Juniper Security Director Cloud, J-Web still displays the status as **Manged by Juniper Security Director Cloud**. Log in to J-Web again to see the label changed to **Add Device to Juniper Security Director Cloud**.
- If there are any network issues between the SRX Series device and Juniper Security Director Cloud, J-Web still displays the status as **Manged by Juniper Security Director Cloud**.

Once added, you can see your device on the **Device Management** > **Devices** page when you log into the Juniper Security Director Cloud portal. You can only delete your device from Juniper Security Director Cloud and not from the J-Web GUI. To remove the device, select your device on the Devices page and click the delete icon.

RELATED DOCUMENTATION

Dashboard Overview | 53

PART 3

Dashboard

CHAPTER 2

J-Web Dashboard

IN THIS CHAPTER

Dashboard Overview

IN THIS SECTION

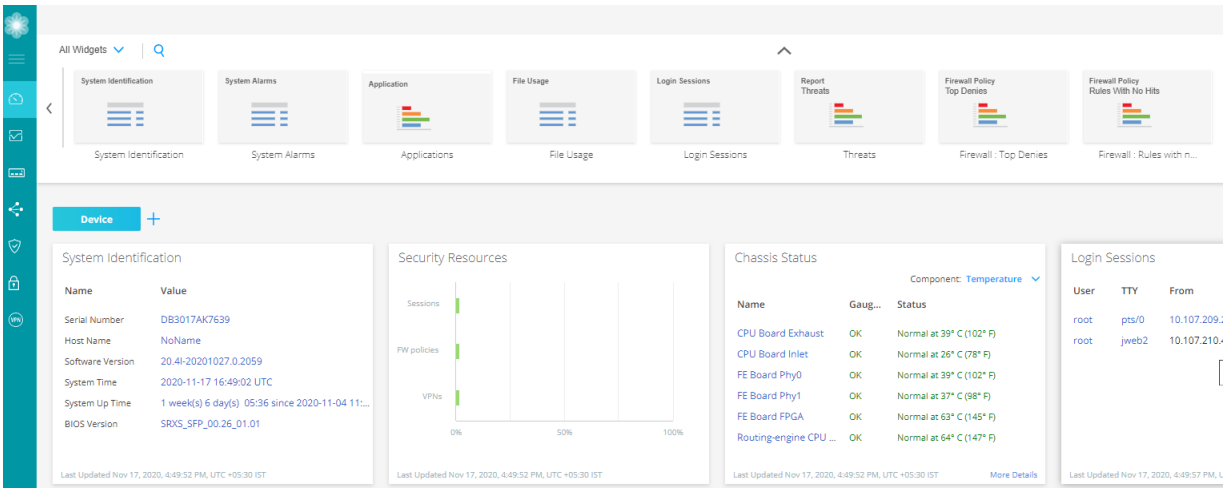
What is J-Web Dashboard

The J-Web dashboard provides a unified overview of the system and network status retrieved from SRX Series devices.

To use the dashboard at the top-level menu, select **Dashboard**. By default, the Dashboard page displays all the widget thumbnails.

Figure 18 on page 54 shows an example of the Dashboard page of SRX345 Services Gateway.

Figure 18: SRX345 Dashboard



Work with Widgets

Each widget pane acts as a separate frame. You can click **+** icon to add separate dashboard and name it as per your ease. You can refresh the display of the Dashboard page by clicking the refresh icon at the top right-hand corner above the widget pane.

You can choose any one of the categories to view widgets on your device:

- All Widgets—Displays all the supported widgets
- Applications—Displays only the supported application related widgets
- Devices—Displays only the supported device related widgets
- Security—Displays only the supported security related widgets

NOTE:

- Starting in Junos OS Release 21.4R1, on-box reports related widgets are removed to speed up the J-Web UI loading process.
- The Threat Activity pane is not available on SRX5400, SRX5600, and SRX5800 devices.
- For SRX Series devices configured for logical systems, the Logical System Identification and Logical System Profile panes are displayed when you log in as a user logical system administrator. These are the only logical system panes available in Dashboard Preferences.

- If the rescue configuration is not set, the set rescue configuration link directs you to the Device Administration > Configuration Management > Rescue page to set the rescue configuration.

To use a widget on the Dashboard:

1. Drag the widgets from the palette or thumbnail container to your dashboard.

   When you add more widgets on the J-Web Dashboard, you can observe high CPU usage on the Routing Engine for a short span of time on every refresh. We recommend that you use four widgets for lower CPU consumption.

2. Mouse over the top of each widget to minimize, refresh, and close by using the respective icons.

   NOTE: The dashlet data is refreshed every minute by default. You cannot manually configure the refresh interval of the dashlet. If the data is not aged in the cache, data loads from the cache during the dashlet refresh. If the data is aged, it is retrieved from the device during the next refresh interval cycle.

Table 8 on page 55 provides the dashboard widgets options based on the selected device.

Table 8: Dashboard Widgets Options

Field	Description
System Alarms	Provides the received time, severity, description of the alarms and the action to be taken.
System Identification	Provides system details such as serial number of the software, hostname, software version, BIOS version, system uptime, and system time.
Login Sessions	Provides the user credentials, login time, idle time, and host.
File Usage	Provides current space requirements for log, temporary, crash, and database files. Click **Maintain** to download or delete some or all of these files. **NOTE**: File Usage widget supports RE3 line cards for SRX5000 line of devices.

Table 8: Dashboard Widgets Options *(Continued)*

Field	Description
Resource Utilization	Provides a graphical representation of the CPU, memory, and storage used for both the data and the control planes. The CPU control also shows the load average value for 1 minute when you mouse over **CPU Control**. **NOTE**: Resource Utilization widget supports RE3 line cards for SRX5000 line of devices.
Signal Strength	Displays the signal strength of the device.
Interface: Most Dropped Packets	Displays top 5 interfaces based on the CLI response; top-count will increase to 10.
Security Resources	Provides the maximum, configured, and activated number of sessions, firewall/VPN policies, and IPsec VPNs.
Storage Usage	Displays used and available storage and usage information about other system components.
Logical System Identification	Provides the logical system name, the security profile assigned to the logical system, the software version, and the system time.
Logical System Profile	Displays the types of resources that are allocated to the user logical system, the number of resources used and reserved, and the maximum number of resources allowed.
NAT - Top Source Translation Hits	Displays the top 10 source translation hits. Click **More Details** to view source NAT logs at **Monitor** > **Logs** > **All Events**.
NAT - Top Destination Translation Hits	Displays the top 10 destination translation hits. Click **More Details** to view destination NAT logs at **Monitor** > **Logs** > **All Events**.

Table 8: Dashboard Widgets Options *(Continued)*

Field	Description
IPsec VPNs (IKE Peers)	Displays status count of IPsec VPN topologies, such as ADVPN Hub and Spoke, Remote Access, and Site-to-Site/Hub & Spoke. Click **More Details** to redirect to the **Monitor** > **Network** > **IPsec VPN** page.
VPN Monitoring	Displays the total number of IPsec VPNs (Total VPNs for All VPNs and total remote users for Remote Access). All VPNs option includes Site to Site, Hub & Spoke, ADVPN Hub, and ADVPN spoke. Remote Access includes Juniper Secure Connect and NCP Exclusive Entry Client. Widget pane also displays the VPNs status with a color code: • Up (Green)—IKE and IPsec SA are up. • Down (Red)—IKE and IPsec are not operationally up. • Partially Up (Amber)—Either IKE or IPsec SA is up or one or few traffic selectors are up. Click **More Details** available on the widget pane to redirect to the **Monitor** > **Network** > **IPsec VPN** page. On the widget pane, for the All VPNs option, each configured IPsec VPN is represented as an individual tunnel icon or box. On the widget pane, for the Remote Access option, each IKE SAs corresponding to the configured IPsec VPN is represented as an individual tunnel icon or box. If there are no IKE SAs for the VPN, then a single box is shown as down. When you hover over the box, widget displays VPN tunnel details such as Remote gateway, VPN name, IKE status, IPsec status, local IP, and remote IP. Click **More Details** to redirect to the **Monitor** > **Network** > **IPsec VPN** page with the VPN name filtered.

4

PART

Monitor

CHAPTER 3

Network

IN THIS CHAPTER

Monitor Interfaces

You are here: **Monitor** > **Network** > **Interfaces**.

Use this page to view general information about all physical and logical interfaces for a device.

Table 9 on page 59 describes the fields on the Interfaces page.

Table 9: Fields on the Interfaces Page

Field	Description
Show Interfaces	Select **All** or any particular slot to show the interface details.
View Details	Displays extensive statistics about the selected interface, including its general status, traffic information, IP address, I/O errors, class-of-service data, and statistics.
Clear Statistics	Clears the statistics for the selected interface.
Auto Refresh Frequency	Indicates the duration of time after which you want the data on the page to be refreshed automatically.

Table 9: Fields on the Interfaces Page *(Continued)*

Field	Description
Interface	Displays the interface name.
Link Status	Displays whether the interface is linked (Up) or not linked (Down).
Address	Displays the IP address of the interface.
Zone	Displays whether the zone is an untrust zone or a trust zone.
Host Inbound Traffic	Displays the following: • Services that are enabled on the device, such as HTTPS and SSH. • Protocols that are enabled on the device, such as BGP and IGMP.

RELATED DOCUMENTATION

Monitor Session | 66

Monitor DHCP Server Bindings

You are here: **Monitor** > **Network** > **DHCP Server Bindings**.

Use this page to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

Table 10 on page 61 describes the fields on the DHCP Server Bindings page.

Table 10: Fields on the DHCP Server Bindings Page

Field	Description
Routing Instance	Select the routing instance name.
DHCP Interface Details	Displays the interface on which the DHCP server is configured.
Clear	Clears all or selected binding information.
Client IP Address	Displays the IP address of the DHCP client.
MAC Address	Displays the MAC address of the DHCP server.
State	State of the address binding table on the extended DHCP local server: • BOUND—Client has an active IP address lease. • FORCE RENEW—Client has received the FORCE RENEW message from the server. • INIT—Initial state. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers.
Lease Time Remaining	Displays the time (in hours and minutes) at which the lease expires.
DHCP Interface	Displays the interface on which the request was received.
Session ID	Displays the Session ID of the subscriber session.

RELATED DOCUMENTATION

About Reports Page | 117

Monitor IPsec VPN

You are here: **Monitor** > **Network** > **IPsec VPN**.

Use the monitoring functionality to view information of IKE, IPsec configuration, Security Associations (SA), and Statistics in a tabular format that includes sortable columns. A VPN provides a means by which remote computers communicate securely across a public WAN such as the Internet. IPsec VPN is a protocol that consist set of standards used to establish a VPN connection.

Table 11 on page 62 describes the fields on the IPsec VPN page.

Table 11: Fields on the IPsec VPN Page

Field	Description
IPsec Statistics list menu	Displays summary of the global IPsec VPN or selected IPsec VPN statistics.
Clear SA list menu	Displays the options **Clear All SAs** or **Clear Selected SA** to clear SAs. If you choose **Clear All SAs**, then you can select **Clear All IKE SAs**, **Clear All IPsec SAs**, or **Clear All IKE & IPsec SAs**. If you choose **Clear Selected SAs**, then you can select **Clear Selected IKE SA**, **Clear Selected IPsec SA**, or **Clear Selected IKE & IPsec SA**.
Refresh icon	Click refresh icon to get latest operational data. **NOTE**: The configuration data is fetched from cache. Any changes to the CLI will be fetched only after you commit it and click Monitor > Network > IPsec VPN to refresh the page and get the latest configuration data.
Search	You can search and filter either the remote gateway or the VPN name.
Remote Gateway	Displays gateway name of the remote system.
IKE Status	Displays if IKE is up or down.

Table 11: Fields on the IPsec VPN Page *(Continued)*

Field	Description
Local IP	Displays the external interface, IP address, and port of the local peer so that its remote peer can communicate with it.
Remote IP	Displays the IP address and port of the remote peer. **NOTE**: The remote IP displays only when the IKE is up.
VPN Name	Displays IPsec VPN name.
TS/Proxy ID Status	Displays information and status (up or down) of the traffic selector or the proxy ID that are negotiated between the peers.
IPsec Soft Life	Displays the soft lifetime (in seconds) which indicates that the IPsec key management system that the SA is about to expire.
IKE Index	Displays index number for a particular IKE SA.
IPsec Index	Displays index number for a particular IPsec SA.
Topology	Displays the topology deployment for an IPsec VPN. For example: Site to Site/Hub & Spoke or Remote Access VPN.
IKE Proposal	Lists algorithms negotiated with the remote peer.
IPsec Proposal	Lists protocols and algorithms negotiated with the remote peer.
Authentication Type	Display if the preshared key or certificate based is used by the Virtual Private network (VPN).

Table 11: Fields on the IPsec VPN Page *(Continued)*

Field	Description
DPD	Displays dead peer detection (DPD) method used by devices to verify the current existence and availability of IPsec peers.
Role	Displays whether the device is an initiator or a responder.
IKE Initiator Cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.
IKE Responder Cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets are received.
IKE Life	Lifetime (in seconds) of an IKE SA. Range: 180 through 86,400. Default is 3600.
Mode	Negotiation method agreed upon by the two IPsec endpoints, or peers, used to exchange information. Each exchange type determines the number of messages and the payload types that each message contains. The modes or exchange types are: • Main—The exchange is done with six messages. This mode, or exchange type, encrypts the payload, protecting the identity of the neighbor. Displays the authentication method used: preshared keys or certificate. • Aggressive—The exchange is done with three messages. This mode, or exchange type, does not encrypt the payload, leaving the identity of the neighbor unprotected.
Peer IKE-ID	Displays the IKE IDs for the local or remote devices.

Table 11: Fields on the IPsec VPN Page *(Continued)*

Field	Description
Remote Access	Displays the remote access URL. **NOTE**: This option is applicable only for the remote access VPN with Juniper Secure Connect (JSC).
Remote User	Displays the remote IKE identity to exchange with the destination peer to establish communication.
DNS	Displays the IP addresses for a primary and a secondary DNS servers.
WINS	Displays the IP addresses for a primary and a secondary WINS servers.
Inbound SPI	Displays security parameter index (SPI) value to authenticate incoming traffic coming from the peer.
Outbound SPI	Displays algorithms, keys, or SPI values to decrypt and to authenticate outbound traffic to the peer.
IPsec Hard Life	Displays number of seconds until the SA expires.
IPsec Lifesize	Displays the lifesize remaining specifies the usage limits in kilobytes. If no lifesize is specified, it shows unlimited.

RELATED DOCUMENTATION

Monitor Session | 66

CHAPTER 4

Logs

IN THIS CHAPTER

Monitor Session

You are here: **Monitor** > **Logs** > **Session**.

Use the monitoring functionality to view the firewall events or sessions that occurred during the time period specified.

NOTE: Session page is available on all the SRX Series devices except the SRX5000 line of devices.

Table 12 on page 67 describes the fields on the Session page.

Table 12: Fields on the Session Page

Field	Description
Last	Select the time from the list to view the activity that you are most interested in. Once you select the time, all the data presented in your view refreshes automatically. You can also use **Customize** to set a custom date and click **Apply** to view the specified session logs.
More	• View PCAP Counters—View packet capture (PCAP) counter statistics for unknown application traffic. Click **Clear Counters** to reset all the packet capture counters value of the unknown application traffic to zero. • Delete PCAP Files—Select this option to permanently delete all the available PCAP files on your device.
Refresh	Click the refresh icon to get the latest session information.
Show Hide Columns	The three vertical dots represents this icon. Enables you to show or hide a column in the grid.
Export to CSV	You can export the session data to a comma-separated value (.csv) file. Select the three vertical dots on the right-side of the page and then click **Export to CSV**. The CSV file is downloaded to your local machine. You can download only maximum of 100 sessions data.

Table 12: Fields on the Session Page *(Continued)*

Field	Description
Filter Criteria	Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string. In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. The following filters are available: • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country • Source Port • Destination Port • Protocol
X	Click **X** to clear your search filter.

Table 12: Fields on the Session Page *(Continued)*

Field	Description
Save Filter	Click **Save Filter** to save filters after you specify the filtering criteria. To save a filter: **1.** Enter the filter criteria you are looking for in the advanced search box. **2.** Click **Save Filter**. **3.** Enter a name for the filter and click the tick icon to save it.
Load Filter	Displays the saved filters list. Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.
View Details	When you hover over the PCAP file, a Detailed View icon appears before the PCAP file. Click the icon to view the log details on the Detailed Log View page. Click on the download icon in the Detailed Log View page to download the packet capture file of an unknown application traffic. The session ID available in the file name identifies the PCAP file. **NOTE**: If the files are not available, the download fails and you will receive an error message.
PCAP	Click on the download icon to download the packet capture (PCAP) file of an unknown application traffic. The download icon appears only if a packet captured for the session log type close. The session ID available in the file name identifies the PCAP file. **NOTE**: If the files are not available, the download fails and you will receive an error message.
Time	Displays the time when the log was received.
Log Type	Displays the log type.
Source Zone	Displays the source zone of the session.

Table 12: Fields on the Session Page *(Continued)*

Field	Description
Source IP	Displays the source IP address from where the session occurred.
User	Displays the username from whom the session log is generated.
Destination Zone	Displays the destination zone of the session.
Destination IP	Displays the destination IP of the session occurred.
Destination Port	Displays the destination port of the session.
Application	Displays the application name from which the session logs are generated.
Action	Displays the action taken for the event: warning, allow, and block.
Policy	Displays the destination country of the log.
Bandwidth	Displays the bandwidth utilization for the session.
NAT Source IP	Displays the translated (or natted) source IP address. It can contain an IPv4 or an IPv6 addresses.
NAT Source Port	Displays the translated source port.
NAT Destination IP	Displays the translated (also called natted) destination IP address.
NAT Destination Port	Displays the translated destination port.
Protocol ID	Displays the protocol ID in the log.
Session ID	Displays the traffic session ID of the log.

Table 12: Fields on the Session Page *(Continued)*

Field	Description
Interface	Displays the interface of the session.
Closure Reason	Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
Packets From Client	Displays the number of packets received from the client.
Bytes From Client	Displays the number of bytes received from the client.
Packets From Server	Displays the number of packets received from the server.
Bytes From Server	Displays the number of bytes received from the server.
Elapsed Time	Displays the time elapsed since the last time interval began.
Source Port	Displays the port number of the source.

RELATED DOCUMENTATION

Monitor Threats | 71

Monitor Threats

You are here: **Monitor** > **Logs** > **Threats**.

Use the monitoring functionality to view the security threats. Threats are defined as any IPS, screen, security intelligence, antivirus, content filtering, or antispam.

NOTE: Threat page is available on all the SRX Series devices except the SRX5000 line of devices.

Table 13 on page 72 describes the fields on the Threats page.

Table 13: Fields on the Threats Page

Field	Description
Last	Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically. You can also use **Customize** to set a custom date and click **Apply** to view the specified threats.
Refresh	Click the refresh icon to get the latest threat information.
Show Hide Columns	This icon is represented by three vertical dots. Enables you to show or hide a column in the grid.
Export to CSV	You can export the threats data to a comma-separated value (.csv) file. Select the three vertical dots on the right-side of the page and click **Export to CSV**. The CSV file is downloaded to your local machine. You can download only maximum of 100 sessions data.

Table 13: Fields on the Threats Page *(Continued)*

Field	Description
Filter Criteria	Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string. In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. The following filters are available: • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country • Source Port • Destination Port • Protocol
X	Click **X** to clear your search filter.

Table 13: Fields on the Threats Page *(Continued)*

Field	Description
Save Filter	Click **Save Filter** to save filters after you specify the filtering criteria. To save a filter: 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click **Save Filter**. 3. Enter a name for the filter and click the tick icon to save it.
Load Filter	Displays the saved filters list. Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.
Time	Displays the time when the threats log was received.
Log Type	Displays the threats log type. For example, IPS, Antivirus, Antispam, and so on.
Name	Displays the name of the event.
Severity	Displays the severity of the threat.
Source Zone	Displays the source zone of the threats.
Source IP	Displays the source IP address from where the threats log occurred.
Source Port	Displays the port number of the source.
User	Displays the username from whom the threat log is generated.
Destination Zone	Displays the destination zone of the threats.
Destination IP	Displays the destination IP of the threats occurred.

Table 13: Fields on the Threats Page *(Continued)*

Field	Description
Destination Port	Displays the port number of the destination.
Application	Displays the nested application or application name from which the threats are generated.
Action	Displays the action taken from the threats.
Session ID	Displays the traffic session ID of the threats.
Closure Reason	Displays the reason for the session closure.
Profile	Displays the threat profile name.
Category	Displays the threat category.
URL	Displays the accessed URL name that triggered the event.
Object	Displays the object name of the threats.
Destination Interface	Displays the interface name of the destination.
Source Interface	Displays the interface name of the source.
Policy	Displays the policy name that triggered the threats log.
Rule	Displays the rule name of the threats log.
Protocol	Displays the protocol ID in the threats log.
CVE-ID	Displays the Common Vulnerabilities and Exposures (CVE) identifiers information for the threat.

Table 13: Fields on the Threats Page *(Continued)*

Field	Description
Elapsed Time	Displays the time elapsed since the last time interval began.
Packet Log ID	Displays the packets ID received before and after the attack for further offline analysis of attacker behavior.
XFF	Displays X-Forwarded-For (XFF) header added to packets by a proxy server that includes the real IP address of the client making the request.
File Name	Displays the filename of the threats log.
Argument	Displays the arguments that are passed to an event when it is invoked from the threats log.
Source Name	Displays the name of the source from where threat is originated.
Feed Name	Displays the feed name of the threat detected.
Count	Displays the number of threats count.
Message Type	Displays the message type for the threat detected.
HTTP Host	Displays the host URL for the threat.

RELATED DOCUMENTATION

Monitor Web Filtering | 76

Monitor Web Filtering

You are here: **Monitor** > **Logs** > **Web Filtering**.

Use this page to view information about the Web filtering events based on web filtering policies, filter options, and grid elements of Web filtering events.

NOTE: Web Filtering page is available on all the SRX Series devices except the SRX5000 line of devices.

Table 14 on page 77 describes the fields on the Web Filtering page.

Table 14: Fields on the Web Filtering Page

Field	Description
Last	Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically. You can also use **Customize** to set a custom date and click **Apply** to view the specified Web filtering event logs.
Refresh	Click the refresh icon to get the latest Web filtering event information.
Show Hide Columns	This icon is represented by three vertical dots. Enables you to show or hide a column in the grid.
Export to CSV	You can export the Web filtering event data to a comma-separated value (.csv) file. Select the three vertical dots on the right-side of the page and click **Export to CSV**. The CSV file is downloaded to your local machine. You can download only maximum of 100 sessions data.

Table 14: Fields on the Web Filtering Page *(Continued)*

Field	Description
Filter Criteria	Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string. In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. The following filters are available: • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country • Source Port • Destination Port
X	Click **X** to clear your search filter.
Save Filter	Click **Save Filter** to save filters after you specify the filtering criteria. To save a filter: 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click **Save Filter**. 3. Enter a name for the filter and click the tick icon to save it.

Table 14: Fields on the Web Filtering Page *(Continued)*

Field	Description
Load Filter	Displays the saved filters list. Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.
Time	Displays the time when the Web filtering event log was received.
Log Type	Displays the Web filtering event log type.
Source Zone	Displays the source zone of the Web filtering event.
Source IP	Displays the source IP address from where the Web filtering event occurred.
User	Displays the username from whom the Web filtering event log is generated.
Destination Zone	Displays the destination zone of the Web filtering event.
Destination IP	Displays the destination IP of the Web filtering event occurred.
Destination Port	Displays the destination port of the Web filtering event.
Application	Displays the application name for which the Web filtering event logs are generated.
Action	Displays the action taken for the event: deny, permit, or redirect.
Session ID	Displays the traffic session ID of the Web filtering event log.
Closure Reason	Displays the reason for the Web filtering event log generation closure.
URL Category Risk	Displays the Web filtering URL risk level.

Table 14: Fields on the Web Filtering Page *(Continued)*

Field	Description
Profile	Displays the Web filtering profile name.
Category	Displays the Web filtering URL category.
URL	Displays the accessed URL name that triggered the event.
Obj	Displays the object name of the Web filtering event log.

RELATED DOCUMENTATION

Monitor ATP | 80

Monitor ATP

You are here: **Monitor** > **Logs** > **ATP**.

Use the monitoring functionality to view the ATP page. Analyzing the Juniper ATP logs yields information such as malware name, action taken, infected host, source of an attack, and destination of an attack.

NOTE: ATP page is available on all the SRX Series devices except the SRX5000 line of devices.

Table 15 on page 81 describes the fields on the ATP page.

Table 15: Fields on the ATP Page

Field	Description
Last	Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically. You can also use **Customize** to set a custom date and click **Apply** to view the specified ATP logs.
Refresh	Click the refresh icon to get the latest ATP log information.
Show Hide Columns	This icon is represented by three vertical dots. Enables you to show or hide a column in the grid.
Export to CSV	You can export the ATP log data to a comma-separated value (.csv) file. Select the three vertical dots on the right-side of the page and click **Export to CSV**. The CSV file is downloaded to your local machine. You can download only maximum of 100 ATP log data.

Table 15: Fields on the ATP Page *(Continued)*

Field	Description
Filter Criteria	Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string. In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. The following filters are available: • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country • Source Port • Destination Port • Protocol
X	Click **X** to clear your search filters.

Table 15: Fields on the ATP Page *(Continued)*

Field	Description
Save Filter	Click **Save Filter** to save filters after you specify the filtering criteria. To save a filter: 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click **Save Filter**. 3. Enter a name for the filter and click the tick icon to save it.
Load Filter	Displays the saved filters list. Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.
Time	Displays the time when the ATP log was received.
Log Type	Displays the ATP log type: Action, Malware event, SMTP action, and IMAP action.
Source Zone	Displays the source zone of the ATP log.
Source IP	Displays the source IP address from where the ATP log occurred.
Source Port	Displays the port number of the source.
User	Displays the username who downloaded the possible malware.
Destination Zone	Displays the destination zone of the ATP log.
Destination IP	Displays the destination IP of the ATP log occurred.
Destination Port	Displays the destination port of the ATP log.
Application	Displays the application name from which the ATP logs are generated.

Table 15: Fields on the ATP Page *(Continued)*

Field	Description
Action	Displays the action taken from the event: log, permit, and log and permit.
Session ID	Displays the session ID of the ATP log.
Policy	Displays the name of policy that enforced this action.
List Hit	Displays the number of times the C&C server has attempted to contact hosts on your network.
URL	Displays the accessed URL name that triggered the event.
Sample SHA256	Displays the SHA-256 hash value of the downloaded file.
File Hash Lookup	Displays the hash of the file sent for matching against known malware.
File Name	Displays the name of the file, including the extension.
Protocol	Displays the protocol that the C&C server used to attempt communication.
File Category	Displays the type of file. Examples: PDF, executable, document.
Hostname	Displays the hostname of device that downloaded the possible malware.
Verdict Number	Displays the a score or threat level for a file.
Malware Info	Displays the malware name or brief description.
Send To	Displays the email address.
Send From	Displays the email address.

Table 15: Fields on the ATP Page *(Continued)*

Field	Description
Tenant ID	Displays the internal unique identifier.

RELATED DOCUMENTATION

Monitor VPN | 85

Monitor VPN

You are here: **Monitor** > **Logs** > **VPN**.

Use the monitoring functionality to view comprehensive stream log details of VPN in a tabular format that includes sortable columns. A VPN provides a means by which remote computers communicate securely across a public WAN such as the Internet.

NOTE: VPN page is available on all the SRX Series devices except the SRX5000 line of devices.

Table 16 on page 85 describes the fields on the VPN page.

Table 16: Fields on the VPN Page

Field	Description
Last	Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically. You can also use **Customize** to set a custom date and click **Apply** to view the specified VPN events.
Refresh	Click the refresh icon at the top right corner to display the fresh content.

Table 16: Fields on the VPN Page *(Continued)*

Field	Description
Show Hide Columns	This icon is represented by three vertical dots. Enables you to show or hide a column in the grid.
Export to CSV	You can export the VPN data to a comma-separated value (.csv) file. Select the three vertical dots on the right-side of the page and click **Export to CSV**. The CSV file is downloaded to your local machine. You can download only maximum of 100 VPN data.
Filter Criteria	Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string. In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. The available filter option is Log type.
X	Click **X** to clear your search filter.
Save Filter	Click **Save Filter** to save filters after you specify the filtering criteria. To save a filter: 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click **Save Filter**. 3. Enter a name for the filter and click the tick icon to save it.
Load Filter	Displays the saved filters list. Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.
Time	Displays the time when the VPN log was received.

Table 16: Fields on the VPN Page *(Continued)*

Field	Description
Log Type	Displays the VPN log type: • Bad SPI • Replay • PV decryption • PV encryption • PV sm keygen • PV replay • Decrypt bad pad • AUTH fail • D3P ERR
Interface Name	Displays the external interface name for the VPN.
Tunnel ID	Displays the VPN tunnel ID.
Source IP	Displays the source IP address from where the VPN connection is established.
Destination IP	Displays the destination IP to where the VPN connection is established.
Length	Displays the total packet length in Bytes.
Type	Displays the VPN type: ESP or AH protocol.
Index	Displays the index number of the IKE SA.
Sequence Number	Displays the sequence number of the packets sent for the VPN event.

Table 16: Fields on the VPN Page *(Continued)*

Field	Description
Message	Displays the error message for the VPN event.

RELATED DOCUMENTATION

Monitor All Events | 88

Monitor All Events

You are here: **Monitor** > **Logs** > **All Events**.

Use this page to view event details associated with session, content filtering, antispam, antivirus, IPS, screen, security intelligence, Web filtering, ATP, and VPN.

NOTE: All Events page is available on all the SRX Series devices except the SRX5000 line of devices.

Table 17 on page 88 describes the fields on the All Events page.

Table 17: Fields on the All Events Page

Field	Description
Last	Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically. You can also use **Customize** to set a custom date and click **Apply** to view the specified event logs.
Refresh	Click the refresh icon to get the latest event information.

Table 17: Fields on the All Events Page *(Continued)*

Field	Description
Show Hide Columns	This icon is represented by three vertical dots. Enables you to show or hide a column in the grid.
Export to CSV	You can export the event data to a comma-separated value (.csv) file. Select the three vertical dots on the right-side of the page and click **Export to CSV**. The CSV file is downloaded to your local machine. You can download only maximum of 100 event data.
Filter Criteria	Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string. In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not. The following filters are available: • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country • Source Port • Destination Port • Protocol

Table 17: Fields on the All Events Page *(Continued)*

Field	Description
X	Click **X** to clear your search filter.
Save Filter	Click **Save Filter** to save filters after you specify the filtering criteria. To save a filter: 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click **Save Filter**. 3. Enter a name for the filter and click the tick icon to save it.
Load Filter	Displays the saved filters list. Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.
Time	Displays the time when the event log was received.
Log Type	Displays the event log type.
Source Zone	Displays the source zone of the event.
Source IP	Displays the source IP address from where the event occurred.
Destination Zone	Displays the destination zone of the event.
Destination IP	Displays the destination IP of the event occurred.
Destination Port	Displays the destination port of the event.
Application	Displays the application name for which the event logs are generated.
Action	Displays the action taken for the event: warning, allow, and block.

Table 17: Fields on the All Events Page *(Continued)*

Field	Description
Policy	Displays the destination country of the event log.
NAT Source IP	Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Source Port	Displays the translated source port.
NAT Destination IP	Displays the translated (also called natted) destination IP address.
NAT Destination Port	Displays the translated destination port.
Protocol	Displays the protocol ID in the event log.
Session ID	Displays the traffic session ID of the event log.
User	Displays the username from whom the event log is generated.
Source Interface	Displays the source interface of the event log.
Destination Interface	Displays the destination interface of the event log.
Closure Reason	Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
Packets From Client	Displays the number of packets received from the client.
Bytes From Client	Displays the number of bytes received from the client.
Packets From Server	Displays the number of packets received from the server.
Bytes From Server	Displays the number of bytes received from the server.

Table 17: Fields on the All Events Page *(Continued)*

Field	Description
Elapsed Time	Displays the time elapsed since the last time interval began.
Source Port	Displays the port number of the source.
Sequence Number	Displays the sequence number of the packets sent.
Message Type	Displays the message type for the event detected.
Count	Displays the number of events count.
Severity	Displays the severity of the threat.
CVE-ID	Displays the Common Vulnerabilities and Exposures (CVE) identifiers information.
Packet log ID	Displays the packets ID received before and after the attack for further offline analysis of attacker behavior.
XFF	Displays the X-Forwarded-For (XFF) header added to packets by a proxy server that includes the real IP address of the client making the request.
Profile	Displays the event profile name.
File Name	Displays the filename of the event log.
Argument	Displays the arguments that are passed from the event log.
Message	Displays the message ID for negotiation.
Bandwidth	Displays the bandwidth utilization for the event log.
Malware Info	Displays the malware name or brief description.

Table 17: Fields on the All Events Page *(Continued)*

Field	Description
Hostname	Displays the hostname of device that downloaded the possible malware.
File Category	Displays the type of file. Examples: PDF, executable, document.
Verdict Number	Displays the a score or threat level for a file.
List Hit	Displays the number of times the C&C server has attempted to contact hosts on your network.
File Hash Lookup	Displays the hash of the file sent for matching against known malware.
Sample SHA256	Displays the SHA-256 hash value of the downloaded file.
File Name	Displays the name of the file, including the extension.
URL	Displays the accessed URL name that triggered the event.
Send To	Displays the email address.
Send From	Displays the email address.
Category	Displays the threat/event category.
Object	Displays the object name of the event log.
URL Category Risk	Displays the Web filtering URL category risk level.
Virus Name	Displays the detected virus name.
Source Name	Displays the name of the source from where event is originated.

Table 17: Fields on the All Events Page *(Continued)*

Field	Description
Feed Name	Displays the feed name of the event detected.
Rule	Displays the rule name of the threats/events log.
Length	Displays the total packet length in Bytes
Type	Displays the event type.
Index	Displays the index number of the IKE SA.

RELATED DOCUMENTATION

Monitor Alarms | 94

Monitor Alarms

You are here: **Monitor** > **Logs** > **Alarms**.

Use this page to view the alarms details such as time, severity, type, and descriptions of the alarm.

Table 18 on page 94 describes the fields on the Alarms page.

Table 18: Fields on the Alarms Page

Field	Description
Show Hide Columns icon	Enables you to show or hide a column in the grid.

Table 18: Fields on the Alarms Page *(Continued)*

Field	Description
Filter Criteria	Enter or select the criteria or parameter on which you want to construct the filter statement. • **Type**—Type of alarm: System, Chassis, or All. • **Severity**—Severity class of the alarm: Minor or Major. • **Description**—Description of the alarm. Click **X** to clear the search entries.
Time	Displays the date and time that the alarm was registered.
Type	Specifies the type of alarm to monitor: • **System**—System alarms include FRU detection alarms (power supplies removed, for instance). • **Chassis**—Chassis alarms indicate environmental alarms such as temperature. • **All**—Indicates to display all the types of alarms.
Severity	Specifies the alarm severity that you want to monitor • **Major**—A major (red) alarm condition requires immediate action. • **Minor**—A minor (yellow) condition requires monitoring and maintenance. • **All**—Indicates to display all the severities.
Description	Displays the brief synopsis of the alarms you want to monitor.

RELATED DOCUMENTATION

Monitor Traffic Map | 96

CHAPTER 5

Maps and Charts

IN THIS CHAPTER

Monitor Traffic Map

IN THIS SECTION

You are here: **Monitor** > **Maps and Charts** > **Traffic Map**.

NOTE: Traffic Map page is available on all the SRX Series devices except the SRX5000 line of devices.

J-Web supports monitoring traffic through a map. Use this page to visualize inbound and outbound traffic between geographic regions. You can click or hover over the bubble to view more details on the inbound or outbound traffic. The size of the bubble indicates the session count or the bandwidth utilization for a traffic. Traffic with unknown geographical IP addresses and private IP addresses are displayed as question mark icon and lock icon, respectively.

NOTE: To view the data on the Traffic Map page, ensure that security logging is enabled. If not, go to **Device Administration** > **Basic Settings** > **Security Logging** and enable **Stream mode Logging** and **On-box reporting**.

Application Risk Category

The color code of the bubble indicates the risk associated with the application. Table 19 on page 97 shows the application risk categories and the risk values.

Table 19: Application Risk Category and Risk Value

Application Risk Category	Risk Value
Critical	>=5
High	>=4 and <5
Unsafe	>=3 and <4
Moderate	>=2 and <3
Low	>=0 and <2

You can calculate the average risk value using the following formula:

```
Average risk value for a country = Application risk total / Session count total
```

Field Descriptions

Table 20 on page 98 displays the fields of the Traffic Map page.

Table 20: Fields on the Traffic Map Page

Field	Description
By Volume	Displays the bandwidth utilization. This is the default value.
By Session	Displays the total number of traffic sessions.
Inbound Traffic	Displays the traffic coming through the device from the source countries.
Outbound Traffic	Displays the traffic goes through the device to the destination countries. This is the default value.
Top Sources	Displays the top 10, 20 (default value), or 50 source countries with the following details: • **Country**—Displays the country name. • **Risk level**—Displays the risk level category. For example, low, critical, unsafe. • **Avg. risk**—Displays the average risk count. • **Sessions or Bandwidth**—Displays the session count or bandwidth utilization.
Top Destinations	Displays the top 10, 20 (default value), or 50 destination countries with the following details: • **Country**—Displays the country name. • **Risk level**—Displays the risk level category. For example, low, critical, unsafe. • **Avg. risk**—Displays the average risk count. • **Sessions or Bandwidth**—Displays the session count or bandwidth utilization.
View Data	Displays the traffic data for the defined time interval. By default, traffic data for the last five minutes is displayed. You can select the predefined time interval or click **Customize** to customize the time interval by entering date and time. **NOTE**: Starting in Junos OS Release 21.4R1, the default duration is changed from Last 1 hour to Last 5 minutes to speed up the J-Web UI loading process.

Table 20: Fields on the Traffic Map Page *(Continued)*

Field	Description
Search	Enter the country name for which you want to view the data and click the search icon. You can view the country flags before the country names. Click on the country name to view its data.

Tasks You Can Perform

You can perform the following tasks from this page:

- Zoom in and out of the page—Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.
- Refresh the data on the page—Click the refresh icon available below the zoom out icon.
- Pan the page—Click and drag the mouse to pan the page.
- View country-specific details—Hover over the bubble to view the country specific details.

RELATED DOCUMENTATION

Monitor Threats Map | 99

Monitor Threats Map

IN THIS SECTION

You are here: **Monitor** > **Maps and Charts** > **Threats Map**.

NOTE: Threats Map page is available on all the SRX Series devices except the SRX5000 line of devices.

Use this page to visualize incoming and outgoing threats between geographic regions. You can view blocked and allowed threat events based on feeds from intrusion prevention systems (IPS), antivirus, antispam engines, Juniper ATP Cloud, and screen options. You can also click a specific geographical location to view the event count and the top five inbound and outbound IP addresses.

NOTE: To view the data on the Threats Map (Live) page, ensure that:

- Security logging is enabled. If not, go to **Device Administration** > **Basic Settings** > **Security Logging** and enable **Stream mode Logging**.
- Required firewall policy is configured on the device.
- Required licenses are configured for IPS and antivirus.
- Your device is enrolled to the Juniper ATP Cloud server.

The threat data is displayed starting from 12:00 AM (midnight) up to the current time (in your time zone) on that day and is updated every 30 seconds. The current date and time are displayed at the top right and a legend is displayed at the bottom left of the page.

If a threat occurs when you are viewing the page, an animation shows the country from which the threat originated (source) and the country in which the threat occurred (destination).

NOTE: Threats with unknown geographical IP addresses and private IP addresses are displayed as UNKNOWN_COUNTRY.

Field Descriptions

Table 21 on page 101 displays the fields of the Threats Map (Live) page.

Table 21: Fields on the Threats Map (Live) Page

Field	Description
Total Threats Blocked & Allowed	Displays the total number of threats blocked and allowed. Click the hyperlinked number to go to the All Events (**Monitor** > **Logs** > **All Events**) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper ATP Cloud, and screen events.
Threats Blocked & Allowed	Displays the total number of threats blocked and allowed by the following categories: • IPS Threats • Virus • Spam • Screen • Juniper ATP Cloud
Top Destination Countries	Displays the top five destination countries and the number of threats per country.
Top Source Countries	Displays the top five source countries and the number of threats per country.

Threat Types

The Threats Map page displays blocked and allowed threat events based on feeds from IPS, antivirus, antispam engines, Juniper ATP Cloud, and screen options. Table 22 on page 102 describes different types of threats blocked and allowed.

Table 22: Types of Threats

Attack	Description
IPS threat events	Intrusion detection and prevention (IDP) attacks detected by the IDP module. The information reported about the attack (displayed on the IPS (**Monitor** > **Logs** > **Threats** page) includes information about: • Specific events names • Specific event names with either source or destination country
Virus	Virus attacks detected by the antivirus engine. The information reported about the attack (displayed on the Antivirus (**Monitor** > **Logs** > **Threats** page) includes information about: • Specific events names • Specific event names with either source or destination country
Spam	E-mail spam that is detected based on the blacklist spam e-mails. The information reported about the attack (displayed on the Antispam (**Monitor** > **Logs** > **Threats** page) includes information about: • Specific events names • Specific event names with source country
Juniper ATP Cloud	Events that are detected based on Juniper ATP Cloud policies. The information reported about the attack (displayed on the Screen (**Monitor** > **Logs** > **ATP** page) includes information about: • Specific events names • Specific event names with either source or destination country

Table 22: Types of Threats *(Continued)*

Attack	Description
Screen	Events that are detected based on screen options. The information reported about the attack (displayed on the Screen (**Monitor** > **Logs** > **Threats** page) includes information about: • Specific events names • Specific event names with either source or destination country

Tasks You Can Perform

You can perform the following tasks from this page:

- Toggle between updating the data and allowing live updates—Click the **Pause** icon to stop the page from updating the threat map data and to stop animations. Click the **Play** icon to update the page data and resume animations.
- Zoom in and out of the page—Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.
- Pan the page—Click and drag the mouse to pan the page.
- View country-specific details:
  - Click a country on the threat map to view threat information specific to that country. A *Country-Name* pop-up appears displaying country-specific information.
  - Click **View Details** in the *Country-Name* pop-up to view additional details. The *Country-Name (Details)* panel appears.

    Table 23 on page 103 provides more details on the country-specific threat information.

Table 23: Country-Specific Threat Information

Field	Description
Displayed in Country-Name pop-up	

Table 23: Country-Specific Threat Information *(Continued)*

Field	Description
Number of threat events Threat Events since 12:00 am	Displays the total number of threat events (inbound and outbound) since midnight for that country.
Inbound (*Number of threat events*)	Displays the total number of inbound threats for the country and the IP address and the number of events for that IP address for the top five inbound events. Click **View All** to view all the destination IP address with threat events count.
Outbound (*Number of threat events*)	Displays the total number of outbound threats for the country and the IP address and the number of events for that IP address for the top five outbound events. Click **View All** to view all the source IP address with threat events count.
View Details—Displayed in Country-Name (Details) panel	
Number of threat events Threat Events since 12:00 am	Displays the total number of threat events (inbound and outbound) since midnight for that country.

Table 23: Country-Specific Threat Information *(Continued)*

Field	Description
Number of Inbound Events	Displays the total number of inbound threats for the country and the number of inbound threat events for each of the following categories: • IPS Threats • Virus • Spam • Screen • Juniper ATP Cloud Click **Top 5 IP Addresses (Inbound)** to view the IP address and the number of events for that IP address for the top five inbound events. Click **View All IP Addresses** to view all the destination IP addresses and number of events for that IP address. **NOTE**: You can view or select **View All IP Addresses** only after you click **Top 5 IP Addresses (Inbound)**.
Number of Outbound Events	Displays the total number of outbound threats for the country and the number of outbound threat events for each of the following categories: • IPS Threats • Virus • Spam • Screen • Juniper ATP Cloud Click **Top 5 IP Addresses (Outbound)** to view the IP address and the number of events for that IP address for the top five outbound events. Click **View All IP Addresses** to view all the source IP addresses and number of events for that IP address. **NOTE**: You can view or select **View All IP Addresses** only after you click **Top 5 IP Addresses (Outbound)**.

RELATED DOCUMENTATION

Monitor Applications | 106

Monitor Applications

You are here: **Monitor** > **Maps and Charts** > **Applications**.

Use this page to view information about bandwidth consumption, session establishment, and risks associated with your applications. Analyzing your network applications yields useful security management information, such as abnormal applications that can lead to data loss, bandwidth hogging, time-consuming applications, and personal applications that can elevate business risks.

NOTE: Applications page is available on all the SRX Series devices except the SRX5000 line of devices.

NOTE: To view the data on the Applications page, ensure that:

- On-box traffic logging and reporting is enabled. If not, go to **Device Administration** > **Basic Settings** > **Security Logging**, enable **Stream mode Logging** and **On-box Reporting**.
- Logging is enabled for a matching traffic firewall policy. If not, go to **Security Policies & Objects** > **Security Policies** and enable **Logging** options under Rule Options.
- Application tracking is enabled for a security zone. If not, go to **Security Policies & Objects** > **Zones/Screens** and enable **Application Tracking** in the Add Zone page.

You can select either the Grid View tab or the Chart View tab to view your data:

- Grid View—View the comprehensive details of applications in a tabular format that includes sortable columns. You can group the applications using Top users by volume, Top apps by volume, timespan, username, and so on. The table includes information such as the application name, volume, users and so on. Table 24 on page 107 describes the fields on the Grid View page.
- Chart View—View a brief summary of all the applications. It shows the top 50 applications consuming maximum bandwidth in your network. The data is presented graphically as a bubble graph, heat map, or zoomable bubble graph. Table 25 on page 108 describes the widgets on the Chart View page.

Table 24: Applications—Fields on the Grid View Page

Field	Description
Top Users By Volume	Top users of the application; sorted by bandwidth consumption.
Top Apps By Volume	Top applications, such as Amazon, Facebook, and so on of the network traffic; sorted by bandwidth consumption.
Top Category By Volume	Top category, such as web, infrastructure, and so on of the application; sorted by bandwidth consumption.
Top Characteristics By Volume	Top behavioral characteristics, such as prone to misuse, bandwidth consumer, and so on of the application.
Sessions By Risk	Number of events/sessions received; grouped by risk.
Time Span	Allows you to select a time period. Click **Custom** to select a preferred date.
View App Logs	Enables you to view the application logs.
Search	Enables you to search a particular content from the data.
Application Name	Name of the application, such as Amazon, Facebook, and so on.
Risk Level	Risk associated with the application: critical, high, unsafe, moderate, low, and unknown.
Users	Total number of users accessing the application.
Volume	Bandwidth used by the application.
Total Sessions	Total number of application sessions.
Category	Category of the application, such as web, infrastructure, and so on.

Table 24: Applications—Fields on the Grid View Page *(Continued)*

Field	Description
Sub-Category	Subcategory of the application. For example, social networking, news, and advertisements. **NOTE**: There can be many sub-categories for a single category. For example, if the Category is Multimedia, it can have sub-categories as Video-streaming and Audio-streaming and so on.
Characteristics	Characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling. **NOTE**: There can be many characteristics displayed by a comma separator. For example, characteristics can be displayed as **Support File Transfer, Loss of Productivity, Bandwidth.**

Table 25: Applications—Widgets on the Chart View Page

Field	Description
Top 50 Applications	Displays the top 50 application consuming maximum bandwidth in your network. The data is presented graphically as a bubble graph, heat map, or zoomable bubble graph.
Show By	Allows you to reorder the bubble graph by bandwidth or by number of sessions from the drop down. If Bandwidth is selected, the size of the bubble depends on the bandwidth used. Whereas, if Number of Session is selected, the size of the bubble depends upon the number of sessions.
Time Span	Allows you to select a time. Click **Custom** to select a preferred date.
Group By	Allows you to group the bubble graph by bandwidth or by number of sessions from the drop down based on risk or categories.

RELATED DOCUMENTATION

Monitor Users | 109

Monitor Users

You are here: **Monitor** > **Maps and Charts** > **Users**.

Use this page to view information about top users accessing high bandwidth-consuming applications and establishing higher number of sessions on your network. Based on this information, network administrators can control the user by rate-limit a device that is accessing applications which consume large bandwidth or create maximum traffic.

NOTE: Users page is available on all the SRX Series devices except the SRX5000 line of devices.

You can select either the Grid View tab or the Chart View tab to view your data:

- Grid View—View the comprehensive details of users in a tabular format that includes sortable columns. You can group the users using Top users by volume, Top apps by volume, timespan, username etc. The table includes information such as the username, volume, top users by volume and so on. Table 26 on page 109 describes the fields on the Grid View page.
- Chart View—View a brief summary of all the users. It shows the top 50 users consuming maximum bandwidth in your network. The data is presented graphically as a bubble graph, heat map, or zoomable bubble graph. Table 27 on page 110 describes the widgets on the Chart View page.

Table 26: Users—Fields on the Grid View Page

Field	Description
Top Users By Volume	Top users of the application; sorted by bandwidth consumption.
Top Apps By Volume	Top applications, such as Amazon, Facebook, and so on of the network traffic; sorted by bandwidth consumption.
Time Span	Allows you to select a time period. Click **Custom** to select a preferred date.
Username	Name of a user.

Table 26: Users—Fields on the Grid View Page *(Continued)*

Field	Description
Volume	Bandwidth consumption of the user.
Total Sessions	Total number of user sessions.
Applications	All the applications used by a user for the time range.
Search	Enables you to search a particular content from the data.

Table 27: Users—Widgets on the Chart View Page

Field	Description
Top 50 Users	Displays the top 50 users consuming maximum bandwidth in your network. The data is presented graphically as a bubble graph, heat map, or zoomable bubble graph.
Show By	Allows you to reorder the bubble graph by bandwidth or by number of sessions from the drop down. If Bandwidth is selected, the size of the bubble depends on the bandwidth used. Whereas, if Number of Session is selected, the size of the bubble depends upon the number of sessions.
Time Span	Allows you to select a time. Click **Custom** to select a preferred date.

RELATED DOCUMENTATION

Monitor Threat Prevention | 111

CHAPTER 6

Statistics

IN THIS CHAPTER

Monitor Threat Prevention

You are here: **Monitor** > **Statistics** > **Threat Prevention**.

Use this page to verify the statistics of advanced-anti-malware sessions and security Intelligence sessions.

Table 28 on page 111 describes the fields on the Threat Prevention page.

Table 28: Fields on the Threat Prevention Page

Field	Description
Advanced Anti Malware Session Statistics	
Sessions	The following options are available: • **TOTAL**—Specify the TOTAL Session. • **HTTP**—Specify the HTTP Session. • **HTTPS**—Specify the HTTP Session. • **SMTP**—Specify the simple mail transfer protocol session. • **SMTPS**—Specify SMTPS session.

Table 28: Fields on the Threat Prevention Page *(Continued)*

Field	Description
Clear Statistics	Clear the statistics.
Graph	Shows the anti-malware session statistics.
Security Intelligence Session Statistics	
Profiles	Select a profile from the list.
Sessions	The following options are available: • **TOTAL**—Displays the identification number of the Services Processing Unit. • **PERMIT**—Specify the permitted session. • **BLOCK-DROP**—Specify the block drop. • **BLOCK-CLOSE**—Specify the block close. • **CLOSE-REDIRECT**—Specify the closure of the redirect session.
Clear Statistics	Clear the statistics.

RELATED DOCUMENTATION

Monitor VPN Phase I | **112**

Monitor VPN Phase I

You are here: **Monitor** > **Statistics** > **Phase I**.

Use this page to view information related to IKE security associations.

Table 29 on page 113 describes the fields on the Phase I page.

Table 29: Fields on the Phase I Page

Field	Description
IKE Security Associations	
Refresh Interval (sec)	Indicates the duration of time after which you want the data on the page to be refreshed.
Refresh	Click the refresh icon at the top right corner to display the fresh content.
Clear IKE SA	Clears all the IKE SA numbers on the display.
SA Index	Index number of a SA.
Remote Address	IP address of the destination peer with which the local peer communicates.
State	State of the IKE security associations: • DOWN—SA has not been negotiated with the peer. • UP—SA has been negotiated with the peer.
Initiator Cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.
Responder Cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received. **NOTE**: A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.

Table 29: Fields on the Phase I Page *(Continued)*

Field	Description
Mode	Negotiation method agreed upon by the two IPsec endpoints, or peers, used to exchange information. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are: • Main—The exchange is done with six messages. This mode, or exchange type, encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate. • Aggressive—The exchange is done with three messages. This mode, or exchange type, does not encrypt the payload, leaving the identity of the neighbor unprotected.

RELATED DOCUMENTATION

Monitor VPN Phase II | 114

Monitor VPN Phase II

You are here: **Monitor** > **Statistics** > **Phase II**.

Use this page to view IPsec statistics and information related to IPsec security associations.

Table 30 on page 114 describes the fields on the Phase II page.

Table 30: Fields on the Phase II Page

Field	Description
Statistics	
Refresh interval (sec)	Indicates the duration of time after which you want the data on the page to be refreshed.
Refresh	Click the refresh icon at the top right corner to display the fresh content.

Table 30: Fields on the Phase II Page *(Continued)*

Field	Description
Clear	Clears all the data on the display page.
IPsec Statistics —Provides details of the IPsec statistics.	
Counter	Displays the ESP (encrypted and decrypted bytes), AH (input and output), and errors statistics.
Value	Displays the values for the respective statistics.
IPsec SA	
IPsec Security Associations	
ID	Index number of the SA.
Gateway/Port	IP address of the remote gateway/port.
Algorithm	Cryptography scheme used to secure exchanges between peers during the IKE Phase II negotiations: • An authentication algorithm used to authenticate exchanges between the peers. Options are hmac-md5-95 or hmac-sha1-96.
SPI	Security parameter index (SPI) identifier. A SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase I and Phase II.
Life	The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.
Monitoring	Specifies if VPN-Liveliness Monitoring has been enabled/disabled. Enabled - ' U ', Disabled- '—'

Table 30: Fields on the Phase II Page *(Continued)*

Field	Description
Vsys	Specifies the root system.

RELATED DOCUMENTATION

Monitor DHCP Server Bindings | 60

CHAPTER 7

Reports

IN THIS CHAPTER

About Reports Page

IN THIS SECTION

Overview

IN THIS SECTION

You are here: **Monitor** > **Reports**.

Use the Reports menu to generate reports on demand. There are several predefined reports listed in this page, see Table 31 on page 119. The generated report is displayed in HTML format. You can group multiple reports and generate a consolidated report.

NOTE: Reports page is available on all the SRX Series devices except the SRX5000 line of devices.

Logical system and tenant support the reports listed in Table 31 on page 119 only for SRX1500, SRX4100, SRX4200, and SRX4600.

Table 31: Predefined Group Reports and Supported Users

Report Name	Root	Logical System Users	Tenant Users Support
Threat Assessment Report	Yes	Yes	Yes
Application and User Usage	Yes	Yes	Yes
Top Talkers	Yes	Yes	Yes
IPS Threat Environment	Yes	Yes	No
URL Report	Yes	Yes	Yes
Viruses Blocked	Yes	Yes	No
Virus: Top Blocked	Yes	Yes	No
Top Firewall Events	Yes	Yes	Yes
Top Firewall Deny Destinations	Yes	Yes	Yes
Top Firewall Denies	Yes	Yes	Yes
Top IPS Events	Yes	Yes	No
Top Anti-spam Detected	Yes	Yes	No

Table 31: Predefined Group Reports and Supported Users *(Continued)*

Report Name	Root	Logical System Users	Tenant Users Support
Top Screen Attackers	Yes	Yes	Yes
Top Screen Victims	Yes	Yes	Yes
Top Screen Hits	Yes	Yes	Yes
Top Firewall Rules	Yes	Yes	Yes
Top Firewall Deny Sources	Yes	Yes	Yes
Top IPS Attack Sources	Yes	Yes	Yes
Top IPS Attack Destinations	Yes	Yes	No
Top IPS Rules	Yes	Yes	No
Top Web Apps	Yes	Yes	No
Top Applications Blocked	Yes	Yes	No
Top URLs by User	Yes	Yes	No
Top Source Zone by Volume	Yes	Yes	Yes
Top Applications by User	Yes	Yes	Yes
Top Botnet Threats By Source Address via IDP Logs	Yes	Yes	No
Top Botnet Threats by Destination Address via IDP Logs	Yes	Yes	No

Table 31: Predefined Group Reports and Supported Users *(Continued)*

Report Name	Root	Logical System Users	Tenant Users Support
Top Botnet Threats by Threat Severity via IDP Logs	Yes	Yes	No
Top Malware Threats by Source Address via IDP Logs	Yes	Yes	No
Top Malware Threats by Destination Address via IDP Logs	Yes	Yes	No
Top Malware Threats by Threat Severity via IDP Logs	Yes	Yes	No
Top Blocked Applications via Webfilter Logs	Yes	Yes	No
Top Permitted Application Subcategories by Volume via Webfilter Logs	Yes	Yes	No
Top Permitted Application Subcategories by Count via Webfilter Logs	Yes	Yes	No

Generate Reports

To generate a report:

1. Click **Reports**.
2. Select the predefined report name and click **Generate Report**.

   The Report Title window appears.

   NOTE: You can select single or multiple report names or all the predefined report names and generate a consolidated report. But you cannot generate group and individual reports at the same time.

3. Complete the configuration according to the guidelines provided in Table 32 on page 122.
4. Click **Save** to save the generated report in the desired location.

A reported is generated. The report includes, the time when it was generated, the table of contents, and the result (a bar graph, a tabular format, and so on). If there is no data available, the report shows, `No data to display`.

Table 32: Generate Report Settings

Field	Action
Name	Enter a name of the report. Maximum 60 characters.
Customer Name	Enter a customer name. Default value is Juniper.
Description	Enter a description of the report.
Show Top	Use the up and down arrow to select the number of records to display in the report.
Show Details	Select an option from the list: • Top Selected—Displays only the top selected details in the report. • All—Displays all the details in the report. **NOTE**: It may take a while to generate reports, depending on the device data size.
Time Span	Select a predefined time span from the list for the report.
From	Specify a start date and time (in MM/DD/YYYY and HH:MM:SS 12-hour or AM/PM formats) to start the report generation. **NOTE**: This option is available when you choose **Custom** for Time Span.
To	Specify a start date and time (in MM/DD/YYYY and HH:MM:SS 12-hour or AM/PM formats) to stop the report generation. **NOTE**: This option is available when you choose **Custom** for Time Span.
Sorting Options	

Table 32: Generate Report Settings *(Continued)*

Field	Action
Show Details	Click the arrow next to Sorting Options and select one of the options from the list: • Largest To Smallest—Display reports from largest to smallest details. • Smallest To Largest—Display reports from smallest to largest details.

Threat Assessment Report

Threat Assessment report contains the following content:

- Executive Summary
- Application Risk Assessment
- Threat & Malware Assessment
- User and Web Access Assessment

The Threat Assessment report displays a new Filename column in the Malware downloaded by User table. This column helps to identify the malware filename.

Application and User Usage

Application and User Usage report contains the following content:

- Top High Risk Applications by Bandwidth
- Top High Risk Applications By Count
- Top Categories By Bandwidth
- Top Applications By Bandwidth
- Top Categories By Count
- Top Applications By Count
- Top Users Of High Risk Applications By Bandwidth
- Top Users By Bandwidth
- High Risk Applications Allowed Per User
- High Risk Applications Blocked Per User

Top Talkers

Top Talkers report contains the following content:

- Top Source IPs by Bandwidth
- Top Destination IPs by Bandwidth
- Top Source IPs by Session
- Top Destination IPs by Session
- Top Users By Bandwidth
- Top Users By Count

IPS Threat Environment

IPS Threat Environment report contains the following content:

- IPS Attacks by Severity Over Time
- Total IPS Attacks by Severity
- Top IPS Categories Blocked
- Top IPS Attacks Blocked
- Top Targeted Hosts by IP
- Top Targeted Hosts by User

NOTE: IPS Threat Environment report is not supported for tenant users.

Viruses Blocked

Viruses Blocked report contains the following content:

- Total Viruses Blocked Over Time
- Top Viruses Blocked

NOTE: Viruses Blocked is not supported for tenant users.

URL Report

URL Report contains the following content:

- Top URLs by Bandwidth
- Top URLs by Count
- Top URL Categories by Bandwidth
- Top URL Categories by Count
- Total URLs Blocked Over Time
- Top Blocked URLs
- Top Blocked URL Categories by Count
- Users With Most Blocked URLs

Virus: Top Blocked

Virus: Top Blocked report contains Virus: Top Blocked content.

NOTE: Virus: Top Blocked is not supported for tenant users.

Top Firewall Events

Top Firewall Events report contains Top Firewall Events.

Top Firewall Deny Destinations

Top Firewall Deny Destinations report contains Top Firewall Deny Destinations.

Top Firewall Denies

Top Firewall Denies report contains Top Firewall Denies.

Top IPS Events

Top IPS Events report contains Top IPS Events.

NOTE: Top IPS Events is not supported for tenant users.

Top Anti-spam Detected

Top Anti-Spam Detected report Top Anti-spam Detected.

NOTE: Top Anti-spam Detected is not supported for tenant users.

Top Screen Attackers

Top Screen Attackers report contains Top Screen Attackers.

Top Screen Victims

Top Screen Victims report contains Top Screen Victims.

Top Screen Hits

Top Screen Hits report contains Top Screen Hits.

Top Firewall Rules

Top Firewall Rules report contains Top Firewall Rules.

Top Firewall Deny Sources

Top Firewall Deny Sources report contains Top Firewall Deny Sources.

Top IPS Attack Sources

Top IPS Attack Sources report contains Top IPS Attack Sources.

Top IPS Attack Destinations

Top IPS Attack Destinations report contains Top IPS Attack Destinations.

NOTE: Top IPS Attack Destinations is not supported for tenant users.

Top IPS Rules

Top IPS Rules report contains Top IPS Rules.

NOTE: Top IPS Rules is not supported for tenant users.

Top Web Apps

Top Web Apps report contains Top Web Apps.

NOTE: Top Web Apps is not supported for tenant users.

Top Applications Blocked

Top Applications Blocked report contains Top Applications Blocked.

NOTE: Top Applications Blocked is not supported for tenant users.

Top URLs by User

Top URLs by User report contains Top URLs by User.

NOTE: Top URLs by User is not supported for tenant users.

Top Source Zone by Volume

Top Source Zone by Volume report contains Top Source Zone by Volume.

Top Applications by User

Top Applications by User report contains Top Applications by User.

Top Botnet Threats By Source Address via IDP Logs

Top Botnet Threats By Source Address via IDP Logs report contains Top Botnet Threats By Source Address via IDP Logs.

NOTE: Top Botnet Threats By Source Address via IDP Logs is not supported for tenant users.

Top Botnet Threats by Destination Address via IDP Logs

Top Botnet Threats by Destination Address via IDP Logs report contains Top Botnet Threats by Destination Address via IDP Logs.

NOTE: Top Botnet Threats by Destination Address via IDP Logs is not supported for tenant users.

Top Botnet Threats by Threat Severity via IDP Logs

Top Botnet Threats by Threat Severity via IDP Logs report contains Top Botnet Threats by Threat Severity via IDP Logs.

NOTE: Top Botnet Threats by Threat Severity via IDP Logs is not supported for tenant users.

Top Malware Threats by Source Address via IDP Logs

Top Malware Threats by Source Address via IDP Logs report contains Top Malware Threats by Source Address via IDP Logs.

NOTE: Top Malware Threats by Source Address via IDP Logs is not supported for tenant users.

Top Malware Threats by Destination Address via IDP Logs

Top Malware Threats by Destination Address via IDP Logs report contains Top Malware Threats by Destination Address via IDP Logs.

NOTE: Top Malware Threats by Destination Address via IDP Logs is not supported for tenant users.

Top Malware Threats by Threat Severity via IDP Logs

Top Malware Threats by Threat Severity via IDP Logs report contains Top Malware Threats by Threat Severity via IDP Logs.

NOTE: Top Malware Threats by Threat Severity via IDP Logs is not supported for tenant users.

Top Blocked Applications via Webfilter Logs

Top Blocked Applications via Webfilter Logs report contains Top Blocked Applications via Webfilter Logs.

NOTE: Top Blocked Applications via Webfilter Logs is not supported for tenant users.

Top Permitted Application Subcategories by Volume via Webfilter Logs

Top Permitted Application Subcategories by Volume via Webfilter Logs report contains Top Permitted Application Subcategories by Volume via Webfilter Logs.

NOTE: Top Permitted Application Subcategories by Volume via Webfilter Logs is not supported for tenant users.

Top Permitted Application Subcategories by Count via Webfilter Logs

Top Permitted Application Subcategories by Count via Webfilter Logs report contains Top Permitted Application Subcategories by Count via Webfilter Logs.

NOTE: Top Permitted Application Subcategories by Count via Webfilter Logs is not supported for tenant users.

PART 5

Device Administration

CHAPTER 8

Basic Settings

IN THIS CHAPTER

Configure Basic Settings

You are here: **Device Administration** > **Basic Settings**.

Use this page to configure your device basic settings.

You can do the following:

- **Save**—Saves all the basic settings configuration and returns to the main configuration page.

  NOTE: For all the configuration options under Basic Settings:

  - Tool tip on the right-side represents different icons for notifications, validation errors, and successful configuration.
  - When you make a configuration change and navigate to a different page without saving it, a pop-up message is displayed to save the configuration.

- **Cancel**—Cancels all your entries and returns to the main configuration page.
- **Commit**—Commits all the basic settings configuration and returns to the main configuration page.
- Expand all—Click the arrow pointing outwards icon to expand all the options.
- Collapse all—Click the arrow pointing inwards to collapse or hide all the options.

Table 33 on page 133 describes the fields on the Basic Settings page.

Table 33: Fields on the Basic Settings Page

Field	Action
System Identity	
Hostname	Enter a hostname for the device.
Domain name	Enter a domain name to specify the network or subnetwork to which the device belongs.
Root password	Enter a password for the root user. **NOTE**: After you have defined a root password, that password is required when you log in to the J-Web or the CLI.
Confirm root password	Re-enter the password to confirm.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
DNS servers	Select an option to specify the DNS server settings: • To specify a server that the device can use to resolve hostnames into addresses: 1. Click **+** at the top right side of the DNS Servers table. 2. Enter an IPv4 address of the server. 3. Click the tick mark to save the changes. Else, click the cancel (**X**) icon to discard the changes. • To edit an existing DNS server hostname: 1. Select a DNS server hostname that you want to edit. 2. Click the pencil icon at the top right side of the DNS Servers table or right-click on the hostname and edit the IPv4 address. 3. Click the tick mark to save the changes. Else, click the cancel (**X**) icon to discard the changes. • To remove an existing DNS server hostname, select it and click the delete icon at the top right side of the DNS Servers table or right-click on the hostname and delete it.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Domain search	Select an option: • To add a domain name: 1. Click **+** at the top right side of the Domain Search table. 2. Enter a domain name. The string must contain an alphanumeric character and can include underscores, hyphen, slash and dot. No spaces allowed. 3. Click the tick mark to save the changes. Else, click the cancel (**X**) icon to discard the changes. • To edit an existing domain name: 1. Select a domain name that you want to edit. 2. Click the pencil icon at the top right side of the Domain Search table or right-click on the domain name and edit the name. 3. Click the tick mark to save the changes. Else, click the cancel (**X**) icon to discard the changes. • To remove an existing domain name, select it and click the delete icon at the top right side of the Domain Search table or right-click on the name and delete it.
Time	
Time zone	Select the time zone from the list in which the router resides.
Time source	Select an option from the list to set the system time:

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
	NTP Servers—Synchronizes the system time with the NTP server that you select. Click one of the following options: • **Add**—Click **+** to add an NTP server. Then, enter the NTP server name, key, and Routing Instance. Select an option from the list for Version and Prefer. • **Edit**—Select an existing NTP server that you want to edit and click the pencil icon available at the upper right of the NTP Server table. You can also right-click on the NTP server and click Edit Row. Then, edit the key and version and click the tick mark. • **Delete**—Select an existing NTP server that you want to delete and click the delete icon available at the upper right of the NTP Server table. You can also right-click on the NTP server and click Delete Row. Click **Yes** to delete the selected server.
	Computer—Uses the computer that you are currently logged into to determine the system time for the device. **NOTE**: When you select this option, the PC time that will be used is displayed in the **Current Date & Time** field.
	Manual—Enables you to manually select the date and time for the device. Set the date and time using the calendar pick tool and time fields. **NOTE**: After you configure the time manually, the session will expire. Log in to J-Web.
Device date & time	Displays the device date and time.
Current date & time	Displays the current date and time.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Management and Loopback Address	
Management address	Enter IPv4 address for the device.
Subnet	Enter subnet of the IPv4 address.
Loopback address	Enter IP address and subnet for the loopback address. **NOTE**: If the SRX Series Firewall does not have a dedicated management port (fxp0), then Loopback Address and Subnet are the only options available for the management access configuration.
Subnet	Enter the address, for example, 255.255.255.0. You can also specify the address prefix. Specifies the range of logical addresses within the address space that is assigned to an organization.
Default gateway	Enter the default gateway address for IPv4.
System Services	
Telnet	Select this option to enable telnet.
SSH	Select this option to enable SSH connections.
FTP	Select this option to enable FTP for secure file transfer.
NETCONF	Select this option to enable NETCONF connections.
Junoscript over SSL	Select this option to enable Junoscript connections over SSL.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Junoscript certificate	Select the local certificate for SSL from the list.
Interface	Select the interface in order of your preference and click on the left arrow/right arrow to add.
HTTPS	Select this option to enable HTTPS connection settings.
Interface	Select the interface in order of your preference and click on the left arrow/right arrow to add.
HTTPS certificate	Specifies the certificate that you want to use to secure the connection from the HTTPS certificates list when you enable HTTPs. Select the HTTPS certificate from the list.
PKI certificate	Select the PKI certificate for HTTPS from the list. **NOTE**: This option is available only if you select pki-local-certificate in the HTTPS Certificate options.
Local certificate	Select the local certificate for HTTPS from the list. **NOTE**: This option is available only if you select local-certificate in the HTTPS Certificate options.
Web API	Select to enable Web API configuration.
Client	Select to enable client for the Web API.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Hostname	Provides the address of permitted HTTP/HTTPS request originators. To add, click **+** and enter the IPv4 address of the permitted HTTP/HTTPS request originator and click tick mark to save the changes. To delete, select the hostname and click the delete icon. Then, click **Yes** to delete it.
HTTP	Select to enable unencrypted HTTP connection settings.
HTTP port	Click top or bottom arrows to select the TCP ports for incoming HTTP connections.
HTTPs	Select to enable encrypted HTTPS connection settings.
HTTPS port	Click top or bottom arrows to select the TCP ports for incoming HTTP connections.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action

Certificate type	Select to specify the certificate that you want to use to secure the connection from the HTTPS certificates list when you enable HTTPs for Web API:
	• Default—Selects the default system generated certificate.
	• PKI Certificate—Select a PKI certificate from the list for HTTPS of Web API.
	• File Path:
	  • File Path—Click **Browse** and select a certificate from your desired location. Or click **Upload** and upload the selected certificate.
	  • **Certificate**—Displays the file path of the uploaded certificate.
	  • **Certificate Key**:
	  • **Browse**—Click and select the certificate key from your desired location.
	  • **Upload**—Click and upload the selected certificate key.
	  • **Certificate Key**—Displays the file path of the uploaded certificate key.

User	Select this option to enable user credentials.
Name	Enter a username.
Password	Enter the user password.
REST API	Enable this option to allow RPC execution over HTTP(S) connection.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Explorer	Select this option to enable REST API explorer.
Control	Select this option to enable control the REST API process.
Allowed sources	Provides the source IP address. Click **+** and enter the IPv4 address of the source. Then, click tick mark. To delete, select an existing address and click the delete icon. Then, click **Yes** to delete it.
Connection limit	Click top or bottom arrows to select the number of simultaneous connections.
HTTP	Select to enable unencrypted HTTP connections for REST API.
Address	Click **+** and enter the IPv4 address for the incoming connections for HTTP of REST API. Then, click tick mark to add it. To delete, select an existing address and click the delete icon. Then, click **Yes** to delete it.
Port	Click top or bottom arrows to select the HTTP port to accept HTTP connections for REST API. **NOTE**: The default port for HTTP of REST API is 3000.
HTTPS	Select to enable encrypted HTTPS connections for REST API.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Address	Click **+** and enter the IPv4 address for the incoming connections for HTTPS of REST API. Then, click tick mark to add it. To delete, select an existing address and click the delete icon. Then, click **Yes** to delete it.
Cipher list	Select the Cipher suites in order of your preference and click on the left arrow or right arrow to add.
Port	Click top or bottom arrows to select the HTTPS port to accept the HTTPS connection of REST API. **NOTE**: The default port for HTTPS of REST API is 3443.
Server certificate	Select server certificate from the list. See "Import a Device Certificate" on page 233 to import a device certificate.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action

CA Profile	Select the certificate authority profile for HTTPS of REST API from the list.
	
	To create Certificate Authority inline:
	
	• Click **Create Certificate Authority Profile**.
	
	• Enter the following details:
	
	  • **CA Profile ***—Enter the CA profile name.
	
	  • **CA Identifier ***—Enter the CA identifier.
	
	  • **File Path on Device for Certificate**:
	
	  • **Browse**—Click and select the certificate from your desired location.
	
	  • **Upload**—Click and upload the selected certificate.
	
	  • **File Path on Device for Certificate**—Displays the file path of the selected certificate.
	
	• Click **OK**.

Security Logging	
Stream mode logging	Select this option to enable logging. **NOTE**: The **Enable Traffic Logs** option is available for user logical system and tenants.
UTC timestamp	Select this option to enable UTC Timestamp for security log timestamps.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Log on	Select one of the log on types for logging. • **Source Address**—Select this option to enter the source IP address. • **Source Interface**—Select this option to select a source interface from the list.
IP address	Enter the source IP address. **NOTE**: This option is available if you select the log on type as **Source Address**.
Format	Specifies the format in which the logs are stored. Select a format in which the logs are stored from the list. • binary—Binary encoded text to conserve resources. • SD-Syslog—Structured system log file. • Syslog—Traditional system log file. By default, None logging format is selected.
Transport protocol	Select an option from the list to specify the type of logging transport protocol: • TCP—Select this option to set the transport protocol to TCP. • UDP—Select this option to set the transport protocol to UDP. • TLS—Select this option to set the transport protocol to TLS. By default, **None** is selected.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Connections	Select the TCP or TLS connections for logging using up and down arrows. **NOTE**: This option is available if you select the transport protocol option as **TCP** or **TLS**.
TLS profile	Select a TLS profile from the list. **NOTE**: This option is available if you select the transport protocol option as **TLS**.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Syslog server	Enables you to configure syslog servers. You can configure a maximum of three syslog servers. Perform one of the following tasks: 1. To create syslog server, click **+**, enter the following details and then click **OK**. • **Name**—Enter the name of the new stream configuration. • **Save At**—Select the location from the list to save the stream. • **Type**—Select a format in which the logs are stored from the list. The log types are: • Structure • Standard • Web • **Host**—Enter the IP address for the stream host name. 2. To edit an existing syslog server, select it and click the pencil icon. Then, edit the saving mode, streaming type, and host in the Edit Syslog page and click **OK**. 3. To delete an existing syslog server, select it and click the delete icon.
On-box reporting	Enable this option to generate on-box reports. **NOTE**: We recommend you use Stream mode logging to syslog server.
SNMP	

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Contact information	Enter any contact information for the administrator of the system (such as name and phone number).
System description	Enter any information that describes the system.
Local engine ID	Enter the MAC address of Ethernet management port 0. Specifies the administratively unique identifier of an SNMPv3 engine for system identification. The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. Generally, the local engine ID suffix is the MAC address of Ethernet management port 0.
System location	Enter any location information for the system (lab name or rack name, for example).
System name override	Specifies the option to override the system hostname. Enter the name of the system.
Community	Specifies the name and authorization for the SNMP community. • Click **+**. • Enter the name of the community being added. • Select the desired authorization (either read-only or read-write) from the list. Click tick mark.
Trap groups	

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Name	Click **+** to add a trap group. Enter the SNMP trap group being configured.
Categories	Select trap categories to add to the trap group being configured. The options available are: • Authentication • Chassis • Configuration • Link • Remote operations • RMON alarm • Routing • Startup • CRRP events
Targets	Specifies one or more IP addresses that specify the systems to receive SNMP traps that are generated by the trap group being configured. Click **+**, enter the target IP address for SNMP trap group, and click tick mark.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Health monitoring	Enable the option to check the SNMP health monitor on the device. The health monitor periodically checks the following key indicators of device health: • Percentage of file storage used • Percentage of Routing Engine CPU used • Percentage of Routing Engine memory used • Percentage of memory used for each system process • Percentage of CPU used by the forwarding process • Percentage of memory used for temporary storage by the forwarding process
Interval	Specifies the sampling frequency interval, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds. For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds. Select a value from 1 through 24855. The default value is 300 seconds.
Rising threshold	Specifies the value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is increasing. For example, if the rising threshold is 90, SNMP generates an event when the value of any key indicator reaches or exceeds 90 seconds. Select a value from 1 through 100. The default value is 90 seconds.

Table 33: Fields on the Basic Settings Page *(Continued)*

Field	Action
Falling threshold	Specifies a value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is decreasing. For example, if the falling threshold is 80, SNMP generates an event when the value of any key indicator falls back to 80 seconds or less. Select a value 0 through 100. The default value is 80 seconds.
Redundant PSU **NOTE**: SRX380 devices support power supply redundancy for power management.	
Power Supply 0	Displays if the power supply is present or not.
Power Supply 1	Displays if the redundant power supply is present or not.
PSU Redundancy	Enable this option to manage power on the SRX380 device. **NOTE**: This option is available only when the device is in the standalone mode.

RELATED DOCUMENTATION

Reset Configuration and Rerun Setup Wizard | 361

CHAPTER 9

Cluster Management

IN THIS CHAPTER

Configure Cluster (HA) Setup

Before you begin:

- Establish a chassis cluster connection between the two units, ensure that you have physical access to both the devices.
- You must configure the two devices separately.
- Your other unit must be on the same hardware and software version as the current unit.
- Note that both units are erased and rebooted, after which all existing data is irretrievable. You have the option to save a backup copy of your configuration before rebooting.

You are here: **Device Administration** > **Cluster Management** > **Cluster Configuration**.

The Junos OS provides high availability on SRX Series device by using chassis clustering. SRX Series Services Gateways can be configured to operate in cluster mode, where a pair of devices can be connected together and configured to operate like a single node, providing device, interface, and service level redundancy.

A chassis cluster can be configured in the following modes:

- Active/passive mode: In active/passive mode, transit traffic passes through the primary node while the backup node is used only in the event of a failure. When a failure occurs, the backup device becomes primary and takes over all forwarding tasks.
- Active/active mode: In active/active mode, has transit traffic passing through both nodes of the cluster all of the time.

NOTE: In the J-Web cluster (HA) setup, you can only configure active/passive mode (RG1).

You can set up chassis cluster using a simplified Cluster (HA) Mode wizard when the standalone SRX Series devices are in factory default. You can also create HA using the same wizard from Device Administration > Reset Configuration when the devices are already in the network.

NOTE: In the factory default settings, a warning message is displayed in SRX300, SRX320, SRX320-POE, SRX340, SRX345, and SRX380 devices to disconnect the ports between the two nodes. This is to avoid displaying the details of the other nodes.

Device Administration > **Cluster Management** > **Cluster Configuration**

To set up cluster (HA):

1. Select **Cluster (HA) Setup**.

   NOTE: For the secondary node to be set up or if the primary and secondary nodes are not already connected, click **Proceed**. If you want to set up the primary node, then disconnect back to back connected ports between the two nodes and click **Refresh** to reload the browser.

   The Setup Chassis Cluster wizard page appears. This wizard guides you through configuring chassis cluster on a two-unit cluster.

   Select the unit

   The welcome page shows the possible chassis cluster connections that you can configure for your SRX Series device. It shows a graphical representation for primary unit (Node 0) and secondary unit (Node 1) and guides you to first configure the primary unit (node 0).

2. Select **Yes, this is the primary unit (Node 0).** to select the unit.

NOTE: If you have already configured the primary node settings, then select **No, this is the secondary unit (Node 1)** and follow the instructions from Step 8.

3. Click **Next**.
4. To configure the primary unit, complete the configuration according to the guidelines provided in Table 34 on page 153.

Table 34: Primary Unit Configuration

Field	Description	Action
System Identity		
Node 0 Cluster ID	Specifies the number by which a cluster is identified.	Enter a number from 1 through 255. By default, 1 is assigned.
Node 0 Priority	Specifies the device priority for being elected to be the primary device in the VRRP group.	Enter a number from 1 through 255. By default, 200 is assigned.
Node 1 Priority	Specifies the device priority for being elected to be the primary device in the VRRP group.	Enter a number from 1 through 255. By default, 100 is assigned.
Node 0 Host Name	Specifies the device host name of the node 0.	By default, host name is assigned. For example, SRX1500-01.
Node 1 Host Name	Specifies the device host name of the node 1.	By default, host name is assigned. For example, SRX1500-02.
Allow root user SSH login	Allows users to log in to the device as root through SSH.	Enable this option.
Management Interface		
IPv4 Address **NOTE**: Make a note of the IPv4 address as you need it to access the settings after you commit the configuration.		

Table 34: Primary Unit Configuration *(Continued)*

Field	Description	Action
Node 0 Management IPv4	Specifies the management IPv4 address of node 0.	Enter a valid IPv4 address for the management interface.
Node 0 Subnet Mask	Specifies subnet mask for IPv4 address.	Enter a subnet mask for the IPv4 address.
Node 1 Management IPv4	Specifies the management IPv4 address of node 1.	Enter a valid IPv4 address for the management interface.
Node 1 Subnet Mask	Specifies subnet mask for IPv4 address.	Enter a subnet mask for the IPv4 address.
Static Route IP	Defines how to route to the other network devices.	Enter an IPv4 address for the static route.
Static Route Subnet	Specifies the subnet for the static route IPv4 address.	Enter a subnet mask for the static route IPv4 address.
Next Hop IPv4	Specifies next hop gateway for the IPv4 address.	Enter a valid IPv4 address for the next hop.
IPv6 Address (Optional)		
Node 0 Management IPv6	Specifies the management IPv6 address of node 0.	Enter a valid IPv6 address for the management interface.
Node 0 Subnet Prefix	Specifies subnet prefix for IPv6 address.	Enter a subnet prefix for the IPv6 address.
Node 1 Management IPv6	Specifies the management IPv6 address of node 1.	Enter a valid IPv6 address for the management interface.
Node 1 Subnet Prefix	Specifies subnet prefix for IPv6 address.	Enter a subnet prefix for the IPv6 address.

Table 34: Primary Unit Configuration *(Continued)*

Field	Description	Action
Static Route IPv6	Defines how to route to the other network devices.	Enter an IPv6 address for the static route.
Static Route Subnet Prefix	Specifies the subnet prefix for the static route IPv6 address.	Enter a subnet prefix for the static route IPv6 address.
Next Hop IPv6	Specifies next hop gateway for the IPv6 address.	Enter a valid IPv6 address for the next hop.
Device Password		
Root Password	Specifies root password of the device.	Enter root password if not already configured for the device.
Re-Enter Password	-	Reenter the root password.
Control Ports **NOTE**: This option is available only for SRX5600 and SRX5800 devices.		

Table 34: Primary Unit Configuration *(Continued)*

Field	Description	Action

Dual Link	Provides redundant link for failover.	By default, this option is disabled.
		Once you enable this option, the following fields appear:
		• **Link 1**
		  • Node 0 FPC—Select an option from the list.
		  • Node 0 Port—Select an option from the list.
		  • Node 1 FPC.
		  • Node 1 Port.
		• **Link 2 (Optional)**
		  • Node 0 FPC—Select an option from the list.
		  • Node 0 Port—Select an option from the list.
		  • Node 1 FPC.
		  • Node 1 Port.

Node 0 FPC	Specifies FPC slot number on which to configure the control port.	Select an option from the list.
Node 0 Port	Specifies port number on which to configure the control port.	Select an option from the list.
Node 1 FPC	Optional. Specifies FPC slot number on which to configure the control port.	Select an option from the list.

Table 34: Primary Unit Configuration *(Continued)*

Field	Description	Action
Node 1 Port	Optional. Specifies port number on which to configure the control port.	Select an option from the list.
Save Backup (Optional)		
Save Backup (to client)	Saves backup of the current configuration to the client local machine. **NOTE**: When restarting the primary unit, J-Web deletes the existing configuration to configure chassis cluster. Therefore, it is recommended that you save a backup file of your current settings before committing the new configuration.	Enable the option to save the backup file of your settings.

5. Click **Reboot and Continue** to restart the primary unit to configure chassis cluster.
6. After rebooting the primary unit (node 0), connect to the management port of the secondary unit to switch to the secondary unit.
7. Click **Refresh** if the management IP address of the secondary unit is same as the existing device default IP address. If not, open a new browser with the new secondary device IP address.
8. To configure the secondary unit, complete the configuration according to the guidelines provided in Table 35 on page 157.

Table 35: Secondary Unit Configuration

Field	Description	Action
Secondary Unit Information		

Table 35: Secondary Unit Configuration *(Continued)*

Field	Description	Action
Cluster ID	Specifies the number by which a cluster is identified. **NOTE**: Cluster ID must be same for both primary and secondary units.	Enter a number from 1 through 255. By default, 1 is assigned.
Device Password		
Root Password	Specifies root password of the device.	Enter new root password.
Re-Enter Password	-	Reenter the root password.
Control Ports **NOTE**: This option is available only for SRX5600 and SRX5800 devices.		

Table 35: Secondary Unit Configuration *(Continued)*

Field	Description	Action

Dual Link	Provides redundant link for failover.	By default, this option is disabled.
		Once you enable dual link option, the following fields appear:
		• **Link 1**
		  • Node 0 FPC—Select an option from the list.
		  • Node 0 Port—Select an option from the list.
		  • Node 1 FPC.
		  • Node 1 Port.
		• **Link 2 (Optional)**
		  • Node 0 FPC—Select an option from the list.
		  • Node 0 Port—Select an option from the list.
		  • Node 1 FPC.
		  • Node 1 Port.

Node 0 FPC	Specifies FPC slot number on which to configure the control port.	Select an option from the list.
Node 0 Port	Specifies port number on which to configure the control port.	Select an option from the list.
Node 1 FPC	Optional. Specifies FPC slot number on which to configure the control port.	Select an option from the list.

Table 35: Secondary Unit Configuration *(Continued)*

Field	Description	Action
Node 1 Port	Optional. Specifies port number on which to configure the control port.	Select an option from the list.
Save Backup (Optional)		
Save Backup (to client)	Saves backup of the current configuration to the client local machine. **NOTE**: When restarting the secondary unit, J-Web deletes the existing configuration to configure chassis cluster. Therefore, it is recommended that you save a backup file of your current settings before committing the new configuration.	Enable the option to save the backup file of your settings.

9. Click **Reboot and Continue** to restart the secondary unit to configure chassis cluster.
10. After rebooting the secondary unit (node 1), launch the J-Web UI using primary unit management IP address.
11. Navigate to **Cluster Management** > **Cluster (HA) Setup**.

    The Cluster Wizard page will open and displays the Cluster Status step.

NOTE:

- J-Web uses `show chassis cluster status` to verify control link status. Number on the link signifies if it is single (1) or dual links (2).

  The control and fabric link status colors are as follows:

  - Green—Indicates that the links are up.
  - Red—Indicates that the links are down.

- Orange—Indicates that one of the dual links is up.
- Grey—Indicates that the fabric link is not configured.

- If chassis cluster is not connected, then the connection is failed and all possible failure reasons will be displayed. For information on troubleshooting tips, see Juniper Knowledge Search.
- You can configure fabric link only after the chassis cluster is formed. For the first time configuration, the chassis status displays as `The fabric ports links is not yet configured`.

12. To configure fabric link, complete the configuration according to the guidelines provided in Table 36 on page 161.

Table 36: Fabric Link Configuration

Field	Description	Action
Fabric Link Details		
Dual Link	Provides redundant link for failover.	Enable this option.
Link 1		
Fabric 0	Specifies the fabric port link for node 0.	Select an interface from the list.
Fabric 1	Specifies the fabric port link for node 1.	-
Link 2 (Optional)		
Fabric 0	Specifies the secondary fabric port link for node 0.	Select an interface from the list.
Fabric 1	Specifies the secondary fabric port link for node 1.	-

13. Click **Configure Link**.
14. Click **Next**.

15. To add redundant Ethernet (reth) interface, click **+** and complete the configuration according to the guidelines provided in Table 37 on page 162.

> **NOTE**: You can also use the pencil icon to edit the reth interface and delete icon to delete the reth interfaces.

Table 37: Add Reth Interface

Field	Description	Action
RETH Name	Specifies the reth interface name.	Enter a name for reth interface.
Node 0 Interfaces	Specifies the list of Node 0 interfaces.	Select an interface from the Available column and move it to the Selected column.
Node 1	Specifies the Node 1 interfaces based on the node 0 interfaces.	-
Advance Settings		
LACP Configuration	Optional. Configure Link Aggregation Control Protocol (LACP).	-
LACP Mode	Optional. Specifies the LACP mode. Available options are: • active—Initiate transmission of LACP packets. • passive—Respond to LACP packets. • periodic—Interval for periodic transmission of LACP packets.	Select an option from the list.

Table 37: Add Reth Interface *(Continued)*

Field	Description	Action
Periodicity	Optional. Specifies the interval at which the interfaces on the remote side of the link transmit link aggregation control protocol data units (PDUs). Available options are: • fast—Transmit link aggregation control PDUs every second. • slow—Transmit link aggregation control PDUs every 30 seconds.	Select an option from the list.
Description	Optional. Specifies the description for LACP.	Enter a description.
VLAN Tagging	Optional. Specifies whether or not to enable VLAN tagging.	Enable this option.
Redundancy Group	Specifies the number of the redundancy group that the reth interface belongs to.	-

16. Click **Save**.

    Virtual reth interface is created.

17. To add a logical interface to the new virtual reth interfaces, complete the configuration according to the guidelines provided in Table 38 on page 163.

Table 38: Add Reth Logical Interface

Field	Description	Action
General		
Reth Interface Name	Specifies the name of the reth interface.	Enter a name for the reth interface.
Logical Interface Unit	Specifies the logical interface unit.	Enter the logical interface unit.

Table 38: Add Reth Logical Interface *(Continued)*

Field	Description	Action
Description	Specifies the description of the reth interface.	Enter the description.
VLAN ID	Optional. Specifies the VLAN ID.	Enter the VLAN ID.
IPv4 Address		
IPv4 Address	Specifies the IPv4 address.	Click **+** and enter a valid IP address.
Subnet Mask	Specifies the subnet mask for IPv4 address.	Enter a valid subnet mask.
IPv6 Address (Optional)		
IPv6 Address	Specifies the IPv6 address.	Enter a valid IP address.
Prefix Length	Specifies the number of bits set in the subnet mask.	Enter the prefix length.

18. Click **OK**.
19. To configure zones, complete the configuration according to the guidelines provided in Table 39 on page 165.

NOTE:

- With factory default configuration, trust and untrust zones are displayed by default.
- You can edit the security zone, add new zones, and delete the newly added zones. You will receive an error message while committing if you try to delete a default zone. This is because, the default zones are referenced in the security policies.
- You can also edit zone description, application tracking, source identity log, interfaces, system services, protocols, and traffic control options.

Table 39: Create Zones

Field	Description	Action
General Information		
Name	Specifies the name of the zone.	Enter a name for the zone.
Description	Specifies a description for the zone.	Enter a description for the zone.
Application Tracking	Enables application tracking (AppTrack) to collect statistics for the application usage on the device, and when the session closes	Enable this option.
Source Identity Log	Specifies the source-identity-log parameter as part of the configuration for a zone to enable it to trigger user identity logging when that zone is used as the source zone (from-zone) in a security policy.	Enable this option.
Interfaces		
Interfaces	Specifies the list of reth interfaces available.	Select an interface from the Available column and move it to the Selected column.
System Services		
Except	Drops the selected services.	Enable this option if you want to drop the selected services.
Services	Specify the types of incoming system service traffic that can reach the device for all interfaces in a zone.	Select a service from the Available column and move it to the Selected column.
Protocols		
Except	Drops the selected protocols.	Enable this option if you want to drop the selected protocols.

Table 39: Create Zones *(Continued)*

Field	Description	Action
Protocols	Specify the types of routing protocol traffic that can reach the device on a per-interface basis.	Select a protocol from the Available column and move it to the Selected column.
Traffic Control Options		
TCP Reset	Specifies the device to send a TCP segment with the RST (reset) flag set to 1 (one) in response to a TCP segment with any flag other than SYN set and that does not belong to an existing session.	Enable this option.

20. Click **OK**.
21. Click **Finish**.

    A cluster setup success message appears.

    If you click the Cluster (HA) Setup menu again, a cluster setup success message appears, and you can click **Cluster Configuration** to view and edit the chassis cluster configuration.

> **NOTE**: If the chassis cluster configuration fails after you click **Finish**, then edit the configuration as required and commit the changes again.

RELATED DOCUMENTATION

About the Cluster Configuration Page | 166

About the Cluster Configuration Page

IN THIS SECTION

You are here: **Device Administration** > **Cluster Configuration**.

Use this page to add, edit, or delete chassis cluster configuration.

Tasks You Can Perform

You can perform the following tasks from this page:

- Edit Node settings. See "Edit Node Settings" on page 169.
- Add an HA cluster interface. See "Add an HA Cluster Interface" on page 170.
- Edit an HA cluster interface. See "Edit an HA Cluster Interface" on page 172.
- Delete HA cluster interface. See "Delete HA Cluster Interface" on page 172.
- Add a redundancy group. See "Add a Redundancy Group" on page 173.
- Edit a redundancy group. See "Edit a Redundancy Group" on page 175.
- Delete redundancy group. See "Delete Redundancy Group" on page 176.

Field Descriptions

Table 40 on page 167 and Table 41 on page 168 describes the fields on the Cluster Configuration page.

Table 40: Fields on the Node Settings Page

Field	Description
Node ID	Displays the node ID.
Cluster ID	Displays the cluster ID configured for the node.
Host Name	Displays the name of the node.

Table 40: Fields on the Node Settings Page *(Continued)*

Field	Description
Backup Router	Displays the IP address used while booting.
Management Interface	Displays the management interface of the node.
IP Address	Displays the management IP address of the node.
Status	Displays the state of the redundancy group. • **Primary**–Redundancy group is active. • **Secondary**–Redundancy group is passive.

Table 41: Fields on the HA Cluster Settings Page

Field	Action
Interfaces	
Global Settings	To configure the global settings: 1. Click **Global Settings** at the upper right side of the Interfaces table. The Global Settings window appears. 2. Enter the number of redundant Ethernet (reth) interfaces allowed. Range is 1 through 128. 3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
Name	Displays the physical interface name.
Member Interfaces/IP Address	Displays the member interface name or IP address configured for an interface.
Redundancy Group	Displays the redundancy group.

Table 41: Fields on the HA Cluster Settings Page *(Continued)*

Field	Action
Redundancy Group	
Group	Displays the redundancy group identification number.
Preempt	Displays the selected Preempt option. • **True**–Primary role can be preempted based on priority. • **False**–Primary role cannot be preempt based on priority.
Gratuitous ARP Count	Displays the number of gratuitous ARP requests that a newly elected primary device in a chassis cluster sends out to announce its presence to the other network devices.
Node Priority	Displays the assigned priority for the redundancy group on that node. The eligible node with the highest priority is elected as primary for the redundant group.

Edit Node Settings

You are here: **Device Administration** > **Cluster Configuration**.

To edit node settings:

1. Select a node setting that you want to edit on the Cluster Configuration page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Node Settings page appears with editable fields.

Table 42: Fields on the Edit Node Settings Page

Field	Description
Node Settings	
Host Name	Enter the name of the host.

Table 42: Fields on the Edit Node Settings Page *(Continued)*

Field	Description
Backup Router	Enter the backup router address to be used during failover.
Destination	
IP	Enter the destination IP address. Click **+** to add the destination IP address or select an existing IP address and click **X** to delete it.
Interface	
Interface	Select an interface available for the router from the list. **NOTE**: You can add and edit two interfaces for each fabric link.
IP	Enter the interface IP address.
Add	Click **+** to add the interface.
Delete	Select one or more existing interfaces and click **X** to delete it.

RELATED DOCUMENTATION

About the Cluster Configuration Page | 166

Add an HA Cluster Interface

You are here: **Device Administration** > **Cluster Configuration**.

To add an HA cluster interface:

1. Click **+** on the upper right side of the Cluster Configuration page.
   The Add HA Cluster Interface page appears.
2. Complete the configuration according to the guidelines provided in Table 43 on page 171.

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 43: Fields on the Add HA Cluster Interface Page

Field	Action
Fabric Link	
Fabric Link 0 (fab0)	
Interface	Enter the interface IP address for fabric link 0 and click **+** to add it. Select an existing interface and click **X** to delete the interface.
Fabric Link 1 (fab1)	
Interface	Enter the interface IP address for fabric link 1 and click **+** to add it. Select an existing interface and click **X** to delete the interface.
Redundant Ethernet	
Interface	Enter the logical interface. This specifies a logical interface consisting of two physical Ethernet interfaces, one on each chassis.
IP	Enter redundant Ethernet IP address.
Redundancy Group	Select one of the redundancy group from the list. Else, enter a redundancy group.
lacp	Select an option from list: • active—Initiate transmission of LACP packets. • passive—Respond to LACP packets.
periodic	Select an option from list for periodic transmission of LACP packets. The options are fast or slow.
+	Click **+** to add the redundant Ethernet configuration.

Table 43: Fields on the Add HA Cluster Interface Page *(Continued)*

Field	Action
X	Select one or more existing redundant Ethernet configurations and click **X** to delete it.

RELATED DOCUMENTATION

- Edit an HA Cluster Interface | 172
- Delete HA Cluster Interface | 172
- Add a Redundancy Group | 173

Edit an HA Cluster Interface

You are here: **Device Administration** > **Cluster Configuration**.

To edit a HA cluster interface:

1. Select an existing HA cluster interface that you want to edit on the Cluster Configuration page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit HA Cluster Interface page appears with editable fields. For more information on the options, see "Add an HA Cluster Interface" on page 170.
3. Click **Save** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

- About the Cluster Configuration Page | 166
- Delete HA Cluster Interface | 172

Delete HA Cluster Interface

You are here: **Device Administration** > **Cluster Configuration**.

To delete HA cluster interface:

1. Select one or more existing HA cluster interfaces that you want to edit on the Cluster Configuration page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the HA cluster interface.

RELATED DOCUMENTATION

Add an HA Cluster Interface | 170

Edit an HA Cluster Interface | 172

Add a Redundancy Group

You are here: **Device Administration** > **Cluster Configuration**.

To add a redundancy group:

1. Click **+** on the upper right side of the Cluster Configuration page.
   The Add Redundancy Group page appears.
2. Complete the configuration according to the guidelines provided in Table 44 on page 173.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 44: Fields on the Add Redundancy Group Page

Field	Action
Redundancy Group	Enter the redundancy group name.
Allow preemption of primaryship	Select the check box to allow a node with a better priority to initiate a failover for a redundancy group. **NOTE**: By default, this feature is disabled. When disabled, a node with a better priority does not initiate a redundancy group failover (unless some other factor, such as faulty network connectivity identified for monitored interfaces, causes a failover).

Table 44: Fields on the Add Redundancy Group Page *(Continued)*

Field	Action
Gratuitous ARP Count	Enter a value. The range is 1 through 16. The default is 4. This specifies the number of gratuitous Address Resolution Protocol requests that a newly elected primary sends out on the active redundant Ethernet interface child links to notify network devices of a change in primary role on the redundant Ethernet interface links.
node0 priority	Enter the node priority number as 0 for a redundancy group.
node1 priority	Enter the node priority number as 1 for a redundancy group.
Interface Monitor	
Interface	Select an interface from the list.
Weight	Enter a value to specify the weight for the interface to be monitored. The range is from 1 through 125.
+	Click **+** to add the interface monitor configuration.
X	Select one or more existing interfaces and click **X** to delete them.
IP Monitoring	
Weight	Enter a value to specify the weight for IP monitoring. The range is 0 through 225.
Threshold	Enter a value to specify the global threshold for IP monitoring. The range is 0 through 225.
Retry Count	Enter a value to specify the number of retries needed to declare reachability failure. The range is 5 through 15.
Retry Interval	Enter a value to specify the time interval in seconds between retries. The range is 1 through 30.

Table 44: Fields on the Add Redundancy Group Page *(Continued)*

Field	Action
IPv4 Addresses to be monitored	
IP	Enter an IPv4 address to be monitored for reachability. You select an existing IP address and can click **X** to delete it.
Weight	Enter a value to specify the weight for the redundancy group interface to be monitored.
Interface	Enter a value to specify the logical interface to monitor this IP address
Secondary IP Address	Enter the secondary IP address for monitoring packets on a secondary link.
+	Click **+** to add the IPv4 Addresses to be monitored configuration.

RELATED DOCUMENTATION

Edit a Redundancy Group | **175**

Delete Redundancy Group | **176**

About the Cluster Configuration Page | **166**

Edit a Redundancy Group

You are here: **Device Administration** > **Cluster Configuration**.

To edit a redundancy group:

1. Select an existing redundancy group that you want to edit on the Cluster Configuration page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Redundancy Group page appears with editable fields. For more information on the options, see "Add a Redundancy Group" on page 173.
3. Click **Save** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

Delete Redundancy Group | 176

About the Cluster Configuration Page | 166

Delete Redundancy Group

You are here: **Device Administration** > **Cluster Configuration**.

To delete redundancy groups:

1. Select one or more existing redundancy groups that you want to edit on the Cluster Configuration page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the redundancy group.

RELATED DOCUMENTATION

Add a Redundancy Group | 173

Edit a Redundancy Group | 175

CHAPTER 10

User Management

IN THIS CHAPTER

About the User Management Page

IN THIS SECTION

You are here: **Device Administration** > **User Management**.

Using this page, you can configure user details, authentication methods, and passwords.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a user. See "Add a User" on page 181.
- Edit a user. See "Edit a User" on page 182.
- Delete a user. See "Delete User" on page 183.

Field Descriptions

Table 45 on page 178 describes the fields on the User Management page.

Table 45: Fields on the User Management Page

Field	Description
User Details	
User Details	Provides the users details to the device's local database. The options available are: • **Add** • **Edit** • **Delete** • **Search** • **Filter**
Authentication Methods	
Authentication Method And Order	Enable authentication methods and drag and drop to change the authentication order. The options available are: • **Password** • **RADIUS Servers** • **TACACS+Servers**
RADIUS Servers	

Table 45: Fields on the User Management Page *(Continued)*

Field	Description
RADIUS Servers	Specifies the details of RADIUS servers. Click **Configure**. To add a new RADIUS server, click **+**. Then enter the details specified below and click **OK**. • **IP Address**—Enter the server's 32–bit IP address. • **Password**—Enter the secret password for the server. • **Confirm Password**—Re-enter the secret password for the server. • **Server Port**—Enter an appropriate port. • **Source Address**—Enter the source IP address of the server. • **Time out**—Specify the amount of time (in seconds) the device should wait for a response from the server. • **Retry Attempts**—Specify the number of times that the server should try to verify the user's credentials. To delete an existing RADIUS server, select it and click **Delete**.
TACACS	

Table 45: Fields on the User Management Page *(Continued)*

Field	Description
TACACS Servers	Specifies the details of TACACS servers. Click **Configure**. To add a new TACACS server, click **+**. Then enter the details specified below and click **OK**. • **IP Address**—Enter the server's 32–bit IP address. • **Password**—Enter the secret password for the server. • **Confirm Password**—Re-enter the secret password for the server. • **Server Port**—Enter an appropriate port. • **Source IP Address**—Enter the source IP address of the server. • **Time out**—Specify the amount of time (in seconds) the device should wait for a response from the server. To delete an existing TACACS server, select it and click **Delete**.
Password Settings **NOTE**: J-Web interface does not support configuring the number of characters by which the new password should be different from the existing password.	
Minimum Reuse	Click top or bottom arrow to specify the minimum number of old passwords that you want to use. Range: 1-20.
Maximum Lifetime	Click top or bottom arrow to specify the maximum lifetime of your password in days. Range: 30-365.
Minimum Lifetime	Click top or bottom arrow to specify the minimum lifetime of your password in days. Range: 1-30.

RELATED DOCUMENTATION

Add a User | 181
Edit a User | 182
Delete User | 183

Add a User

You are here: **Device Administration** > **User Management**.

To add a user:

1. Click the add icon (**+**) on the upper right side of the User Details page.
   The Create User page appears.
2. Complete the configuration according to the guidelines provided in Table 46 on page 181.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 46: Fields on the Add User Page

Field	Description
Username	Enter a unique name for the user. Do not include spaces, colons, or commas in the username.
Login ID	Enter a unique ID for the user. Range: 100 through 64000.
Full Name	Enter the user's full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
Password	Enter a login password for the user. The login password must meet the following criteria: • The password must be at least 6 characters long. • You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.
Confirm password	Reenter the login password for the user.

Table 46: Fields on the Add User Page *(Continued)*

Field	Description
Role	Select the user's access privilege from the following options: • **super-user** • **operator** • **read-only** • **unauthorized** • **lsys** • **tenant**

RELATED DOCUMENTATION

About the User Management Page | **177**

Edit a User | **182**

Delete User | **183**

Edit a User

You are here: **Device Administration** > **User Management**.

To edit a user:

1. Select an existing user profile that you want to edit on the User Profiles page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit User page appears with editable fields. For more information on the options, see "Add a User" on page 181.
3. Click **Save** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

About the User Management Page | 177

Add a User | 181

Edit a User | 182

Delete User

You are here: **Device Administration** > **User Management**.

To delete users:

1. Select one or more users that you want to delete from the User Profile page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the User Management Page | 177

Add a User | 181

Edit a User | 182

CHAPTER 11

Multi Tenancy—Resource Profiles

IN THIS CHAPTER

About the Resource Profiles Page

IN THIS SECTION

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

NOTE: This menu is supported for only SRX4000 line of devices, SRX5000 line of devices and SRX1500 devices.

You can view Resource profile for logical systems. Resource profiles are mandatory for creating logical systems.

Tasks You Can Perform

You can perform the following tasks from this page:

- Global Settings. See "Global Settings" on page 186.
- Create a resource profile. See "Add a Resource Profile" on page 187.
- Edit a resource profile. See "Edit a Resource Profile" on page 191.
- Delete a resource profile. See "Delete Resource Profile" on page 191.
- View the details of a resource profile—To do this, select the resource profile for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected resource profile and select **Detailed View**.
  - Mouse over to the left of the selected resource profile and click **Detailed View**.
- Filter the resource profiles based on select criteria. To do this, select the filter icon at the top right-hand corner of the Resource Profiles table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the resource profiles table. To do this, click the Show Hide Columns icon in the top right corner of the Resource Profiles table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for resource profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  NOTE: You can search only the resource profile name.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 47 on page 186 describes the fields on the Resource Profiles page.

Table 47: Fields on the Resource Profiles Page

Field	Description
Profile Name	Displays the resource (security) profile names.
Configured Resource	Displays the configured resource(s).
Logical Systems/Tenants	Displays the logical system or tenants created.

RELATED DOCUMENTATION

- Global Settings | 186
- Add a Resource Profile | 187
- Edit a Resource Profile | 191
- Delete Resource Profile | 191

Global Settings

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

To add global settings:

1. Click the **Global Settings** on the upper right side of the Resource Profiles page.
   The Global Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 48 on page 187.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 48: Fields on the Global Settings page

Field	Action
Enable CPU limit	Enable or disable the CPU limit.
CPU Target	Specify the targeted CPU utilization allowed for the whole system (0 through 100 percent). Set a CPU target. You can enable disable this option to set the value. This will be applicable to all the logical system resource profiles. If you set 50 % here, then none of the profile(s) can have a value more than this and all the profiles should share this 50% of the CPU.

RELATED DOCUMENTATION

- About the Resource Profiles Page | **184**
- Add a Resource Profile | **187**
- Edit a Resource Profile | **191**
- Delete Resource Profile | **191**

Add a Resource Profile

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

To add a resource profile:

1. Click the add icon (**+**) on the upper right side of the Resource Profile page.

   The Add Resource Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 49 on page 187.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 49: Fields on the Add Resource Profile Page

Field	Description
General	

Table 49: Fields on the Add Resource Profile Page *(Continued)*

Field	Description
Profile Name	Enter a name of the security profile. The string must contain an alphanumeric character and can include underscores; no spaces allowed; 31 characters maximum.
IPS Policy	Select the IPS policy from the list.
Resource Allocation	
nat-pat-portnum	Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile.
dslite-softwire-initiator	Specify the number of IPv6 dual-stack lite (DS-Lite) softwire initiators that can connect to the softwire concentrator configured in either a user logical system or the primary logical system.
cpu	Specify the percentage of CPU utilization that is always available to a logical system.
appfw-rule	Specify the number of application firewall rule configurations that a primary administrator can configure for a primary logical system or user logical system when the security profile is bound to the logical systems.
nat-interface-port-ol	Specify the number of application firewall rule set configurations that a primary administrator can configure for a primary logical system or user logical system when the security profile is bound to the logical systems.
nat-rule-referenced-prefix	Specify the security NAT interface port overloading the quota of a logical system.
nat-port-ol-ipnumber	Specify the number of NAT port overloading IP number configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

Table 49: Fields on the Add Resource Profile Page *(Continued)*

Field	Description
nat-cone-binding	Specify the number of NAT cone binding configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
nat-static-rule	Specify the number of NAT static rule configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
nat-destination-rule	Specify the number of NAT destination rule configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
nat-source-rule	Specify the NAT source rule configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
nat-nopat-address	Specify the number of NAT without port address translation configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
nat-pat-address	Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
nat-destination-pool	Specify the number of NAT destination pool configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
nat-source-pool	Specify the NAT source pool configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
flow-gate	Specify the number of flow gates, also known as pinholes that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

Table 49: Fields on the Add Resource Profile Page *(Continued)*

Field	Description
flow-session	Specify the number of flow sessions that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
policy	Specify the number of security policies with a count that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
security-log-stream-number	Specify the security log stream number.
scheduler	Specify the number of schedulers that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
zone	Specify the zones that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
auth-entry	Specify the number of firewall authentication entries that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.
address-book	Specify the application firewall profile quota of a logical system.
Reserved	A reserved quota that guarantees that the resource amount specified is always available to the logical system.
Maximum	A maximum allowed quota.
Range	The minimum and maximum range permitted for each corresponding resource name.

RELATED DOCUMENTATION

About the Resource Profiles Page | 184
Global Settings | 186
Edit a Resource Profile | 191
Delete Resource Profile | 191

Edit a Resource Profile

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

To edit a resource profile:

1. Select the existing resource profiles that you want to edit on the Resource Profiles page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Resource Profiles page appears with editable fields. For more information on the options, see "Add a Resource Profile" on page 187.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Resource Profiles Page | 184
Global Settings | 186
Add a Resource Profile | 187
Delete Resource Profile | 191

Delete Resource Profile

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profile**.

To delete Resource Profiles:

1. Select the resource profiles that you want to delete on the Resource Profiles page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Resource Profiles Page | **184**
- Global Settings | **186**
- Add a Resource Profile | **187**
- Edit a Resource Profile | **191**

CHAPTER 12

Multi Tenancy—Interconnect Ports

IN THIS CHAPTER

About the Interconnect Ports Page

IN THIS SECTION

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

On SRX Series Services Gateways, the logical tunnel interface is used to interconnect logical systems. Use this page to interconnect logical system that serves as an internal virtual private LAN service (VPLS) switch connecting one logical system on the device to another.

NOTE: This menu is available only for SRX4000 line of devices and SRX5000 line of devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a LT Logical Interface. See "Add a LT Logical Interface" on page 195.
- Edit a LT Logical Interface. See "Edit a LT Logical Interface" on page 202.
- Delete an Interconnect Interface. See "Delete Logical Interface" on page 202.
- Search for Text in an Interconnect Ports table. See "Search for Text in an Interconnect Ports Table" on page 202.

Field Descriptions

Table 50 on page 194 describes the fields on the Interconnect ports page.

Table 50: Fields on the Interconnect Ports Page

Field	Description
Interface	Displays the interface name. Logical interfaces configured under this interface appear in a collapsible list under the physical interface.
Link Status	Displays the operational status of the link. Status can be either Up or Down.
IP Addresses	Displays the configured IP addresses. Multiple IP addresses configured on one logical interface are displayed in a collapsible list under the logical interface.
Encapsulation	Displays the mode of encapsulation. Encapsulation is the process of taking data from one protocol and translating it into another protocol, so the data can continue across a network. It can from the following points: • Ethernet • Frame Relay • Ethernet VPLS Ethernet and Frame Relay are used if logical tunnel interfaces connected between two logical systems. Ethernet VPLS will be used on logical tunnel interface which is connecting VPLS switch to logical system.
LSYS/Tenant/VPLS Switch	Displays the name of the logical system or the name of VPLS Switch.

Table 50: Fields on the Interconnect Ports Page *(Continued)*

Field	Description
Peer Interface	Displays the peer details.
Peer Encapsulation	Displays the peer encapsulation mode.
Peer LSYS/VPLS Switch	Displays the name of the peer logical system and VPLS Switch.
Type	Displays the type for logical interface—Logical System, Tenant, or VPLS Switch.

RELATED DOCUMENTATION

Add a LT Logical Interface | **195**

Add a LT Logical Interface

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

To add a LT logical interface:

1. Click the add icon (**+**) available on the upper right side of the Interconnect Ports page.
   The Create LT Logical Interface page appears.
2. Complete the configuration according to the guidelines provided in Table 51 on page 195.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
   If you click **OK**, a new LT logical interface with the provided configuration is created.

Table 51 on page 195 provides guidelines on using the fields on the Create LT Logical Interface page.

Table 51: Fields on the Create LT Logical Interface Page

Field	Description
Local Details	

Table 51: Fields on the Create LT Logical Interface Page *(Continued)*

Field	Description
Unit	Enter the Logical unit number for interface.
Type	Select a logical interface type from the list. The options available are Logical System, Tenant, and VPLS Switch.
Logical System	This option is available when you select the logical interface type as Logical System. Select a logical system from the list. If not present in the list, then we need to create a logical system. **NOTE**: Starting from Junos OS 19.1R1, the user interface will auto complete the logical system names when you type the partial name.
Tenant	This option is available when you select the logical interface type as Tenant. Select a tenant from the list. **NOTE**: Starting from Junos OS 19.1R1, the user interface will auto complete the tenant names when you type the partial name.
VPLS Switch	This option is not available if the logical interface type is VPLS Switch. Select a VPLS switch from the list.
Description	Enter description for the interface.

Table 51: Fields on the Create LT Logical Interface Page *(Continued)*

Field	Description
IPv4 Address	**NOTE**: This option is not available if the logical interface type is VPLS Switch. Specify the IPv4 address. To add an IPv4 address: 1. Click **+** at the upper right of the IPv4 Address table. 2. Enter the following details: • **IPv4 address**—Enter an IPv4 address. IP Addresses added here would be used as interconnect IP. • **Prefix Length**—Enter the prefix length. This specifies the number of bits set in the subnet mask. 3. Click the tick mark to add the IPv4 address or click **X** to discard the changes. To edit an IPv4 address: 1. Select an existing IPv4 address and click the pencil icon at the upper right of the IPv4 Address table. 2. Edit the IPv4 address and prefix length. 3. Click the tick mark to add the IPv4 address or click **X** to discard the changes. To delete an IPv4 address: 1. Select one or more existing IPv4 addresses and click the delete icon at the upper right of the IPv4 Address table. 2. Click **OK** to delete the IPv4 address. If you want to discard the changes, click **Cancel**.

Table 51: Fields on the Create LT Logical Interface Page *(Continued)*

Field	Description
IPv6 Address	**NOTE**: This option is not available if the logical interface type is VPLS Switch. Specify the IPv6 address. To add an IPv6 address: 1. Click **+** at the upper right of the IPv6 Address table. 2. Enter the following details: • **IPv6 address**—Enter an IPv6 address. IP Addresses added here would be used as interconnect IP. • **Prefix Length**—Enter the prefix length. This specifies the number of bits set in the subnet mask. 3. Click the tick mark to add the IPv6 address or click **X** to discard the changes. To edit an IPv6 address: 1. Select an existing IPv6 address and click the pencil icon at the upper right of the IPv6 Address table. 2. Edit the IPv6 address and prefix length. 3. Click the tick mark to add the IPv6 address or click **X** to discard the changes. To delete an IPv6 address: 1. Select one or more existing IPv6 addresses and click the delete icon at the upper right of the IPv6 Address table. 2. Click **OK** to delete the IPv6 address. If you want to discard the changes, click **Cancel**.
Peer Details	
Type	Select any one of the connection types from the list: • Logical system • Tenant • VPLS Switch

Table 51: Fields on the Create LT Logical Interface Page *(Continued)*

Field	Description
Logical System	This option is available when you select the connection type as Logical System. Select a logical system from the list. If not present in the list, then we need to create a logical system.
Tenant	This option is available when you select the connection type as Tenant. Select a tenant from the list.
VPLS Switch	This option is available when you select the connection type as VPLS Switch. Select a VPLS switch from the list.
Unit	Enter the peering logical system unit number.
Description	Specify the interface description. Enter description for the interface.

Table 51: Fields on the Create LT Logical Interface Page *(Continued)*

Field	Description
IPv4 Address	**NOTE**: This option is not available if the logical interface type is VPLS Switch. Specify the IPv4 address. To add an IPv4 address: 1. Click **+** at the upper right of the IPv4 Address table. 2. Enter the following details: • **IPv4 address**—Enter an IPv4 address. IP Addresses added here would be used as interconnect IP. • **Prefix Length**—Enter the prefix length. This specifies the number of bits set in the subnet mask. 3. Click the tick mark to add the IPv4 address or click **X** to discard the changes. To edit an IPv4 address: 1. Select an existing IPv4 address and click the pencil icon at the upper right of the IPv4 Address table. 2. Edit the IPv4 address and prefix length. 3. Click the tick mark to add the IPv4 address or click **X** to discard the changes. To delete an IPv4 address: 1. Select one or more existing IPv4 addresses and click the delete icon at the upper right of the IPv4 Address table. 2. Click **OK** to delete the IPv4 address. If you want to discard the changes, click **Cancel**.

Table 51: Fields on the Create LT Logical Interface Page *(Continued)*

Field	Description
IPv6 Address	**NOTE**: This option is not available if the logical interface type is VPLS Switch. Specify the IPv6 address. To add an IPv6 address: 1. Click **+** at the upper right of the IPv6 Address table. 2. Enter the following details: • **IPv6 address**—Enter an IPv6 address. IP Addresses added here would be used as interconnect IP. • **Prefix Length**—Enter the prefix length. This specifies the number of bits set in the subnet mask. 3. Click the tick mark to add the IPv6 address or click **X** to discard the changes. To edit an IPv6 address: 1. Select an existing IPv6 address and click the pencil icon at the upper right of the IPv6 Address table. 2. Edit the IPv6 address and prefix length. 3. Click the tick mark to add the IPv6 address or click **X** to discard the changes. To delete an IPv6 address: 1. Select one or more existing IPv6 addresses and click the delete icon at the upper right of the IPv6 Address table. 2. Click **OK** to delete the IPv6 address. If you want to discard the changes, click **Cancel**.

RELATED DOCUMENTATION

Edit a LT Logical Interface | 202

Edit a LT Logical Interface

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

To edit a LT logical interface:

1. Select an existing logical interface that you want to edit on the Interconnect Ports page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit LT Logical Interface page appears with editable fields. For more information on the fields, see "Add a LT Logical Interface" on page 195.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

Delete Logical Interface | 202

Delete Logical Interface

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

To delete a logical interface:

1. Select one or more the logical interfaces that you want to delete on the Interconnect Ports page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the logical interface.

RELATED DOCUMENTATION

Search for Text in an Interconnect Ports Table | 202

Search for Text in an Interconnect Ports Table

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

You can use the search icon in the top right corner of the Interconnect Ports page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.
   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

About the Interconnect Ports Page | 193

CHAPTER 13

Multi Tenancy—Logical Systems

IN THIS CHAPTER

About the Logical Systems Page

IN THIS SECTION

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

NOTE: This menu is supported for only SRX4000 line of devices, SRX5000 line of devices and SRX1500 devices.

Use this page to view, add, and delete Logical System.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a logical system. See "Add a Logical System" on page 206.
- Edit a logical system. See "Edit a Logical System" on page 217.
- Delete a logical system. See "Delete Logical System" on page 217.
- Search for Text in a logical system table. See "Search Text in Logical Systems Table" on page 218.
- View the details of the logical systems—To do this, select the logical systems for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected tenant and select **Detailed View**.
  - Mouse over to the left of the selected tenant and click **Detailed View**.
- Filter the logical systems based on select criteria. To do this, select the filter icon at the top right-hand corner of the logical systems table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the logical systems table. To do this, click the Show Hide Columns icon in the top right corner of the logical systems table and select the options you want to view or deselect the options you want to hide on the page.
- Root users can switch to Logical system context. To do this, click **Enter LSYS** on the upper right of the table. See Table 53 on page 206.

Field Descriptions

Table 52 on page 205 describes the fields on the Logical Systems page.

Table 52: Fields on the Logical Systems Page

Field	Description
Name	Displays the name of the logical system.
Resource Profile	Displays the name of the resource profile.
Users	Displays the logical system admin and users.
Assigned Interfaces	Displays the assigned logical interfaces.

Table 52: Fields on the Logical Systems Page *(Continued)*

Field	Description
Zone	Displays the zone of the resource profile.

Table 53 on page 206 describes the options on the LSYS page.

Table 53: Enter LSYS Page Options

Field	Description
Select Widget	Specifies the following widgets: • Logical System Profile. • Logical System CPU Profile. • Logical System FW No Hits. Drag and drop a widget to add it to your dashboard. Once widgets are added to the dashboard, they can be edited, refreshed, or removed by hovering over the widget header and selecting the option. The manual refresh option must be used to refresh the widget data.
Add Tabs	Click **+** to add a dashboard.

RELATED DOCUMENTATION

Add a Logical System | 206
Edit a Logical System | 217
Delete Logical System | 217
Search Text in Logical Systems Table | 218

Add a Logical System

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

To add a logical system:

1. Click the add icon (**+**) on the upper right side of the Logical Systems page.

   The Create Logical Systems page appears.
2. Complete the configuration according to the guidelines provided in Table 54 on page 207.
3. Click **Finish** to save the changes. If you want to discard your changes, click **Cancel**.

Table 54: Fields on the Add Logical Systems Page

Field	Description
General Details	
Name	Enter a logical system name of a selected Resource Profile. Only one Resource Profile can be selected, per logical system. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Logical System Resource Profile	
Click one: • Add icon (**+**)—Adds Resource Profiles. • Edit icon (**/**)—Edits the selected Resource Profiles. • Delete icon (**X**)—Deletes the selected Resource Profiles. • **Search icon**—Enables you to search a Resource Profile in the grid. • **Filter icon** —Enables you to filter the selected option in the grid. • **Show Hide Column Filter icon**—Enables you to show or hide a column in the grid.	
Profile Name	Enter a name of the security profile. The string must contain an alphanumeric character and can include underscores; no spaces allowed; 31 characters maximum.
IPS Policy	Select an IPS policy from the list.
Resource Allocation	

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
Resource Name	Displays the resource name. • nat-pat-portnum—Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile. • dslite-softwire-initiator—Specify the number of IPv6 dual-stack lite (DS-Lite) softwire initiators that can connect to the softwire concentrator configured in either a user logical system or the primary logical system. • cpu—Specify the percentage of CPU utilization that is always available to a logical system. • appfw-rule—Specify the number of application firewall rule configurations that a primary administrator can configure for a primary logical system or user logical system when the security profile is bound to the logical systems. • nat-interface-port-ol—Specify the number of application firewall rule set configurations that a primary administrator can configure for a primary logical system or user logical system when the security profile is bound to the logical systems. • nat-rule-referenced-prefix—Specify the security NAT interface port overloading the quota of a logical system. • nat-port-ol-ipnumber—Specify the number of NAT port overloading IP number configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-cone-binding—Specify the number of NAT cone binding configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-static-rule—Specify the number of NAT static rule configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-destination-rule—Specify the number of NAT destination rule configurations that user logical system administrators and primary logical system administrators

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
	can configure for their logical systems if the security profile is bound to the logical systems. • nat-source-rule—Specify the NAT source rule configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-nopat-address—Specify the number of NAT without port address translation configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-pat-address—Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-destination-pool—Specify the number of NAT destination pool configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-source-pool—Specify the NAT source pool configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • flow-gate—Specify the number of flow gates, also known as pinholes that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • flow-session—Specify the number of flow sessions that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • policy—Specify the number of security policies with a count that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • security-log-stream-number—Specify the Security log stream number quota of a logical system.

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
	• scheduler—Specify the number of schedulers that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • zone—Specify the zones that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • auth-entry—Specify the number of firewall authentication entries that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • address-book—Specify the entries in the address book. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, DNS names, wildcard addresses, and address range.
Range	Display range for each resource.
Edit	Select a resource and click on the pencil icon to edit Reserved and Maximum fields.
Reserved	Specify reserved quota that guarantees that the resource amount specified is always available to the logical system.
Maximum	Specify the maximum allowed quota.
IPS Max Sessions	Enter maximum number of sessions. Use up and down arrow keys to increase or decrease the number.
Users Click one: • Add icon (**+**)—Create users. • Edit icon (**/**)—Edit the selected users. • Delete icon (**X**)—Delete the selected users.	

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
Create-Edit users	
Username	Enter a username. Maximum length is 64 characters.
Role	• Logical System Administrator • Read only Access User **NOTE**: LSYS Read Only user can only view the options but cannot modify them.
Password	Enter a password for the user which is more than 6 characters but less than 128 characters.
Confirm Password	Re-enter the new password to confirm.
Interfaces Click One: • **Enable/Disable** —Enable or disable the physical interface. • Add icon (**+**)—Add logical interfaces. • Edit icon (**/**)—Edit the selected users. • Delete icon (**X**)—Delete the selected users.	
Create-Edit logical interfaces	
General	
Physical Interface Name	Displays the name of the Physical Interface.
Logical Interface Unit	Enter the logical Interface Unit

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
Description	Enter the description.
VLAN ID	Enter the VLAN ID. VLAN ID is mandatory.
IPV4 Address	
IPV4 Address	Click + and enter a valid IP address.
Subnet Mask	Enter a valid subnet mask.
Delete	Select the IPv4 address and click the delete icon to delete the address.
IPV6 Address	
IPV6 Address	Enter a valid IP address.
Subnet Mask	Enter a valid subnet mask.
Delete	Select the IPv6 address and click the delete icon to delete the address.
Zones Click One: • Add icon (**+**)—Create security zones. • Edit icon (**/**)—Edit the selected security zones. • Delete icon (**X**)—Delete the selected security zone. • Search icon—Search for a security zone.	
Create-Edit Security Zones	
General	

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
Name	Enter a valid name of the zone.
Description	Enter a description of the zone.
Application Tracking	Enables the application tracking support.
Source Identity Log	Enable source identity log for this zone.
Interfaces	Select an interface from the Available column and move it to Selected column.
Selected interfaces	Displays the selected interfaces.

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
System Services	Select system services from the following options: **NOTE**: Select the Except check box to allow services other than the selected services. • all—Specify all system services. • any-service—Specify services on entire port range. • appqoe—Specify the APPQOE active probe service. • bootp—Specify the Bootp and dhcp relay agent service. • dhcp—Specify the Dynamic Host Configuration Protocol. • dhcpv6—Enable Dynamic Host Configuration Protocol for IPV6. • dns—Specify the DNS service. • finger—Specify the finger service. • ftp—Specify the FTP protocol. • http—Specify the web management using HTTP. • https—Specify the web management using HTTP secured by SSL. • ident-reset—Specify the send back TCP RST IDENT request for port 113. • ike—Specify the Internet key exchange. • lsping—Specify the Label Switched Path ping service. • netconf—Specify the NETCONF Service. • ntp—Specify the network time protocol service. • ping—Specify the internet control message protocol. • r2cp—Enable Radio-Router Control Protocol service. • reverse-ssh—Specify the reverse SSH Service. • reverse-telnet—Specify the reverse telnet Service.

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
	• rlogin—Specify the Rlogin service • rpm—Specify the Real-time performance monitoring. • rsh—Specify the Rsh service. • snmp—Specify the Simple Network Management Protocol Service. • snmp-trap—Specify the Simple Network Management Protocol trap. • ssh—Specify the SSH service. • tcp-encap—Specify the TCP encapsulation service. • telnet—Specify the Telnet service. • tftp—Specify the TFTP • traceroute—Specify the traceroute service. • webapi-clear-text—Specify the Webapi service using http. • webapi-ssl—Specify the Webapi service using HTTP secured by SSL. • xnm-clear-text—Specify the JUNOScript API for unencrypted traffic over TCP. • xnm-ssl—Specify the JUNOScript API Service over SSL.

Table 54: Fields on the Add Logical Systems Page *(Continued)*

Field	Description
Protocols	Select a protocol from the following options: **NOTE**: Select the Except check box to allow protocols other than the selected protocols. • bfd—Bidirectional Forwarding Detection. • bgp—Broder Gateway protocol. • dvmrp—Distance Vector Multicast Routing Protocol. • igmp—Internet group management protocol. • ldp— label Distribution Protocol. • msdp—Multicast source discovery protocol. • nhrp—Next Hop Resolution Protocol. • ospf—Open shortest path first. • ospf3—Open shortest path first version 3. • pgm—Pragmatic General Multicast. • pim—Protocol independent multicast. • rip—Routing information protocol. • ripng—Routing information protocol next generation. • router-discovery—Router Discovery. • rsvp—Resource reservation protocol. • sap—Session Announcement Protocol. • vrrp—Virtual Router redundancy protocol.
Traffic Control Options	Enable this option to send RST for NON-SYN packet not matching TCP session.

RELATED DOCUMENTATION

- About the Logical Systems Page | 204
- Add a Logical System | 206
- Edit a Logical System | 217
- Delete Logical System | 217
- Search Text in Logical Systems Table | 218

Edit a Logical System

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

To edit a logical system profile:

1. Select the existing logical system profile that you want to edit on the Logical System Profile page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit a Logical System Profile page appears with editable fields. For more information on the options, see "Add a Logical System" on page 206.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Logical Systems Page | 204
- Add a Logical System | 206
- Delete Logical System | 217
- Search Text in Logical Systems Table | 218

Delete Logical System

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

To delete logical system:

1. Select the logical system that you want to delete on the Logical System page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Logical Systems Page | 204
- Add a Logical System | 206
- Edit a Logical System | 217
- Search Text in Logical Systems Table | 218

Search Text in Logical Systems Table

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter a partial text or full text of the keyword in the search bar and execute. The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

- About the Logical Systems Page | 204
- Add a Logical System | 206
- Edit a Logical System | 217
- Delete Logical System | 217

CHAPTER 14

Multi Tenancy—Tenants

IN THIS CHAPTER

About the Tenants Page

IN THIS SECTION

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

You can use this page to add, view, and delete Tenants.

NOTE: This menu is supported for only SRX4000 line of devices, SRX5000 line of devices and SRX1500 devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a tenant. See "Add a Tenant" on page 221.

- Edit a tenant. See "Edit a Tenant" on page 229.
- Delete a tenant. See "Delete Tenant" on page 229.
- Search for Text in a tenants table. See "Search Text in Tenants Table" on page 230.
- View the details of the tenants—To do this, select the tenant for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected tenant and select **Detailed View**.
  - Mouse over to the left of the selected tenant and click **Detailed View**.
- Filter the tenant based on select criteria. To do this, select the filter icon at the top right-hand corner of the tenant table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the tenant table. To do this, click the Show Hide Columns icon in the top right corner of the tenant table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 55 on page 220 describes the fields on the Tenants page.

Table 55: Fields on the Tenants Page

Field	Description
Name	Displays the name of the tenant system.
Resource Profile	Displays the name of the resource profile.
Users	Displays the tenant system admin and users, and its associated permissions.
Assigned Interfaces	Displays the assigned logical interfaces.
Zones	Displays the zones for the tenant.
Routing Instance	Displays the routing instance that is explicitly assigned to the tenant system.

RELATED DOCUMENTATION

Add a Tenant

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

To add a tenant:

1. Click the add icon (**+**) on the upper right side of the Tenants page.
   The Create Tenant page appears.
2. Complete the configuration according to the guidelines provided in Table 56 on page 221.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 56: Fields on the Create Tenant Page

Field	Description
General Details	
Name	Enter a name for the tenant. Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Routing Instance	By default, the tenant name is taken as the routing instance name.
Tenant Resource Profile	
Profile Name	Displays the name of the resource profile.
Configured Resources	Displays the resources and its reserved or maximum quantity assigned for this resource profile.

Table 56: Fields on the Create Tenant Page *(Continued)*

Field	Description
Logical Systems/Tenants	Displays other logical systems and/or tenants using this resource profile.

Click one:

- Add icon (**+**)—Adds resource profiles.
- Edit icon (**/**)—Edits the selected resource profiles.
- Search icon—Enables you to search a resource profile in the grid.
- Filter icon—Enables you to filter the selected option in the grid.
- Show Hide Column Filter icon—Enables you to show or hide a column in the grid.

Create-Edit Tenant Resource Profile

See "Add a Resource Profile" on page 187 for details on creating and editing resource profile.

User Details

You can define tenant administrators and users.

Click one:

- Add icon (**+**)—Create users.
- Edit icon (**/**)—Edit the selected users.
- Delete icon—Delete the selected users.

Create-Edit users

Username	Enter a username. Maximum length is 64 characters.

Table 56: Fields on the Create Tenant Page *(Continued)*

Field	Description
Role	Select an option from the list to specify the role of the user: • Tenant Administrator • Read only Access User **NOTE**: Logical system or tenant Read Only user can only view the options but cannot modify them.
Password	Specify the password for the user.
Confirm Password	Confirm the password.

Assign Interfaces

Only one logical interface can be part of one tenant, whereas a tenant can have multiple logical interfaces.

Click One:

- **Enable/Disable** —Enable or disable the physical interface.
- Add icon (**+**)—Add logical interfaces.
- Edit icon (**/**)—Edit the selected users.
- Delete icon—Delete the selected users.

Create-Edit logical interfaces

General

Physical Interface Name	Displays the name of the Physical Interface.
Logical Interface Unit	Enter the logical interface unit.
Description	Enter the description.
VLAN ID	Enter the VLAN ID. VLAN ID is mandatory.

Table 56: Fields on the Create Tenant Page *(Continued)*

Field	Description
IPV4 Address	
IPV4 Address	Click + and enter a valid IP address.
Subnet Mask	Enter a valid subnet mask.
Delete	Select the IPv4 address and click the delete icon to delete the address.
IPV6 Address	
IPV6 Address	Enter a valid IP address.
Subnet Mask	Enter a valid subnet mask.
Delete	Select the IPv6 address and click the delete icon to delete the address.
Zone Configuration Click One: • Add icon (**+**) — Create security zones. • Edit icon (**/**) —Edit the selected security zones. • Delete icon (**X**)—Delete the selected security zone. • Search - Search for a security zone.	
Create-Edit Security Zones	
General	
Name	Enter a valid name of the zone.
Description	Enter a description of the zone.

Table 56: Fields on the Create Tenant Page *(Continued)*

Field	Description
Application Tracking	Enables the application tracking support.
Source Identity Log	Enable source identity log for this zone.
Interfaces	Select an interface from the Available column and move it to Selected column.
Selected interfaces	Displays the selected interfaces.

Table 56: Fields on the Create Tenant Page *(Continued)*

Field	Description
System Services Options	Select system services from the following options: **NOTE**: Select the Except check box to allow services other than the selected services. • all—Specify all system services. • any-service—Specify services on entire port range. • appqoe—Specify the APPQOE active probe service. • bootp—Specify the Bootp and dhcp relay agent service. • dhcp—Specify the Dynamic Host Configuration Protocol. • dhcpv6—Enable Dynamic Host Configuration Protocol for IPV6. • dns—Specify the DNS service. • finger—Specify the finger service. • ftp—Specify the FTP protocol. • http—Specify the web management using HTTP. • https—Specify the web management using HTTP secured by SSL. • ident-reset—Specify the send back TCP RST IDENT request for port 113. • ike—Specify the Internet key exchange. • lsping—Specify the Label Switched Path ping service. • netconf—Specify the NETCONF Service. • ntp—Specify the network time protocol service. • ping—Specify the internet control message protocol. • r2cp—Enable Radio-Router Control Protocol service. • reverse-ssh—Specify the reverse SSH Service. • reverse-telnet—Specify the reverse telnet Service.

Table 56: Fields on the Create Tenant Page *(Continued)*

Field	Description
	• rlogin—Specify the Rlogin service • rpm—Specify the Real-time performance monitoring. • rsh—Specify the Rsh service. • snmp—Specify the Simple Network Management Protocol Service. • snmp-trap—Specify the Simple Network Management Protocol trap. • ssh—Specify the SSH service. • tcp-encap—Specify the TCP encapsulation service. • telnet—Specify the Telnet service. • tftp—Specify the TFTP • traceroute—Specify the traceroute service. • webapi-clear-text—Specify the Webapi service using http. • webapi-ssl—Specify the Webapi service using HTTP secured by SSL. • xnm-clear-text—Specify the JUNOScript API for unencrypted traffic over TCP. • xnm-ssl—Specify the JUNOScript API Service over SSL.

Table 56: Fields on the Create Tenant Page *(Continued)*

Field	Description
Protocols	Select a protocol from the following options: **NOTE**: Select the Except check box to allow protocols other than the selected protocols. • bfd—Bidirectional Forwarding Detection. • bgp—Broder Gateway protocol. • dvmrp—Distance Vector Multicast Routing Protocol. • igmp—Internet group management protocol. • ldp—label Distribution Protocol. • msdp—Multicast source discovery protocol. • nhrp—Next Hop Resolution Protocol. • ospf—Open shortest path first. • ospf3—Open shortest path first version 3. • pgm—Pragmatic General Multicast. • pim—Protocol independent multicast. • rip—Routing information protocol. • ripng—Routing information protocol next generation. • router-discovery—Router Discovery. • rsvp—Resource reservation protocol. • sap—Session Announcement Protocol. • vrrp—Virtual Router redundancy protocol.
Traffic Control Options	Enable this option to send RST for NON-SYN packet not matching TCP session.

RELATED DOCUMENTATION

- About the Tenants Page | 219
- Edit a Tenant | 229
- Delete Tenant | 229
- Search Text in Tenants Table | 230

Edit a Tenant

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

To edit a tenant:

1. Select the existing tenant that you want to edit on the Tenants page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit a Tenant page appears with editable fields. For more information on the options, see "Add a Tenant" on page 221.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Tenants Page | 219
- Add a Tenant | 221
- Delete Tenant | 229
- Search Text in Tenants Table | 230

Delete Tenant

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

To delete tenants:

1. Select the tenants that you want to delete on the Tenants page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Tenants Page | 219
- Add a Tenant | 221
- Edit a Tenant | 229
- Search Text in Tenants Table | 230

Search Text in Tenants Table

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter a partial text or full text of the keyword in the search bar and execute. The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

- About the Tenants Page | 219
- Add a Tenant | 221
- Edit a Tenant | 229
- Delete Tenant | 229

CHAPTER 15

Certificate Management—Device Certificates

IN THIS CHAPTER

About the Device Certificates Page

You are here: **Device Administration** > **Certificate Management** > **Device Certificates**.

Manage the device certificates to authenticate Secure Socket Layer (SSL). SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

You can perform the following tasks:

- Import a certificate to manually load externally generated certificates or CSR. See "Import a Device Certificate" on page 233.

  NOTE: You must obtain the private key, passphrase, and the signed certificate from certificate authority (CA) server.

- Export a local certificate or CSR from the default location to a specific location within the device. See "Export a Device Certificate" on page 234.

- View the details of a certificate. See "View Details of a Device Certificate" on page 238.

- Generate a certificate. See "Add a Device Certificate" on page 235.
- Delete a certificate. See "Delete Device Certificate" on page 238.
- Search for text in a device certificate table. See "Search Text in the Device Certificates Table" on page 242.
- Filter the device certificates information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the Device Certificates table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page

Table 57 on page 232 provides the details of the fields of the Device Certificates page.

Table 57: Fields on Device Certificates Page

Field	Description
Certificate ID	Displays the certificate ID. Certificate ID is a unique value across the device. This will be used to create a key pair along with the algorithm to associate with the key.
Issuer Org	Displays the details of the authority that issued the certificate.
Status	Displays whether the status of the certificate is valid, expired, and so on.
Expiration Date	Displays certificate expiration date.
Encryption Type	Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption.
Signature Status	Displays whether the status of the certificate is signed or in certificate signing request (CSR) stage.

Import a Device Certificate

To import a device certificate:

1. Select **Device Administration** > **Certificate Management** > **Device Certificates**.
2. Click **Import**.

   The Import Certificate page appears.
3. Complete the configuration according to the guidelines provided in Table 58 on page 233.
4. Click **OK** to import the certificate.

   You are taken to the Device Certificates page. If the certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

   After importing a certificate, you can use it when you create an SSL proxy profile and for IPsec VPN peers authentication.
5. Click **Cancel** to cancel your entries and returns to the Device Certificates page.

Table 58: Fields on the Import Certificate Page

Field	Action
Type	Select an option to specify whether the certificate that you are importing is an Externally Generated Certificate or a CSR.
Certificate ID	Enter a unique value for the certificate ID for an externally generated certificate. Select an option from the list to specify the certificate ID for a CSR.
File path for Certificate	Click **Browse** to navigate to the path from where you want to import the certificate.
File path for Private Key	Click **Browse** to navigate to the path from where you want to import the private key.
Passphrase	Enter the passphrase used to protect the private key or key pair of the certificate file.

RELATED DOCUMENTATION

About the Device Certificates Page | 231

Export a Device Certificate | 234

Export a Device Certificate

To export a device certificate:

1. Select **Device Administration** > **Certificate Management** > **Device Certificates**.
2. Click **Export**.

   The Export Certificate page appears.
3. Complete the configuration according to the guidelines provided in Table 59 on page 234.
4. Click **OK** to export the certificate.

   Once you save or download the exported file(s), a confirmation message is displayed; if not, an error message is displayed.

Table 59: Fields on the Export Certificate Page

Field	Action
Type	Select an option from the list to specify whether the certificate that you are exporting is a Local Certificate or a CSR.
Certification Name	Select an option from the list for the local certificate name.
Certificate ID	This option is available only for CSR. Select an option from the list for the CSR certificate ID.
Format	Select an option from the list to specify whether the exporting certificate format is Privacy-Enhanced Mail (PEM) or Distinguished Encoding Rules (DER).
Key Pair	Enable or disable exporting key pair of a certificate.
Passphrase	Enter the passphrase to protect the private key or key pair of the certificate file.

RELATED DOCUMENTATION

- About the Device Certificates Page | 231
- Import a Device Certificate | 233
- Add a Device Certificate | 235
- Delete Device Certificate | 238
- View Details of a Device Certificate | 238
- Search Text in the Device Certificates Table | 242

Add a Device Certificate

To add a device certificate:

1. Select **Device Administration** > **Certificate Management** > **Device Certificates**.
2. Click the add icon (+).

   The Generate Certificate page appears.
3. Complete the configuration according to the guidelines provided in Table 60 on page 235.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

   If you click **OK**, a new certificate with the provided configuration is created.

Table 60: Fields on the Generate Certificate Page

Field	Action
Certificate Details	
Certificate Type	Select one of the certificate types from the list that you want to generate: • Local Self-Signed—Allows for use of SSL-based (Secure Sockets Layer) services without requiring that the user or administrator to undertake the considerable task of obtaining an identity certificate signed by a CA. Self-signed certificates are usually used for internal purpose. • Local Certificate—Validates the identity of the security device. A local certificate imports or references an SSL certificate.

Table 60: Fields on the Generate Certificate Page *(Continued)*

Field	Action
CA Profile Name	This option is available for a local certificate. Select one of the CA profile name from the list or click **Create** to add a CA Profile. For details on adding a CA profile, see the table in the *Adding a Certificate Authority Profile* section.
Certificate ID	Enter a unique value for the certificate ID.
Encryption Type	Select one of the types of encryption from the list: • RSA Encryption • DSA Encryption **NOTE**: The certificate cannot be used in SSL Proxy profile if it is generated using type DSA. • ECDSA Encryption
Key Size	Select one of the key sizes from the list: • RSA encryption supports 1024 bits, 2048 bits, or 4096 bits. • DSA encryption supports 1024 bits, 2048 bits, or 4096 bits. • ECDSA encryption supports 256 bits, 384 bits, or 521 bits.
Subject (Minimum of one field required)	
Domain Component	Enter the domain component that you want to be associated with the certificate.
Common Name	Enter a common name with the certificate.
Organizational Unit Name	Enter the organizational unit that you want to be associated with the certificate.
Organizational Name	Enter the organizational name that you want to be associated with this certificate.

Table 60: Fields on the Generate Certificate Page *(Continued)*

Field	Action
Serial Number	Enter a serial number of the device.
Locality	Enter the locality name.
State	Enter the state name.
Country	Enter the country name.
Subject Alt Name **NOTE**: For a local certificate, any one field is mandatory	
Domain Name	Enter a Domain Name that you want to associate with the certificate.
Email	Enter a user email address.
IPv4 Address	Enter the IPv4 address of the device.
IPv6 Address	This option is available for a local certificate. Enter the IPv6 address of the device.
Advanced	

Digest	Select the digest from the list:
	• For local Self-signed certificate (RSA/DSA/ECDSA) options are: None, SHA-1 digests, or SHA-256 digests.
	• For local certificate options are:
	  • RSA/DSA: None, SHA-1 digests, or SHA-256 digests
	  • ECDSA: None, SHA-256 digests, or SHA-384 digests.

Signing Certificate	Enable or disable specifies that the certificate is used to sign other certificates.

RELATED DOCUMENTATION

- About the Device Certificates Page | 231
- Import a Device Certificate | 233
- Export a Device Certificate | 234
- Delete Device Certificate | 238
- View Details of a Device Certificate | 238
- Search Text in the Device Certificates Table | 242

Delete Device Certificate

To delete a device certificate:

1. Select **Device Administration** > **Certificate Management** > **Device Certificates**.
2. Select the certificate you want to delete.
3. On the upper right side of the Device Certificates page, click the delete icon to delete.

   A confirmation window appears.
4. Click **Yes** to delete.

RELATED DOCUMENTATION

- About the Device Certificates Page | 231
- Import a Device Certificate | 233
- Export a Device Certificate | 234
- Add a Device Certificate | 235
- View Details of a Device Certificate | 238
- Search Text in the Device Certificates Table | 242

View Details of a Device Certificate

To view the details of a device certificate:

1. Select **Device Administration** > **Certificate Management** > **Device Certificates**.
2. Select an existing certificate.
3. Select **More** > **Detailed View**.

The View Certificate page appears with the details of the certificate.

> **NOTE**: When you hover over the certificate ID, a Detailed View icon appears before the certificate ID. You can also use this icon to view the certificate details.

4. Click **OK** after viewing the certificate details.

Table 61 on page 239 provides the field details of the certificate on the View Certificate page.

Table 61: Fields on the View Certificate Page

Field	Action
Certificate Details	
Certificate ID	Displays the certificate ID.
Certificate Version	Displays the certificate revision number.
Certificate Type	Displays the certificate type. For example, Signed.
Encryption Type	Displays the encryption type. For example, RSA.
Key Size	Displays the key size of the encryption type.
Serial Number	Displays the unique serial number of the certificate.
Subject	
Domain Component	Displays the domain component associated with the certificate.
Common Name	Displays the common name associated with the certificate.
Organizational Unit Name	Displays the organizational unit associated with the certificate.
Organizational Name	Displays the organizational name associated with this certificate.

Table 61: Fields on the View Certificate Page *(Continued)*

Field	Action
Serial Number	Displays the serial number of the device.
Locality	Displays the locality name.
State	Displays the state name.
Country	Displays the country name.
Subject Alt Name	
Domain Name	Displays the Fully Qualified Domain Name (FQDN).
Email	Displays the email ID of the certificate holder.
IPv4 Address	Displays the IPv4 address.
IPv6 Address	Displays the IPv6 address.
Issuer Information	
Common Name	Displays the issuer common name associated with the certificate.
Domain Component	Displays the issuer domain component associated with the certificate.
Organization Name	Displays the issuer organizational name.
Organization Unit Name	Displays the issuer organizational unit.
Locality Name	Displays the issuer locality name.
State or Province Name	Displays the issuer state or region name.

Table 61: Fields on the View Certificate Page *(Continued)*

Field	Action
Validity	
Not Before	Displays the start time when the certificate becomes valid.
Not After	Displays the end time when the certificate becomes invalid.
Auto Re Enrollment	
Status	Displays whether the auto re enrollment is enabled or disabled.
Next Trigger Time	Displays the how long auto-reenrollment should be initiated before expiration.
Fingerprint	
MD5	Displays the MD5 fingerprints to identify the certificate.
SHA1	Displays the SHA-1 fingerprints to identify the certificate.
Signature Algorithm	
Algorithm	Displays whether the signature algorithm is SHA-1, SHA-256, or SHA-384 digest.
Distribution CRL	
URL	Displays the URL of the certificate revocation list (CRL) server.
LDAP	Displays the name of the location from which the CRL is retrieved through Lightweight Directory Access Protocol (LDAP).
Authority Information Access OCSP	
URL	Displays the URL of the Online Certificate Status Protocol (OCSP) server.

RELATED DOCUMENTATION

- About the Device Certificates Page | 231
- Import a Device Certificate | 233
- Export a Device Certificate | 234
- Add a Device Certificate | 235
- Delete Device Certificate | 238
- Search Text in the Device Certificates Table | 242

Search Text in the Device Certificates Table

You are here: **Device Administration** > **Certificate Management** > **Device Certificates**.

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.

   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

- About the Device Certificates Page | 231
- Import a Device Certificate | 233
- Export a Device Certificate | 234
- Add a Device Certificate | 235
- Delete Device Certificate | 238
- View Details of a Device Certificate | 238

CHAPTER 16

Certificate Management—Trusted Certificate Authority

IN THIS CHAPTER

About the Trusted Certificate Authority Page

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

SSL forward proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL forward proxy checks certificate authority (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

You can perform the following tasks:

- Generate a default trusted CAs. See "Generate Default Trusted Certificate Authorities" on page 245.
- Enroll a CA certificate using the Simple Certificate Enrollment Process (SCEP) or Certificate Management Protocol (CMPv2). With SCEP or CMPv2, you can configure Juniper Network device to obtain a local certificate online and start the online enrollment for the specified certificate ID. See "Enroll a CA Certificate" on page 246.

- Import a CA certificate to manually load CA certificates and CRL. See "Import a CA Certificate" on page 247.
- Add a CA profile. See "Add a Certificate Authority Profile" on page 248.
- Edit a CA profile. See "Edit a Certificate Authority Profile" on page 252.
- Delete a CA profile. See "Delete Certificate Authority Profile" on page 253.
- Search for text in a Trusted Certificate Authority table. See "Search Text in the Trusted Certificate Authority Table" on page 254.
- Filter the trusted CA information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the trusted CA table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

Table 62 on page 244 provides the details of the fields of the Trusted Certificate Authority Page.

Table 62: Fields on Trusted Certificate Authority Page

Field	Description
CA Profile	Displays the name of the CA profile.
Certificate ID	Displays the CA certificate ID.
Issuer Org	Displays the issuer organizational name.

Table 62: Fields on Trusted Certificate Authority Page *(Continued)*

Field	Description
Status	Displays the status of the CA certificate. For example: • Valid. • Expires in number of day(s). • Expired. • Download Required. This status is for a CA profile with manual enrollment. • Enrollment Required. This status is for a CA profile with automatic enrollment.
Expiration Date	Displays CA certificate expiration date.
Encryption Type	Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption.

Generate Default Trusted Certificate Authorities

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

For SSL forward proxy, you need to load trusted CA certificates on your system. By default, Junos OS provides a list of trusted CA certificates that include default certificates used by common browsers. To generate default Trusted CA profiles with default name as Local, click **Generate Default Trusted CAs** and then click **Continue**. This process may take several minutes.

RELATED DOCUMENTATION

About the Trusted Certificate Authority Page | **243**

Enroll a CA Certificate | **246**

Import a CA Certificate | **247**

Enroll a CA Certificate

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To enroll a trusted CA certificate:

1. Click **Enroll**.

   The Enroll CA Certificate page appears.
2. Complete the configuration according to the guidelines provided in Table 63 on page 246.
3. Click **OK** to enroll the CA certificate.

Table 63: Fields on the Enroll CA Certificate Page

Field	Action
CA Profile Name	Select a CA profile name from the list that you want to enroll.
Protocol	Select a protocol from the list for the CA certificate that you want to enroll. • SCEP—Simple Certificate Enrollment Protocol (SCEP) • CMPV2—Certificate Management Protocol version 2 (CMPv2)
NOTE: The following fields are available only if you select CMPv2 protocol. All the fields are mandatory.	
CA Secret	Enter the out-of-band secret value received from the CA server.
CA Reference	Enter the out-of-band reference value received from the CA server.
CA Dn	Enter the distinguished name (DN) of the CA enrolling the EE certificate. **NOTE**: This optional parameter is mandatory if the CA certificate is not already enrolled. If the CA certificate is already enrolled, the subject DN is extracted from the CA certificate.

Table 63: Fields on the Enroll CA Certificate Page *(Continued)*

Field	Action
Certificate Details	Click **Add** to generate a new certificate inline.

RELATED DOCUMENTATION

- About the Trusted Certificate Authority Page | 243
- Generate Default Trusted Certificate Authorities | 245
- Enroll a CA Certificate | 246
- Add a Certificate Authority Profile | 248
- Edit a Certificate Authority Profile | 252
- Delete Certificate Authority Profile | 253
- Search Text in the Trusted Certificate Authority Table | 254

Import a CA Certificate

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To import a CA certificate:

1. Click **Import**.

   The Import CA Certificate page appears.
2. Complete the configuration according to the guidelines provided in Table 64 on page 247.
3. Click **OK** to import the CA certificate.

   You are taken to the Trusted Certificate Authority page. If the CA certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

Table 64: Fields on the Import CA Certificate Page

Field	Action
CA Profile Name	Select a CA profile name from the list that you want to import.

Table 64: Fields on the Import CA Certificate Page *(Continued)*

Field	Action
File path for CA Certificate	Click **Browse** to navigate to the path from where you want to import the CA certificate.
File path for CRL	Click **Browse** to navigate to the path from where you want to import the Certificate Revocation List (CRL).

Add a Certificate Authority Profile

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To add a Certificate Authority (CA) profile:

1. Click the add icon (+).
   The Add CA Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 65 on page 248.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   If you click **OK**, a new CA profile with the provided configuration is created.

Table 65: Fields on the Add CA Profile Page

Field	Action
Profile Details	
CA Profile Name	Enter a unique CA profile name.
CA Identity	Enter a CA identity name.

Table 65: Fields on the Add CA Profile Page *(Continued)*

Field	Action
Revocation Check	Select an option from the list: • Disable—Disables verification of status of digital certificates. • OCSP—Online Certificate Status Protocol (OCSP) checks the revocation status of a certificate. • CRL—A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.
URL	For OCSP, enter HTTP addresses for OCSP responders. For CRL, enter the name of the location from which to retrieve the CRL through HTTP or Lightweight Directory Access Protocol (LDAP).
On Connection Failure	Enable this option to skip the revocation check if the OCSP responder is not reachable. **NOTE**: This option is applicable only for OCSP.
Disable Responder Revocation Check	Enable this option to disable revocation check for the CA certificate received in an OCSP response. **NOTE**: This option is applicable only for OCSP.
Accept Unknown Status	When set to enable, accepts the certificate with unknown status. **NOTE**: This option is applicable only for OCSP.
Nonce Payload	Disable the option—Explicitly disable the sending of a nonce payload. Enable the option—Enable the sending of a nonce payload. This is the default. **NOTE**: This option is applicable only for OCSP.
CRL Refresh Interval	Enter the time interval (in hours) between CRL updates. Range: 0 through 8784 hours. **NOTE**: This option is applicable only for CRL.

Table 65: Fields on the Add CA Profile Page *(Continued)*

Field	Action
Password	Enter the password for authentication with the server.
Disable on Download Failure	Enable this option to override the default behavior and permit certificate verification even if the CRL fails to download. **NOTE**: This option is applicable only for CRL.
Enrollment	
CA Certificate	Select an option whether you want to enroll the CA certificate manually or automatically.
File path for Certificate	Click **Browse** to navigate to the path from where you want to enroll the CA certificate.
URL	Enter the URL from where you want to enroll the CA certificate automatically.
Retry	Number of enrollment retry attempts before terminating. Range: 0 - 1080.
Retry-interval	Interval in seconds between the enrollment retries. Range: 0 - 3600.
Advanced	
Administrator	Enter an administrator e-mail address to which the certificate request is sent.
Source Address	Enter a source IPv4 or IPv6 address to be used instead of the IP address of the egress interface for communications with external servers.
Auto Re Enrollment	Enable this option to request that the issuing CA replace a certificate before its specified expiration date.
Re Generate Key Pair	Enable this option to automatically generate a new key pair when auto-reenrolling a device certificate.

Table 65: Fields on the Add CA Profile Page *(Continued)*

Field	Action
Protocol	Select an option from the list: Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol version 2 (CMPv2).
Challenge Password	Enter the challenge password used by the certificate authority (CA) for certificate enrollment and revocation. This challenge password must be the same used when the certificate was originally configured.
Trigger Time	Enter the percentage for the reenroll trigger time before expiration. Range: 1 through 99 percent
Digest	Select an option from the list: None, SHA-1 digest (default), or MD5-digest. **NOTE**: This option is applicable only when you select SCEP protocol.
Encryption	Select an option from the list: None, DES, DES 3. **NOTE**: This option is applicable only when you select SCEP protocol.
Routing Instance	Select an option from the list of configured routing instances.

Table 65: Fields on the Add CA Profile Page *(Continued)*

Field	Action
Proxy Profile	Select an option from the list. Or To create a new proxy profile inline: **1.** Click **Create**. Create Proxy Profile page appears. **2.** Enter the following details: • Profile Name—Enter a unique proxy profile name. • Connection Type: • Server IP—Enter the IP address of the server. • Host Name—Enter the host name. • Port Number—Select the port number by using top/down arrows. Range: 0 through 65535 **3.** Click **OK**.

RELATED DOCUMENTATION

About the Trusted Certificate Authority Page | 243

Generate Default Trusted Certificate Authorities | 245

Enroll a CA Certificate | 246

Import a CA Certificate | 247

Edit a Certificate Authority Profile | 252

Delete Certificate Authority Profile | 253

Search Text in the Trusted Certificate Authority Table | 254

Edit a Certificate Authority Profile

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To edit a Certificate Authority (CA) profile:

1. Select a CA profile.
2. On the upper right side of the Trusted Certificate Authority page, click the pencil icon.

   See "Add a Certificate Authority Profile" on page 248 for the options available for editing on the Edit CA Profile page.

   NOTE: When you select a CA profile to edit, you cannot edit the following fields:

   - CA Profile Name
   - Revocation Check
   - Enrollment > CA Certificate
   - Advanced > Auto Re Enrollment
   - Advanced > Protocol

3. Click **OK**

RELATED DOCUMENTATION

About the Trusted Certificate Authority Page | 243
Generate Default Trusted Certificate Authorities | 245
Enroll a CA Certificate | 246
Import a CA Certificate | 247
Add a Certificate Authority Profile | 248
Delete Certificate Authority Profile | 253
Search Text in the Trusted Certificate Authority Table | 254

Delete Certificate Authority Profile

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To delete a Certificate Authority (CA) profile:

1. Select a CA profile.
2. On the upper right side of the Trusted Certificate Authority page, click the delete icon to delete.

A confirmation window appears.

3. Click **Yes** to delete.

RELATED DOCUMENTATION

- About the Trusted Certificate Authority Page | 243
- Generate Default Trusted Certificate Authorities | 245
- Enroll a CA Certificate | 246
- Import a CA Certificate | 247
- Add a Certificate Authority Profile | 248
- Edit a Certificate Authority Profile | 252
- Search Text in the Trusted Certificate Authority Table | 254

Search Text in the Trusted Certificate Authority Table

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.

   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

- About the Trusted Certificate Authority Page | 243
- Generate Default Trusted Certificate Authorities | 245
- Enroll a CA Certificate | 246
- Import a CA Certificate | 247
- Add a Certificate Authority Profile | 248
- Edit a Certificate Authority Profile | 252
- Delete Certificate Authority Profile | 253

CHAPTER 17

Certificate Management—Certificate Authority Group

IN THIS CHAPTER

About the Certificate Authority Group Page

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

Multiple CA profiles can be grouped in one trusted CA group for a given topology. The CA group can be used either in SSL or IPsec.

SSL forward proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL forward proxy checks certificate authority (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

You can perform the following tasks:

- Import a CA group to manually load the CA group. See "Import a Trusted CA Group" on page 256.
- Add a CA group. See "Add a CA Group" on page 257.

> **NOTE**: You can group up to maximum of 20 CA profiles in a single trusted CA group. A minimum of one CA profile is a must to create a trusted CA group.

- Edit a CA group. See "Edit a CA Group" on page 258.
- Delete a CA group. See "Delete CA Group" on page 259.
- Search for text in a CA group table. See "Search Text in the Certificate Authority Group Table" on page 259.
- Filter the CA group information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the CA group table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

Table 66 on page 256 provides the details of the fields of the Certificate Authority Group Page.

Table 66: Fields on Certificate Authority Group Page

Field	Description
Group Name	Displays a Name for the CA profile group.
CA Profiles	Displays the name of CA profiles.
Used For	Displays whether the CA profile group is used for IPsec VPN or for SSL proxy.

Import a Trusted CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To import a trusted CA group:

1. Click **Import**.

   The Import Trusted CA Group page appears.
2. Complete the configuration according to the guidelines provided in Table 67 on page 257.
3. Click **OK** to import the CA group.

   You are taken to the Certificate Authority Group page. If the CA group content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

After importing a CA profile group, you can use it when you create an SSL proxy.

Table 67: Fields on the Import Trusted CA Group Page

Field	Action
CA Group Name	Enter the name of a CA group.
File path for CA Group	Click **Browse** to navigate to the path from where you want to import the CA group. **NOTE**: Only .pem format is supported.

RELATED DOCUMENTATION

- About the Certificate Authority Group Page | 255
- Add a CA Group | 257
- Edit a CA Group | 258
- Delete CA Group | 259
- Search Text in the Certificate Authority Group Table | 259

Add a CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To add a CA group:

1. Click the add icon (+).

   The Add CA Group page appears.
2. Complete the configuration according to the guidelines provided in Table 68 on page 258.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

   If you click **OK**, a new CA group with the provided configuration is created.

   After added a CA group, you can use it for IPsec VPN.

Table 68: Fields on the Add CA Group Page

Field	Action
CA Group Name	Enter a unique CA group name.
CA Profiles	Select a CA profile name from the list in the Available column and then click the right arrow to move it to the Selected column. **NOTE**: You can add up to maximum of 20 CA profiles per trusted CA group.

RELATED DOCUMENTATION

- About the Certificate Authority Group Page | 255
- Import a Trusted CA Group | 256
- Edit a CA Group | 258
- Delete CA Group | 259
- Search Text in the Certificate Authority Group Table | 259

Edit a CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To edit a CA group:

1. Select a CA group.
2. On the upper right side of the Certificate Authority Group page, click the pencil icon.

   See "Add a CA Group" on page 257 for the options available for editing on the Edit CA Group page.
3. Click **OK**

RELATED DOCUMENTATION

- About the Certificate Authority Group Page | 255
- Import a Trusted CA Group | 256
- Add a CA Group | 257

Delete CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To delete a CA group:

1. Select a CA group.
2. On the upper right side of the Certificate Authority Group page, click the delete icon to delete.

   A confirmation window appears.
3. Click **Yes** to delete.

RELATED DOCUMENTATION

Search Text in the Certificate Authority Group Table

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.

   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

About the Certificate Authority Group Page | **255**

Import a Trusted CA Group | **256**

Add a CA Group | **257**

Edit a CA Group | **258**

Delete CA Group | **259**

CHAPTER 18

License Management

IN THIS CHAPTER

Manage Your Licenses

IN THIS SECTION

About License Management Page

You are here: **Device Administration** > **License Management**.

You can add a new license key, delete one or more license keys, update, or download license keys.

Table 69 on page 262 describes the fields on the License Management page.

Table 69: Fields on the License Maintenance Page

Field	Function
Feature	Displays the name of the licensed feature.
Licenses Used	Displays the number of licenses currently being used on the device. Usage is determined by the configuration on the device. If a feature license exists and that feature is configured, the license is considered used.
Licensed Installed	Displays the number of licenses installed on the device for the particular feature.
Licenses Needed	Displays the number of licenses required for legal use of the feature. Usage is determined by the configuration on the device. If a feature is configured and the license for that feature is not installed, a single license is needed.
License Expires on	Displays the expiry details on the license feature.

Add License

To add a new license key with the J-Web license manager:

1. Perform one of the following:

   - **License File URL**—Enter the full URL to the destination file containing the license key.

     NOTE: Use this option to send a subscription-based license key entitlement (such as UTM) to the Juniper Networks licensing server for authorization. If authorized, the server downloads the license to the device and activates it.

   - **License Key**—Paste the license key text, in plain-text format, for the license.

     Use a blank line to separate multiple license keys.

> **NOTE**: Use this option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.)

2. Click **OK** to add the license key or click **Cancel** to return to the License Management page.

Delete Installed Licenses

To delete one or more license keys with the J-Web license manager:

1. Select the check box of the license or licenses you want to delete.
2. Click **Delete**.

> **NOTE**: If you have deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

3. Click **OK** to delete the selected license or licenses or click **Cancel** to return to the License Management page.

Update Installed Licenses

To send license update to the License Management Server (LMS):

1. Click **Update**.

   The Update Licenses page appears.
2. Click **OK** to send license update to LMS.

Update Trial Licenses

To send license update to the LMS and to update the trail licenses:

1. Click **Update Trial**.

   The Update Trial Licenses page appears.
2. Click **OK** to update the trail licenses.

Display License Keys

To display the license keys installed on the device with the J-Web license manager:

1. Click **Display Keys** to view all of the license keys installed on the device.
2. Click **Back** to return to the License Management page.

Download License Keys

Downloads the license keys installed on the device with the J-Web license manager.

1. Click **Download Keys** to download all of the license keys installed on the device to a single file.
2. Select **Save it to disk** and specify the file to which the license keys are to be written.

Software Feature Licenses

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. Table 70 on page 264 describes the Junos OS features that require licenses.

Table 70: Junos OS Services Feature Licenses

Junos OS License Requirements	Device								
Feature	J Series	SRX100	SRX210	SRX220	SRX240	SRX650	SRX1000 Line	SRX3000 Line	SRX5000 Line
Access Manager			X		X				
BGP Route Reflectors	X		X		X	X			
Dynamic VPN		X	X	X	X	X			
IDP Signature Update	X	X *	X *	X *	X *	X	X	X	X
Application Signature Update (Application Identification)							X	X	X
Juniper-Kaspersky Anti-Virus	X	X	X	X	X	X			
Juniper-Sophos Anti-Spam	X	X	X	X	X	X			
Juniper-Websense Integrated Web Filtering	X	X	X	X	X	X			

Table 70: Junos OS Services Feature Licenses *(Continued)*

Junos OS License Requirements	Device								
Feature	J Series	SRX100	SRX210	SRX220	SRX240	SRX650	SRX1000 Line	SRX3000 Line	SRX5000 Line
SRX100 Memory Upgrade		X							
UTM	X		X *		X *	X			

RELATED DOCUMENTATION

Enroll Your Device with Juniper ATP Cloud | **279**

CHAPTER 19

Security Package Management

IN THIS CHAPTER

About the Security Package Management Page

IN THIS SECTION

You are here: **Device Administration** > **Security Package Management**

Use this page to configure the SRX Series device to install, upload, and automatically download the updated security packages from the specified URL.

You can perform the following tasks from this page:

- IPS signatures:
  - Install and upload IPS signatures package. See "Install or Upload IPS Signatures Package" on page 270.
  - Configure IPS signatures settings. See "IPS Signatures Settings" on page 272.

- Application signatures:
  - Install an application signature package. See "Install Application Signatures Package" on page 274.
  - Configure application signature package install settings. See "Application Signatures Settings" on page 274.
- URL categories:
  - Install an URL category package. See "Install URL Category Package" on page 276.
  - Configure URL category package install settings. See "URL Categories Settings" on page 276.

Field Descriptions

Table 71 on page 267 to Table 73 on page 269 describes the fields on the Security Package Management page.

Table 71: Fields on the IPS Signatures Page

Field	Description
Installed IPS Signature Package	
Version	Displays the security package version that is currently installed on the device.
Status	Displays the following statuses of the security package installation: • *<Version number>* installation in progress • Installed successfully • Failed
Published Date	Displays the security package released date and time.
Detector	Displays the detector version number that is currently installed on the device.
Rollback Action	Displays the previously installed security package version on the system. Click the version number to rollback to the previous version.

Table 71: Fields on the IPS Signatures Page *(Continued)*

Field	Description
Latest IPS Signature Package	
Version	Displays the ten latest security package versions.
View Details	Click **View Details** to learn more about the security package version.
Install	You can choose either of the options: • Install package—Installs the selected security package version on the device. • Upload package—Uploads a selected package version to install it on the device.
Settings	You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time.

Table 72: Fields on the Application Signatures Page

Field	Description
Installed Application Signature Package	
Version	Displays the security package version that is currently installed on the device.
Status	Displays the following statuses of the security package installation: • *<Version number>* installation in progress • Installed successfully • Failed
Published Date	Displays the security package released date and time.

Table 72: Fields on the Application Signatures Page *(Continued)*

Field	Description
Rollback Action	Displays the previously installed security package version on the system. Click the version number to roll back to the previous version.
Latest Application Signature Package	
Version	Displays the ten latest security package versions.
View Details	Click **View Details** to learn more about the security package version.
Install	You can choose to install the selected security package version on the device.
Install Settings	You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time.

Table 73: Fields on the URL Categories Page

Field	Description
URL Category Package	
Version	Displays the Enhanced Web Filtering (EWF) categories package version that is currently installed on the device.
Status	Displays the following statuses of the security package installation: • *<Version number>* installation in progress • Installed successfully • Failed
Base Filter	Click the base filter name to view the available URL categories.

Table 73: Fields on the URL Categories Page *(Continued)*

Field	Description
Install	Installs the latest EWF category package on the device.
Install Settings	You can configure a proxy server to download and install EWF categories package. You can also schedule an automatic installation of EWF categories package for a later date and time.

RELATED DOCUMENTATION

- Install or Upload IPS Signatures Package | 270
- Install Application Signatures Package | 274
- Install URL Category Package | 276
- IPS Signatures Settings | 272
- Application Signatures Settings | 274
- URL Categories Settings | 276

Install or Upload IPS Signatures Package

You are here: **Device Administration** > **Security Package Management**.

You can choose to install the selected security package version or upload a selected package version to install it on the device.

NOTE: When using either of the installation methods, you can continue to configure the other features while the installation is in progress. Once the installation is complete, you will see a notification on the UI.

To install the security packages:

1. Select a security package version you want to install and then click **Install** available at the top-right of the Latest IPS Signature Package table.
2. Click **Install package** to install the selected security package version.

   The installation status is shown in the Status column of the Installed IPS Signature Package table.

To upload the security packages (offline security packages installation):

1. Click **Install** available at the top-right of the Latest IPS Signature Package table. Then, select **Upload package**.
2. Click **Browse** to upload a downloaded security package version and then click **OK**.

   The installation starts automatically and the status is shown in the Status column of the Installed IPS Signature Package table.

   To download the security package on the host machine:

   a. Go to https://support.juniper.net/support/downloads/.

   b. Select **All Products** from the list and enter the *SRX Series model*. For example, SRX300.

   c. Press **Enter** or click **Find a Product**.

   d. Scroll down and go to **Related Software** section.

   e. Click **+** and click on the Offline Signature Files.

      You are directed to the Download Results page.

   f. Click **+** to choose any one of the following:

      - Offline APPID Sigpack Files—This includes only the App ID files.
      - Offline Sigpack Files—This includes both IPS and App ID files.

   g. Click the **gz** link of the package you want to download from the Downloads column.

      You are directed to the Web download site.

   h. Log in with your username and password.

   i. Select **I agree** for the EULA information and click **Proceed**.

   j. On the Download Software page that appears, the following options are available:

      - If you want to download the package on your host machine, click the **CLICK HERE** link and save the file to your machine.
      - If you want to download the package on your device, copy the URL and install it on the device using the CLI commands.

RELATED DOCUMENTATION

About the Security Package Management Page | 266

Install Application Signatures Package | 274

Install URL Category Package | 276

IPS Signatures Settings

You are here: **Device Administration** > **Security Package Management**

You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time.

To configure the security package installation settings:

1. Click the Settings icon available at the top-right of the Latest IPS Signature Package table. The Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 74 on page 272.
3. Click **OK**.
   The security package will automatically install in the scheduled interval. The installation status is shown in the Status column of the Installed IPS Signature Package table.

Table 74: Fields on the Settings Page

Field	Action
Security Package URL	Displays the URL from where the security package is downloaded. Default URL is https://signatures.juniper.net/cgi-bin/index.cgi.
Routing Instance	Select a routing instance from the list to reach the proxy server. To create a new routing instance, click **Create New**. For more information on the fields, see "Add a Routing Instance" on page 537.

Table 74: Fields on the Settings Page *(Continued)*

Field	Action
Proxy profile	This is optional. Select a proxy profile from the list. The proxy profile acts as a proxy server to download the security package. To create a new proxy profile, click **Create New**. For more information on the fields, see "Add a Proxy Profile" on page 800.
Schedule Install	
Schedule	Enable the option to schedule automatic download and installation of security package at a specific date, time, and interval. **NOTE**: The package also includes application signatures. If you've set up a separate schedule for installing application signatures, then this schedule will take precedence.
Start Time	Select a time to start automatic download and to install the updated security package from the specified URL. Format: YYYY-MM-DD.hh:mm (24 hours).
Interval	Amount of time (in hours) that the device waits before updating the security package. Range: 1 through 336

RELATED DOCUMENTATION

- About the Security Package Management Page | **266**
- Install Application Signatures Package | **274**
- Install Application Signatures Package | **274**
- Install URL Category Package | **276**

Install Application Signatures Package

You are here: **Device Administration** > **Security Package Management**.

You can choose to install the selected security package version on the device.

To install the security packages:

1. Select a security package version you want to install and then click **Install** available at the top-right of the Latest Application Signature Package table.
2. Click **Install package** to install the selected security package version.

   The installation status is shown in the Status column of the Installed Application Signature Package table.

RELATED DOCUMENTATION

- About the Security Package Management Page | **266**
- Install or Upload IPS Signatures Package | **270**
- Install URL Category Package | **276**

Application Signatures Settings

You are here: **Device Administration** > **Security Package Management**

You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time.

To configure the security package installation settings:

1. Click the Settings icon available at the top-right of the Latest Application Signature Package table. The Install Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 75 on page 275.
3. Click **OK**.

   The security package will automatically install in the scheduled interval. The installation status is shown in the Status column of the Installed Application Signature Package table.

Table 75: Fields on the Install Settings Page

Field	Action
Security Package URL	Displays the URL from where the security package is downloaded. Default URL is https://signatures.juniper.net/cgi-bin/index.cgi.
Proxy profile	This is optional. Select a proxy profile from the list. The proxy profile acts as a proxy server to download the security package. To create a new proxy profile, click **Create New**. For more information on the fields, see "Add a Proxy Profile" on page 800.
Schedule Install	
Schedule	Enable the option to schedule automatic download and installation of security package at a specific date, time, and interval. **NOTE**: If IPS signatures package installation is already scheduled, then it also includes application signatures package. If you want to set up a separate schedule for installing application signatures, then disable the Schedule option for IPS signatures.
Start Time	Select a time to start automatic download and to install the updated security package from the specified URL. Format: YYYY-MM-DD.hh:mm (24 hours).
Interval	Amount of time (in hours) that the device waits before updating the security package. Range: 1 through 336

RELATED DOCUMENTATION

About the Security Package Management Page | 266

Install URL Category Package

You are here: **Device Administration** > **Security Package Management**.

You can choose to install the latest URL category package version to install it on the device.

To install the latest URL category package:

1. Click **Install** available at the top-right of the URL Category Package table.
2. Click **Install package** to install the latest URL category package version.
   The installation status is shown in the Status column of the URL Category Package table.

RELATED DOCUMENTATION

URL Categories Settings

You are here: **Device Administration** > **Security Package Management**

You can configure a proxy server to download and install EWF categories package. You can also schedule an automatic installation of EWF categories package for a later date and time.

To configure the EWF categories package installation settings:

1. Click the Settings icon available at the top-right of the URL Category Package table.
   The Install Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 76 on page 277.
3. Click **OK**.
   The EWF categories package will automatically install in the scheduled interval. The installation status is shown in the Status column of the URL Category Package table.

Table 76: Fields on the Install Settings Page

Field	Action
Security Package URL	Displays the URL from where the EWF categories package is downloaded. Default URL is https://update.juniper-updates.net/.
Routing Instance	Select a routing instance from the list to reach the proxy server. To create a new routing instance, click **Create New**. For more information on the fields, see "Add a Routing Instance" on page 537.
Proxy profile	This is optional. Select a proxy profile from the list. The proxy profile acts as a proxy server to download the EWF categories package. To create a new proxy profile, click **Create New**. For more information on the fields, see "Add a Proxy Profile" on page 800.
Schedule Install	
Schedule	Enable the option to schedule automatic download and installation of EWF categories package at a specific date, time, and interval.
Start Time	Select a time to start automatic download and to install the updated EWF categories package from the specified URL. Format: YYYY-MM-DD.hh:mm (24 hours).
Interval	Amount of time (in hours) that the device waits before updating the EWF categories package. Range: 1 through 336

RELATED DOCUMENTATION

- About the Security Package Management Page | **266**
- Install or Upload IPS Signatures Package | **270**
- Install Application Signatures Package | **274**

CHAPTER 20

ATP Management

IN THIS CHAPTER

Enroll Your Device with Juniper ATP Cloud

Before enrolling a device:

- Ensure that you have a Juniper ATP Cloud account with an associated license (free, basic, or premium) to configure a Juniper ATP Cloud realm. The license controls the features of the Juniper ATP Cloud. For more information on the Juniper ATP Cloud account, see Registering a Juniper Advanced Threat Prevention Cloud Account.
- Decide which region the realm you create will cover because you must select a region when you configure a realm.
- Ensure the device is registered in the ATP cloud portal.
- In the CLI mode, configure `set security forwarding-process enhanced-services-mode` on your SRX300, SRX320, SRX340, SRX345, and SRX550M devices to open ports and get the device ready to communicate with ATP cloud.
- ATP cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet.
- ATP cloud requires the following ports to be open on the SRX Series device: 80, 8080, and 443.

You are here: **Device Administration** > **ATP Management** > **Enrollment**.

Use this page to enroll your SRX Series Firewall with Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud).

Juniper ATP Cloud is a cloud-based threat identification and prevention solution. It protects your device from malware and sophisticated cyber threats by inspecting e-mail and web traffic for advanced threats.

Juniper ATP Cloud integrates with the SRX Series devices to simplify its deployment and enhance the anti-threat capabilities of the SRX Series Firewall.

ATP uses a Junos OS operation (op) script to help you configure your SRX Series device to connect to the ATP cloud service.

The Junos OS operation (op) script performs the following tasks:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series device.
- Creates local certificates and enrolls them with the cloud server.
- Performs basic ATP cloud configuration on the SRX Series device.
- Establishes a secure connection to the cloud server.

To enroll your device with Juniper ATP Cloud from J-Web:

1. *Proxy Profile Configuration (Optional)*

   a. Select an option in the Proxy Profile list and proceed with Step 2.

   > **NOTE**:
   > - The list displays the existing proxy profiles that you have created using the Proxy Profile page (Security Policies & Objects > Proxy Profiles).
   > - The SRX Series Firewall and Juniper ATP Cloud communicates through the proxy server if a proxy profile is configured. Otherwise, they directly communicate with each other.

   b. Or click **Create Proxy** to create a proxy profile.

      The Create Proxy Profile page appears.

   c. Complete the configuration by using the guidelines in Table 77 on page 281.

   d. Click **OK**.

      A new proxy profile is created.

   e. Click **Apply Proxy**.

      Applying proxy enables the SRX Series Firewall and Juniper ATP Cloud to communicate through the proxy server.

Table 77: Fields on the Create Proxy Profile Page

Field	Action
Profile Name	Enter a name for the proxy profile.
Connection Type	Select the connection type server from the list that proxy profile uses: • Server IP—Enter the IP address of the proxy server. • Host Name—Enter the name of the proxy server.
Port Number	Select a port number for the proxy profile. Range is 0 to 65535.

2. *Enroll SRX Series Firewall with ATP Cloud*

   a. Click **Enroll**.

      The ATP Cloud Enrollment page appears.

      NOTE: If there are any existing configuration changes, a message appears for you to commit the changes and then to proceed with the enrollment process.

   b. Complete the configuration by using the guidelines in Table 78 on page 282.

   c. Click **OK**.

      The SRX Series Firewall enrollment progress, successful message, or any errors will be shown at the end of the ATP Cloud Enrollment page.

      NOTE:

      - A new realm is created if you have enabled **Create New Realm** and then the SRX Series Firewall is enrolled to Juniper ATP Cloud. If there is any existing enrollment for the same SRX Series Firewall, CLI sends the data to Juniper ATP Cloud portal to do the duplicate validation during the enrollment process. You cannot check for the duplicate validation through J-Web.
      - Click **Diagnostics** to troubleshoot any enrollment errors.

- Click **UnEnroll** if you wish to disenroll your device from ATP

Table 78: Fields on the ATP Cloud Enrollment Page

Field	Description
Create New Realm	By default, this option will be disabled if you have an ATP Cloud account with an associated license. Enable this option to add a new realm if you do not have an ATP Cloud account with an associated license.
Location	Select a region of the world from the list.
Email	Enter your E-mail address.
Password	Enter a unique string at least eight characters long. It must include both uppercase letters, lowercase letters, and at least one number. It can also include special characters. No spaces are allowed and you cannot use the same sequence of characters that are in your e-mail address.
Confirm Password	Reenter the password.
Company Name	Enter a company name to enroll into the realm. A company name can only contain alphanumeric characters, special characters (underscore and dash).
Realm	Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed.

About the Diagnostics Page

You are here: **Device Administration** > **ATP Management** > **Diagnostics**.

Use this page to diagnose and verify threat prevention.

Table 79 on page 283 describes the fields on the Diagnostics page.

Table 79: Fields on the Diagnostics Page

Field	Description
Diagnostics	
ATP Diagnostics	Select an option from the list to diagnose.
Diagnostics Logs	Displays the diagnostic logs for the selected option.
Run Diagnostics	Enables you to see the diagnostics of a certain region.
Check Connectivity	
Check	Click **Check** to verify the connectivity.
Server Details	
Server hostname	Specify the host name of the server.
Server realm	Specifies the name of a server realm.
Server port	Specify the server port number.
Connection Plane	
Connection time	Specify the connection time of the server.
Connection Status	Specify the connection status.
Service Plane	
Card Info	Specify the card number.
Connection Active Number	Specify the connection active numbers.

Table 79: Fields on the Diagnostics Page *(Continued)*

Field	Description
Connection Relay statistics	Specify the connection relay statistics.
Other Details	
Configured Proxy Server	Specify the configured proxy server.
Port Number	Specify the port number of the proxy server.

RELATED DOCUMENTATION

Monitor Threat Prevention | 111

CHAPTER 21

Operations

IN THIS CHAPTER

Maintain Files

IN THIS SECTION

About Files Page

You are here: **Device Administration** > **Operations** > **Files**.

You can clean up files, download, or delete files and delete the JUNOS Package backup.

Clean Up Files

To maintain files:

1. Click **Clean Up Files**.

   The device will perform the following tasks:

- Rotates log files—Indicates all information in the current log files is archived and fresh log files are created.
- Deletes log files in **/var/log**—Indicates any files that are not currently being written to are deleted.
- Deletes temporary files in **/var/tmp**—Indicates any files that have not been accessed within two days are deleted.
- Deletes all crash files in **/var/crash**—Indicates any core files that the device has written during an error are deleted.
- Deletes all software images (***.tgz** files) in **/var/sw/pkg**—Indicates any software image copied to this directory during software upgrades are deleted.

The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.

2. Click one:
   - **OK**—Deletes the files and returns to the Files page.
   - **Cancel**—Cancels your entries and returns to the Files page.

Download and Delete Files

Table 80 on page 286 provides the maintenance options to download and delete files.

Table 80: Download and Delete Files Maintenance Options

File Type	Function
Log Files	Lists the log files located in the **/var/log** directory on the device. Select an option: • **Delete**—Deletes files. • **Download**—Downloads files.

Table 80: Download and Delete Files Maintenance Options *(Continued)*

File Type	Function
Temporary Files	Lists the temporary files located in the **/var/tmp** directory on the device. Select an option: • **Delete**—Deletes files. • **Download**—Downloads files.
Jailed Temporary Files	Lists the jailed temporary files located in the **/var/jail/tmp** directory on the device. Select an option: • **Delete**—Deletes files. • **Download**—Downloads files.
Old JUNOS Software	Lists the software images located in the **/var/sw/pkg** (***.tgz** files) directory on the device. Select an option: • **Delete**—Deletes files. • **Download**—Downloads files.
Crash (Core) File	Lists the core files located in the **/var/crash** directory on the device. Select an option: • **Delete**—Deletes files. • **Download**—Downloads files.

Table 80: Download and Delete Files Maintenance Options *(Continued)*

File Type	Function
Database Files	Lists the database files located in the **/var/db** directory on the device. Select an option: • **Delete**—Deletes files. • **Download**—Downloads files.

Delete Backup JUNOS Package

Table 81 on page 288 provides the maintenance options to delete the JUNOS Package backup.

Table 81: Delete Backup JUNOS Package Files Maintenance Options

Field	Function
Delete backup Junos package	Reviews the backup image information listed. Click **Delete backup JUNOS package** and then select an option. **NOTE**: The **Delete backup** option is hidden if the router is in dual-root partitioning scheme The available options are: • **OK**—Deletes the backup image and returns to the Files page. • **Cancel**—Cancels the deletion of the backup image and returns to the Files page.

SEE ALSO

Maintain Reboot Schedule | 289

Maintain System Snapshots | 290

Maintain Reboot Schedule

You are here: **Device Administration** > **Operations** > **Reboot**.

You can schedule reboot or halt the system using options such as reboot Immediately, reboot in, reboot with the system time, or halt immediately.

NOTE: A halted system can only be accessed from the system console port.

To reboot or halt the system:

1. Complete the configuration according to the guidelines provided in Table 82 on page 289.

Table 82: Reboot Schedule Maintenance Options

Field	Action
Reboot Immediately	Select this option to reboot the device immediately.
Reboot in *number of* minutes	Select this option to reboot the device after the specified number of minutes from the current time.
Reboot when the system time is *hour:minute*	Select this option to reboot the device at the absolute time that you specify, on the current day. Select a two-digit hour in 24-hour format and a two-digit minute.
Halt Immediately **NOTE**: This option is not available in SRX4600 device.	Select this option to stop the device immediately. After the software has stopped, you can access the device through the console port only.
Reboot From Media **NOTE**: This option is not available in SRX4600 device.	Choose the boot device from the Reboot From Media list: • **internal**—Reboots from the internal media (default). • **usb**—Reboots from the USB storage device.

Table 82: Reboot Schedule Maintenance Options *(Continued)*

Field	Action
Message	Type a message to be displayed to the user on the device before the reboot occurs.

2. Click **Schedule**.

   Schedules a reboot based on the scheduled configuration.

3. The J-Web interface requests confirmation to perform the reboot or to halt.

   Click **OK** to confirm to reboot or alt the system or click **Cancel** to return to the Reboot page.

NOTE:

- If the reboot is scheduled to occur immediately, the device reboots. You cannot access J-Web until the device has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web login page.
- If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web interface Reboot page.
- If the device is halted, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.
- If you cannot connect to the device through the console port, shut down the device by pressing and holding the power button on the front panel until the POWER LED turns off. After the device has shut down, you can power on the device by pressing the power button again. The POWER LED lights during startup and remains steadily green when the device is operating normally.

RELATED DOCUMENTATION

Maintain System Snapshots | 290

Maintain System Snapshots

You are here: **Device Administration** > **Operations** > **Snapshot**.

You can configure boot devices to replace primary boot device or to act as a backup boot device.

The snapshot process copies the current system software, along with the current and rescue configurations, to alternate media. Optionally, you can copy only the factory and rescue configurations.

To maintain the system snapshots, you create a snapshot of the running system software and save the snapshot to an alternate media.

1. Complete the configuration according to the guidelines provided in Table 83 on page 291.
2. Click **Snapshot**.

   Creates a boot device on an alternate media.
3. Click **OK** to perform the system snapshot to a media or click **Cancel** to return to the Snapshot page.

Table 83: Snapshot Maintenance Options

Field	Function
Target Media	Specifies the boot device to copy the snapshot to. **NOTE**: You cannot copy software to the active boot device. Select an option for a boot device that is not the active boot device: • **internal**—Copies software to the internal media. • **usb**—Copies software to the device connected to the USB port.
Partition	Partitions the media. This process is usually necessary for boot devices that do not already have software installed on them. Select the check box.
Factory	Copies only the default files that were loaded on the internal media when it was shipped from the factory, plus the rescue configuration if one has been set. Select the check box. **NOTE**: After a boot device is created with the default factory configuration, it can operate only in an internal media slot.

RELATED DOCUMENTATION

Upload Software Packages | 293

Install Software Packages | 294

Rollback Software Package Version | 295

CHAPTER 22

Software Management

IN THIS CHAPTER

Upload Software Packages

You are here: **Device Administration** > **Software Management** > **Upload Package**.

You can upload a software package file to the device for installation.

To upload software packages:

1. Complete the configuration according to the guidelines provided in Table 84 on page 293.

Table 84: Upload Package Maintenance Options

Field	Action
File to Upload	Enter the location of the software package on the local system or click **Choose File** to navigate to the location.
Reboot If Required	Select the check box to automatically reboot when the upgrade is complete.
Do not save backup	Select the check box so that backup copy of the current Junos OS package is not saved.

Table 84: Upload Package Maintenance Options *(Continued)*

Field	Action
Format and re-partition the media before installation **NOTE**: This option is not available for SRX4600 devices.	Select the check box to format the internal media with dual-root partitioning.

2. Click **Upload and Install Package**.

   The software is activated after the device has rebooted.

RELATED DOCUMENTATION

Install Software Packages | 294

Rollback Software Package Version | 295

Install Software Packages

You are here: **Device Administration** > **Software Management** > **Install Package**.

You can install a software package from a remote server.

To install software packages:

1. Complete the configuration according to the guidelines provided in Table 85 on page 294.

   Table 85: Install Package Maintenance Options

Field	Action
Package Location	Enter the full address of the software package location on the FTP or HTTP server. For example, use one of the following formats: ***ftp://hostname/pathname/package-name*** ***http://hostname/pathname/package-name***

Table 85: Install Package Maintenance Options *(Continued)*

Field	Action
User	Enter the username to use on a remote server.
Password	Enter the password to use on a remote server.
Reboot If Required	Select the check box to automatically reboot when the upgrade is complete.
Do not save backup	Select the check box so that backup copy of the current Junos OS package is not saved.
Format and re-partition the media before installation	Select the check box to format the internal media with dual-root partitioning.

2. Click **Fetch and Install Package**.

   The software is activated after the device reboots.

RELATED DOCUMENTATION

Rollback Software Package Version | 295

Rollback Software Package Version

You are here: **Device Administration** > **Software Management** > **Rollback**.

You can rollback to the previously installed version of the device software.

To rollback software package version:

1. Click **Rollback** to rollback to the previous version of the software.

   NOTE: You cannot stop the process once the rollback operation is requested.

2. Reboot the device when the rollback process is complete and for the new software to take effect. To reboot, perform the steps in "Maintain Reboot Schedule" on page 289.

> **NOTE**: To rollback to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

RELATED DOCUMENTATION

Upload Software Packages | **293**

Install Software Packages | **294**

CHAPTER 23

Configuration Management

IN THIS CHAPTER

Manage Upload Configuration Files

You are here: **Device Administration** > **Configuration Management** > **Upload**.

You can compare two configuration files, download a configuration file to your local system, or roll back the configuration to any of the previous versions stored on the device.

To manage upload configuration files:

1. Enter the absolute path and filename in the **File to Upload** box.

   NOTE: You can also click **Browse** to navigate to the file location and select it.

2. Click **Upload and Commit** to upload and commit the configuration.

   The device checks the configuration for the correct syntax before committing it.

   NOTE: The file configuration replaces the existing configuration and continues the upload and commit process. If any errors occur when the file is loading or committing, J-Web displays the error and restores the previous configuration.

RELATED DOCUMENTATION

Manage Configuration History | 298

Manage Rescue Configuration | 302

Manage Configuration History

You are here: **Device Administration** > **Configuration Management** > **History**.

You can view configuration history and database information about users editing the configuration database.

To manage configuration history:

1. Complete the configuration according to the guidelines provided in Table 86 on page 298.

   Table 86: History Maintenance Options

Field	Function
Number	Indicates the version of the configuration file. To view a configuration, click the **version number**.
Date/Time	Indicates the date and time the configuration was committed.
User	Indicates the name of the user who committed the configuration.

Table 86: History Maintenance Options *(Continued)*

Field	Function
Client	Indicates the method by which the configuration was committed. The available options are: • **cli**—A user entered a Junos OS CLI command. • **junoscript**—A Junos XML management protocol client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way. • **snmp**—An SNMP **set** request started the operation. • **button**—The CONFIG button on the router was pressed to commit the rescue configuration (if set) or to clear all configurations except the factory configuration. • **autoinstall**—Autoinstallation is performed. • **other**—Another method was used to commit the configuration.
Comment	Indicates comments.

Table 86: History Maintenance Options *(Continued)*

Field	Function
Log Message	Indicates the method used to edit the configuration. • **Imported via paste**—Configuration was edited and loaded with the **Device Administration** > **Tools** > **CLI Editor** option. • **Imported upload** [*filename*]—Configuration was uploaded with the **Device Administration** > **Configuration Management** > **Upload** option. • **Modified via** *quick-configuration*—Configuration was modified with the specified version of the J-Web user interface. • **Rolled back via** *user-interface*—Configuration was rolled back to a previous version through the user interface specified by *user-interface*, which can be **Web Interface** or **CLI**.

Table 86: History Maintenance Options *(Continued)*

Field	Function
Action	Indicates action to perform with the configuration file. Select any one of the following available options: • **Download**—Downloads a configuration file to your local system. Select the options on your Web browser to save the configuration file to a target directory on your local system. The file is saved as an ASCII file. • **Rollback**—Rolls back the configuration to any of the previous versions stored on the device. The History page displays the results of the rollback operation. **NOTE**: Click **Rollback** to load the device and download the selected configuration. This behavior is different from entering the **rollback** configuration mode command from the CLI, where the configuration is loaded, but not committed.

2. To compare configurations files:

   a. Select any two configuration files you want to compare.

   b. Click **Compare**.

      The History page displays the differences between the two configuration files at each hierarchy level as follows:

      - Lines that have changed are highlighted side by side in green.
      - Lines that exist only in the most recent configuration file are displayed in red on the left.
      - Lines that exist only in the least recent configuration file are displayed in blue on the right.

RELATED DOCUMENTATION

Manage Rescue Configuration | 302

Manage Upload Configuration Files | 297

Manage Rescue Configuration

You are here: **Device Administration** > **Configuration Management** > **Rescue**.

If you inadvertently commit a configuration that denies management access, the only recourse may be to connect the console. Alternatively, you can rescue configuration that allows the management access to the device.

To load and commit the rescue configuration, press and immediately release the **Config** button on the chassis.

You can set or delete the rescue configuration.

To set or delete rescue configuration:

Click one:

- **View rescue configuration**—Displays the current rescue configuration (if it exists).
- **Set rescue configuration**—Sets the current running configuration as the rescue configuration. Click **OK** to confirm or **Cancel** to return to the Rescue page.
- **Delete rescue configuration**—Deletes the current rescue configuration. Click **OK** to confirm or **Cancel** to return to the Rescue page.

RELATED DOCUMENTATION

Manage Your Licenses | 261

Manage Device Certificates

CHAPTER 24

Alarm Management

IN THIS CHAPTER

Monitor Chassis Alarm

IN THIS SECTION

About Chassis Alarm Page

You are here: **Device Administration** > **Alarm Management** > **Chassis Alarm**.

You can create a chassis alarm definition by selecting various options such as DS1, Ethernet, and integrated service, and so on.

Create Chassis Alarm Definition

To create Chassis Alarm Definition:

1. Enter the information specified in Table 87 on page 304 to create Chassis Alarm Definition.

Table 87: Chassis Alarm Definition Options

Chassis Component	Alarm Configuration Option
DS1	Alarm indicator signal (ais) Yellow alarm (ylw) Select an alarm condition from the list for DS1: • Ignore • Red • Yellow • None
Ethernet	Link is down (link-down) Select an alarm condition from the list for Ethernet: • Ignore • Red • Yellow • None
Integrated Services	Hardware or software failure (failure) Select an alarm condition from the list for Integrated Services: • Ignore • Red • Yellow • None

Table 87: Chassis Alarm Definition Options *(Continued)*

Chassis Component	Alarm Configuration Option
Management Ethernet	Link is down (link-down) Select an alarm condition from the list for Management Ethernet: • Ignore • Red • Yellow • None
Optical Transport Network Optical channel Data Unit (OTN ODU)	Backward defect indication (odu-bdi) Payload type mismatch (odu-ptim) Trail trace identifier mismatch (odu-ttim) Select an alarm condition from the list for OTN ODU: • Ignore • Red • Yellow • None

Table 87: Chassis Alarm Definition Options *(Continued)*

Chassis Component	Alarm Configuration Option
Optical Transport Network Optical channel Transport Unit (OTN OTU)	Loss of frame (oc-lof) Loss of multiframe (oc-lom) Loss of signal (oc-los) Backward defect indication (oc-bdi) Forward error correction excessive FEC errors (out-fec-excessive-errs) Incoming alignment error (out-iae) Trail trace identifier mismatch (out-ttim) Wavelength-Lock (Wavelength Lock) Select a alarm condition from the list for OTN OTU: • Ignore • Red • Yellow • None
Serial	Clear-to-send (CTS) signal absent (cts-absent) Data carrier detect (DCD) signal absent (dcd-absent) Data set ready (DSR) signal absent (dsr absent) Loss of receive clock (loss-of-rx-clock) Loss of transmit clock (loss-of-tx-clock) Select an alarm condition from the list for Serial: • Ignore • Red • Yellow • None

Table 87: Chassis Alarm Definition Options *(Continued)*

Chassis Component	Alarm Configuration Option
Services	Services module hardware down (hw-down) Services link down (linkdown) Services module held in reset (pic-hold-reset) Services module reset (pic-reset) Receive errors (rx-errors) Services module software down (sw-down) Transmit errors (tx-errors) Select an alarm condition from the list for Services: • Ignore • Red • Yellow • None

Table 87: Chassis Alarm Definition Options *(Continued)*

Chassis Component	Alarm Configuration Option
DS3	Alarm indication signal (ais) Excessive number of zeros (exz) Far-end receive failure (ferf) Idle alarm (idle) Line code violation (lcv) Loss of frame (lof) Loss of signal (los) Phase-locked loop out of lock (pll) Yellow alarm (ylw) Select an alarm condition from the list for DS3: • Ignore • Red • Yellow • None

2. Click **OK** to create Chassis Alarm Definition.
   The Chassis Alarm Definition page appears.
3. Click **Cancel** to cancel your entries and returns to the Chassis Alarm Definition page.

Edit Chassis Alarm Definition

To edit Chassis Alarm Definition:

1. Click the pencil icon on the upper right side of the Chassis Alarm Definition page.
   See Table 87 on page 304 for the options available for editing the Chassis Alarm Definition page.
2. Click **OK**.

RELATED DOCUMENTATION

Monitor System Alarm | 309

Monitor System Alarm

IN THIS SECTION

About System Alarm Page

You are here: **Device Administration** > **Alarm Management** > **System Alarm**.

You can enable system login alarm login classes. The configured Login Classes will display system alarms while logging in.

Create System Alarm Configuration

To create System Alarm Configuration:

1. Enter the information specified in Table 88 on page 309 to create System Alarm Configuration.

Table 88: RPM Information Troubleshooting Options

Field	Function
Currently Running Tests	
Graph	Click the Graph link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.
Test Name	Configured name of the RPM test.

Table 88: RPM Information Troubleshooting Options *(Continued)*

Field	Function
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping
Target Address	IP address or URL of the remote server that is being probed by the RPM test.
Source Address	Explicitly configured source address that is included in the probe packet headers. If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.
Minimum RTT	Shortest round-trip time from the J Series device to the remote server, as measured over the course of the test.
Maximum RTT	Longest round-trip time from the J Series device to the remote server, as measured over the course of the test.
Average RTT	Average round-trip time from the J Series device to the remote server, as measured over the course of the test.
Standard Deviation RTT	Standard deviation of round-trip times from the J Series device to the remote server, as measured over the course of the test.

Table 88: RPM Information Troubleshooting Options *(Continued)*

Field	Function
Probes Sent	Total number of probes sent over the course of the test.
Loss Percentage	Percentage of probes sent for which a response was not received.
Round-Trip Time for a Probe	
Samples	Total number of probes used for the data set. The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.
Latest Sample	System time when the last probe in the sample was received.
Mean Value	Average round-trip time for the 50-probe sample.
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.
Lowest Value	Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.
Highest Value	Longest round-trip time from the J Series device to the remote server, as measured over the 50-probe sample.

Table 88: RPM Information Troubleshooting Options *(Continued)*

Field	Function
Time of Highest Sample	System time when the highest value in the 50-probe sample was received.
Cumulative Jitter for a Probe	
Samples	Total number of probes used for the data set. The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.
Latest Sample	System time when the last probe in the sample was received.
Mean Value	Average jitter for the 50-probe sample.
Standard Deviation	Standard deviation of the jitter values for the 50-probe sample.
Lowest Value	Smallest jitter value, as measured over the 50-probe sample.
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.
Highest Value	Highest jitter value, as measured over the 50-probe sample.
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.

2. Click **OK** to create System Alarm Configuration.

   System Alarm Configuration page appears.

3. Click **Cancel** to cancel your entries and returns to the System Alarm Configuration page.

Edit System Alarm Configuration

To edit System Alarm Configuration:

1. Click the pencil icon on the upper right side of the System Alarm Configuration page.

   See Table 88 on page 309 for the options available for editing the System Alarm Configuration page.
2. Click **OK**.

SEE ALSO

Monitor Chassis Alarm | 303

CHAPTER 25

RPM

IN THIS CHAPTER

Setup RPM

IN THIS SECTION

Problem

Description

You are here: **Device Administration** > **RPM** > **Setup RPM**.

You can configure RPM parameters to monitor real-time performance through the J-Web interface. You can specify an RPM owner, request information related to probe, hardware timestamp, generates Traps, and specify a probe server.

Solution

To configure RPM parameters:

1. Enter the information specified in Table 89 on page 315 to troubleshoot the issue.
2. From the main RPM configuration page, click one:

- **Apply**—Applies the configuration and stays on the RPM configuration page.
- **OK**—Applies the configuration and returns to the RPM configuration page.
- **Cancel**—Cancels your entries and returns to the RPM configuration page.

Table 89: RPM Setup Troubleshooting Options

Field	Function
Probe Owners	
Identification	
Owner Name	Specifies an RPM owner for which one or more RPM tests are configured. In most implementations, the owner name identifies a network on which a set of tests is being run (a particular customer, for example). Type the name of the RPM owner.
Performance Probe Tests	
Identification	
Test name	Specifies a unique name to identify the RPM test. Type the name of the RPM test.
Target (Address or URL)	Specifies an IP address or a URL of a probe target. Type the IP address, in dotted decimal notation, or the URL of the probe target. If the target is a URL, type a fully formed URL that includes **http://**.
Source Address	Specifies an IP address to be used as the probe source address. Type the source address to be used for the probe. If the source IP address is not one of the device's assigned addresses, the packet uses the outgoing interface's address as its source.

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
Routing Instance	Specifies a routing instance over which the probe is sent. Type the routing instance name. The routing instance applies only to probes of type `icmp` and **icmp-timestamp**. The default routing instance is **inet.0**.
History Size	Specifies the number of probe results saved in the probe history. Type a number between 0 and 255. The default history size is 50 probes.
Request Information	
Probe Type	Specifies the type of probe to send as part of the test. Select the desired probe type from the list: • **http-get** • **http-get-metadata** • **icmp-ping** • **icmp-ping-timestamp** • **tcp-ping** • **udp-ping**
Interval	Specifies the wait time (in seconds) between each probe transmission. Type a number between 1 and 255 (seconds).
Test Interval	Specifies the wait time (in seconds) between tests. Type a number between 0 and 86400 (seconds).

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
Probe Count	Specifies the total number of probes to be sent for each test. Type a number between 1 and 15.
Moving Average Size	Specifies the number of samples used for a moving average. Type a number between 0 and 225.
Destination Port	Specifies the TCP or UDP port to which probes are sent. To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server and the remote server must be Juniper Networks devices configured to receive and transmit RPM probes on the same TCP or UDP port. Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.
DSCP Bits	Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is `000000`. Type a valid 6-bit pattern.
Data Size	Specifies the size of the data portion of the ICMP probes. Type a size (in bytes) between 0 and 65507.
Data Fill	Specifies the contents of the data portion of the ICMP probes. Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data.
Hardware Timestamp	

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
One Way Hardware Timestamp	Specifies the hardware timestamps for one-way measurements. To enable one-way timestamping, select the check box.
Hardware Timestamp	Specifies timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter: • ICMP ping • ICMP ping timestamp • UDP ping—destination port UDP-ECHO (port 7) only • UDP ping timestamp—destination port UDP-ECHO (port 7) only To enable timestamping, select the check box.
Destination Interface	Specifies the name of an output interface for probes. Select the interface from the list.
Maximum Probe Thresholds	
Successive Lost Probes	Specifies the total number of probes that must be lost successively to trigger a probe failure and generate a system log message. Type a number between 0 and 15.
Lost Probes	Specifies the total number of probes that must be lost to trigger a probe failure and generate a system log message. Type a number between 0 and 15.

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
Round Trip Time	Specifies the total round-trip time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds).
Jitter	Specifies the total jitter (in microseconds) for a test that triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds).
Standard Deviation	Specifies the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds).
Egress Time	Specifies the total one-way time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds).
Ingress Time	Specifies the total one-way time (in microseconds), from the remote server to the device, that triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds)
Jitter Egress Time	Specifies the total outbound-time jitter (in microseconds) for a test that triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds)

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
Jitter Ingress Time	Specifies the total inbound-time jitter (in microseconds) for a test that triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds).
Egress Standard Deviation	Specifies the maximum allowable standard deviation of outbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds).
Ingress Standard Deviation	Specifies the maximum allowable standard deviation of inbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. Type a number between 0 and 60,000,000 (microseconds).
Traps	
Egress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in outbound time is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Egress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
Egress Time Exceeded	Generates SNMP traps when the threshold for maximum outbound time is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in inbound time is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Time Exceeded	Generates traps when the threshold for maximum inbound time is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Jitter Exceeded	Generates traps when the threshold for jitter in round-trip time is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
Probe Failure	Generates traps when the threshold for the number of successive lost probes is reached. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
RTT Exceeded	Generates traps when the threshold for maximum round-trip time is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Standard Deviation Exceeded	Generates traps when the threshold for standard deviation in round-trip times is exceeded. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Test Completion	Generates traps when a test is completed. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Test Failure	Generates traps when the threshold for the total number of lost probes is reached. • To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Maximum Number of Concurrent Probes	

Table 89: RPM Setup Troubleshooting Options *(Continued)*

Field	Function
Maximum Number of Concurrent Probes	Specifies the maximum number of concurrent probes allowed. Type a number between 1 and 500.
Probe Server	
TCP Probe Server	Specifies the port on which the device is to receive and transmit TCP probes. Type number 7, or a port number from 49160 through 65535.
UDP Probe Server	Specifies the port on which the device is to receive and transmit UDP probes. Type number 7, or a port number from 49160 through 65535.

RELATED DOCUMENTATION

View RPM | 323

View RPM

IN THIS SECTION

Problem

Description

You are here: **Device Administration** > **RPM** > **View RPM**.

You can configure the RPM probes, to view the RPM statistics and to ensure that the device is configured to receive and transmit TCP and UDP RPM probes on correct ports.

You can view the RPM configuration to verify the following information:

- The RPM configuration is within the expected values.
- The RPM probes are functioning and the RPM statistics are within expected values.
- The device is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

In addition to the RPM statistics for each RPM test, the J-Web interface displays the round-trip times and cumulative jitter graphically. In the graphs, the round-trip time and jitter values are plotted as a function of the system time. Large spikes in round-trip time or jitter indicate a slower outbound (egress) or inbound (ingress) time for the probe sent at that particular time.

Solution

To view RPM information:

1. Enter the information specified in Table 90 on page 324.

Table 90: RPM Information Troubleshooting Options

Field	Function
Currently Running Tests	
Graph	Click the Graph link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.
Test Name	Configured name of the RPM test.

Table 90: RPM Information Troubleshooting Options *(Continued)*

Field	Function
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping
Target Address	IP address or URL of the remote server that is being probed by the RPM test.
Source Address	Explicitly configured source address that is included in the probe packet headers. If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.
Minimum RTT	Shortest round-trip time from the J Series device to the remote server, as measured over the course of the test.
Maximum RTT	Longest round-trip time from the J Series device to the remote server, as measured over the course of the test.
Average RTT	Average round-trip time from the J Series device to the remote server, as measured over the course of the test.
Standard Deviation RTT	Standard deviation of round-trip times from the J Series device to the remote server, as measured over the course of the test.

Table 90: RPM Information Troubleshooting Options *(Continued)*

Field	Function
Probes Sent	Total number of probes sent over the course of the test.
Loss Percentage	Percentage of probes sent for which a response was not received.
Round-Trip Time for a Probe	
Samples	Total number of probes used for the data set. The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.
Latest Sample	System time when the last probe in the sample was received.
Mean Value	Average round-trip time for the 50-probe sample.
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.
Lowest Value	Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.
Highest Value	Longest round-trip time from the J Series device to the remote server, as measured over the 50-probe sample.

Table 90: RPM Information Troubleshooting Options *(Continued)*

Field	Function
Time of Highest Sample	System time when the highest value in the 50-probe sample was received.
Cumulative Jitter for a Probe	
Samples	Total number of probes used for the data set. The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.
Latest Sample	System time when the last probe in the sample was received.
Mean Value	Average jitter for the 50-probe sample.
Standard Deviation	Standard deviation of the jitter values for the 50-probe sample.
Lowest Value	Smallest jitter value, as measured over the 50-probe sample.
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.
Highest Value	Highest jitter value, as measured over the 50-probe sample.
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.

RELATED DOCUMENTATION

Setup RPM | 314

CHAPTER 26

Tools

IN THIS CHAPTER

Troubleshoot Ping Host

IN THIS SECTION

About Ping Host Page

You are here: **Device Administration** > **Tools** > **Ping Host**.

The ping diagnostic tool sends a series of ICMP "echo request" packets to the specified remote host.

The receipt of such packets will usually result in the remote host replying with an ICMP "echo response." Note that some hosts are configured not to respond to ICMP "echo requests," so a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you may find that you are not able to ping outside your local network.

You can ping a host to verify that the host can be reached over the network or not.

To use the ping host tool:

1. Enter the information specified in Table 91 on page 330 to troubleshoot the issue.

   The Remote Host field is the only required field.

2. Click the expand icon next to Advanced options.

3. Click **Start**.

   The results of the ping operation are displayed in Table 92 on page 332. If no options are specified, each ping response is in the following format:

   ```
   bytes bytes from ip-address: icmp_seq=number ttl=number time=time
   ```

4. Click **OK** to stop the ping operation before it is complete.

Table 91: Ping Host Troubleshooting Options

Field	Action
Remote Host	Type the hostname or IP address of the host to ping.
Advanced Options	
Don't Resolve Addresses	• To suppress the display of the hop hostnames along t the path, select the check box. • To display the hop hostnames along the path, clear the check box.
Interface	From the list, select the interface on which ping requests are sent. If you select **any**, the ping requests are sent on all interfaces.
Count	From the list, select the number of ping requests to send.
Don't Fragment	• To set the don't fragment (DF) bit in the IP header of the ping request packet, select the check box. • To clear the DF bit in the IP header of the ping request packet, clear the check box.

Table 91: Ping Host Troubleshooting Options *(Continued)*

Field	Action
Record Route	• To record and display the path of the packet, select the check box. • To suppress the recording and display of the path of the packet, clear the check box.
Type-of-Service	From the list, select the decimal value of the ToS in the IP header of the ping request packet.
Routing Instance	From the list, select the routing instance name for the ping attempt.
Interval	From the list, select the interval in seconds, between the transmission of each ping request.
Packet Size	Type the size, in bytes, of the packet. The size can be from 0 through 65468. The device adds 8 bytes to the size of the ICMP header.
Source Address	Type the source IP address of the ping request packet.
Time-to-Live	From the list, select the TTL hop count for the ping request packet.
Bypass Routing	• To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box. • To route the ping requests using the routing table, clear the check box. If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.

Table 92: Ping Host Results and Output Summary

Field	Function
bytes **bytes from** ***ip-address***	• ***bytes***—Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus **8**. • ***ip-address***—IP address of destination host that sent the ping response packet.
icmp_seq=0 **icmp_seq=***number*	***time***—Sequence Number field of the ping response packet. You can use this value to match the ping response to the corresponding ping request.
ttl=*number*	***number***—TTL hop-count value of the ping response packet.
time=*time*	***time***—Total time between the sending of the ping request packet and the receiving of the ping response packet, in milliseconds. This value is also called round-trip time.
number **packets transmitted**	***number***—Number of ping requests (probes) sent to host.
number **packets received**	***number***—Number of ping responses received from host.
percentage **packet loss**	***percentage***—Number of ping responses divided by the number of ping requests, specified as a percentage.
round-trip min/avg/max/ stddev = ***min-time/ avg-time/ max-time/ std-dev*** **ms**	• ***min-time***—Minimum round-trip time (see **time=***time* field in this table). • ***avg-time***—Average round-trip time. • ***max-time***—Maximum round-trip time. • ***std-dev***—Standard deviation of the round-trip times.

Table 92: Ping Host Results and Output Summary *(Continued)*

Field	Function
Output = Packet loss of 100 percent	If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply: • The host is not operational. • There are network connectivity problems between the device and the host. • The host might be configured to ignore ICMP echo requests. • The host might be configured with a firewall filter that blocks ICMP echo requests or ICMP echo responses. • The size of the ICMP echo request packet exceeds the MTU of a host along the path. • The value you selected in the TTL box was less than the number of hops in the path to the host, in which case the host might reply with an ICMP error message. For more information about ICMP, see RFC 792, *Internet Control Message Protocol*.

RELATED DOCUMENTATION

Troubleshoot Ping MPLS | 333
Troubleshoot Traceroute | 339
Troubleshoot Packet Capture | 342

Troubleshoot Ping MPLS

IN THIS SECTION

About Ping MPLS Page

You are here: **Device Administration** > **Tools** > **Ping MPLS**.

You can send variations of ICMP "echo request" packets to the specified MPLS endpoint.

To use the ping MPLS tool:

1. Click the expand icon next to the ping MPLS option you want to use.
2. Enter information specified in Table 93 on page 334 to troubleshoot the issue.
3. Click **Start**.

   The results of the ping operation are displayed in Table 94 on page 337.
4. Click **OK** to stop the ping operation before it is complete.

Table 93: Ping MPLS Troubleshooting Options

Field	Action
Ping RSVP-signaled LSP	
LSP Name	Type the name of the LSP to ping.
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J Series device interface.
Count	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Select the check box to display detailed output rather than brief ping output.
Ping LDP-signaled LSP	
FEC Prefix	Type the forwarding equivalence class (FEC) prefix and length of the LSP to ping.
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J Series device interface.
Count	From the list, select the number of ping requests to send. The default is 5 requests.

Table 93: Ping MPLS Troubleshooting Options *(Continued)*

Field	Action
Detailed Output	Select the check box to display detailed output rather than brief ping output.
Ping LSP to Layer 3 VPN prefix	
Layer 3 VPN Name	Type the name of the VPN to ping.
Count	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Select the check box to display detailed output rather than brief ping output.
VPN Prefix	Type the IP address prefix and length of the VPN to ping.
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J Series device interface.
Ping LSP for a Layer 2 VPN connection by interface	
Interface	From the list, select the J Series device interface on which ping requests are sent. If you select **any**, the ping requests are sent on all interfaces. (See the interface naming conventions in the *Junos OS Interfaces Configuration Guide for Security Devices*.)
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J series device interface.
Count	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Select the check box to display detailed output rather than brief ping output.
Ping LSP for a Layer 2 VPN connection by instance	
Layer 2VPN Name	Type the name of the Layer 2 VPN to ping.

Table 93: Ping MPLS Troubleshooting Options *(Continued)*

Field	Action
Remote Site Identifier	Type the remote site identifier of the Layer 2 VPN to ping.
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J Series device interface.
Local Site Identifier	Type the local site identifier of the Layer 2 VPN to ping.
Count	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Select the check box to display detailed output rather than brief ping output.
Ping LSP to a Layer 2 circuit remote site by interface	
Interface	From the list, select the J Series device interface on which ping requests are sent. If you select **any**, the ping requests are sent on all interfaces.
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J Series device interface.
Count	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Select the check box to display detailed output rather than brief ping output.
Ping LSP to a Layer 2 circuit remote site by VCI	
Remote Neighbor	Type the IP address of the remote neighbor (PE router) within the virtual circuit to ping.
Circuit Identifier	Type the virtual circuit identifier for the Layer 2 circuit.
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J Series device interface.

Table 93: Ping MPLS Troubleshooting Options *(Continued)*

Field	Action
Count	From the list, select the number of ping requests to send.
Detailed Output	Select the check box to display detailed output rather than brief ping output.
Ping endpoint of LSP	
VPN Prefix	Type either the LDP FEC prefix and length or the RSVP LSP endpoint address for the LSP to ping.
Source Address	Type the source IP address of the ping request packet—a valid address configured on a J Series device interface.
Count	From the list, select the number of ping requests to send.
Detailed Output	Select the check box to display detailed output rather than brief ping output.

Table 94: Ping MPLS Results and Output Summary

Field	Function
Exclamation point (!)	Echo reply was received.
Period (.)	Echo reply was not received within the timeout period.
x	Echo reply was received with an error code. Errored packets are not counted in the received packets count and are accounted for separately.
number **packets transmitted**	***number***—Number of ping requests (probes) sent to a host.
number **packets received**	***number***—Number of ping responses received from a host.

Table 94: Ping MPLS Results and Output Summary *(Continued)*

Field	Function
percentage **packet loss**	***percentage***—Number of ping responses divided by the number of ping requests, specified as a percentage.
time	For Layer 2 circuits only, the number of milliseconds required for the ping packet to reach the destination. This value is approximate, because the packet has to reach the Routing Engine.
Output = Packet loss of 100 percent	If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply: • The host is not operational. • There are network connectivity problems between the device and the host. • The host might be configured to ignore echo requests. • The host might be configured with a firewall filter that blocks echo requests or echo responses. • The size of the echo request packet exceeds the MTU of a host along the path. • The outbound node at the remote endpoint is not configured to handle MPLS packets. • The remote endpoint's loopback address is not configured to **127.0.0.1**.

RELATED DOCUMENTATION

Troubleshoot Traceroute | 339

Troubleshoot Packet Capture | 342

Troubleshoot Traceroute

IN THIS SECTION

About Traceroute Page

You are here: **Device Administration** > **Tools** > **Traceroute**.

The traceroute diagnostic tool uses a series of packets crafted to elicit an ICMP "time exceeded" messages from intermediate points in the network between your device and the specified host.

The time-to-live for a packet is decremented each time the packet is routed, so traceroute generally receives at least one "time exceeded" response from each waypoint. Traceroute starts with a packet with a time-to-live value of one, and increments the time to live for subsequent packets, thereby constructing a rudimentary map of the path between hosts.

Use this page to display a list of routers between the device and a specified destination host.

To use the traceroute tool:

1. Click the expand icon next to Advanced options.
2. Enter information in the Traceroute page as described in Table 95 on page 340.

   The Remote Host field is the only required field.
3. Click **Start**.

   The results of the traceroute operation are displayed in Table 96 on page 341. If no options are specified, each line of the traceroute display is in the following format:

   ```
   hop-number host (ip-address) [as-number]time1 time2 time3
   ```

   The device sends a total of three traceroute packets to each router along the path and displays the round-trip time for each traceroute operation. If the device times out before receiving a Time Exceeded message, an asterisk (*) is displayed for that round-trip time.
4. Click **OK** to stop the traceroute operation before it is complete.

Table 95: Ping Traceroute Troubleshooting Options

Field	Action
Remote Host	Type the hostname or IP address of the destination host of the traceroute.
Advanced Options	
Don't Resolve Addresses	• To suppress the display of the hop hostnames along the path, select the check box. • To display the hop hostnames along the path, clear the check box.
Interface	From the list, select the interface on which traceroute packets are sent. If you select **any**, the traceroute requests are sent on all interfaces.
Time-to-Live	From the list, select the time-to-live (TTL) hop count for the traceroute request packet.
Type-of-Service	From the list, select the decimal value of the type-of-service (ToS) value to include in the IP header of the traceroute request packet.
Resolve AS Numbers	• To display the autonomous system (AS) number of each intermediate hop between the device and the destination host, select the check box. • To suppress the display of the AS number of each intermediate hop between the device and the destination host, clear the check box.
Routing Instance	From the list, select the routing instance name for the ping attempt.
Gateway	Type the gateway IP address to route through.
Source Address	Type the source IP address of the outgoing traceroute packets.

Table 95: Ping Traceroute Troubleshooting Options *(Continued)*

Field	Action
Bypass Routing	• To bypass the routing table and send the traceroute packets to hosts on the specified interface only, select the check box. • To route the traceroute packets by means of the routing table, clear the check box. If the routing table is not used, traceroute packets are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, traceroute responses are not sent.

Table 96: Ping Traceroute Results and Output Summary

Field	Function
Ping Traceroute Results and Output Summary	
hop-number	Number of the hop (router) along the path.
host	Hostname, if available, or IP address of the router. To suppress the display of the hostname, select the Don't Resolve Addresses check box.
ip-address	IP address of the router.
as-number	AS number of the router.
time1	Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.
time2	Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.
time3	Round-trip time between the sending of the third traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.

Table 96: Ping Traceroute Results and Output Summary *(Continued)*

Field	Function
Output = Complete path to the destination host not displayed	If the device does not display the complete path to the destination host, one of the following explanations might apply: • The host is not operational. • There are network connectivity problems between the device and the host. • The host, or a router along the path, might be configured to ignore ICMP traceroute messages. • The host, or a router along the path, might be configured with a firewall filter that blocks ICMP traceroute requests or ICMP time exceeded responses. • The value you selected in the Time Exceeded box was less than the number of hops in the path to the host. In this case, the host might reply with an ICMP error message. For more information about ICMP, see RFC 792, *Internet Control Message Protocol*.

RELATED DOCUMENTATION

Troubleshoot Packet Capture | 342

Troubleshoot Packet Capture

IN THIS SECTION

About Packet Capture Page

You are here: **Device Administration** > **Tools** > **Packet Capture**.

You can quickly capture and analyze router control traffic on a device.

The packet capture diagnostic tool allows inspection of control traffic (not transient traffic). The summary of each decoded packet is displayed as it is captured. Captured packets are written to a PCAP file which can be downloaded.

NOTE: Starting in Junos OS Release 19.3R1, J-Web supports RE3 line cards for SRX5000 line of devices.

To use J-Web packet capture:

1. Enter the information specified in Table 97 on page 343 to troubleshoot the issue.
2. Save the captured packets to a file or specify other advanced options by clicking the expand icon next to Advanced options.
3. Click **Start**.

   The captured packet headers are decoded and displayed in the Packet Capture display as specified in Table 98 on page 348.
4. Click one:

   - **Stop Capturing**—Stops capturing the packets and stays on the same page while the decoded packet headers are being displayed.
   - **OK**—Stops capturing packets and returns to the Packet Capture page.

Table 97: Packet Capture Troubleshooting Options

Field	Description
Interface	Specifies the interface on which the packets are captured. From the list, select an interface—for example, **ge-0/0/0**. If you select **default**, packets on the Ethernet management port 0 are captured.

Table 97: Packet Capture Troubleshooting Options *(Continued)*

Field	Description
Detail level	Specifies the extent of details to be displayed for the packet headers. • Brief—Displays the minimum packet header information. This is the default. • Detail—Displays packet header information in moderate detail. • Extensive—Displays the maximum packet header information. From the list, select **Detail**.
Packets	Specifies the number of packets to be captured. Values range from **1** to **1000**. Default is **10**. Packet capture stops capturing packets after this number is reached. From the list, select the number of packets to be captured —for example, **10**.
Addresses	Specifies the addresses to be matched for capturing the packets using a combination of the following parameters: • Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination, or both. • Type—Specifies if packet headers are matched for host address or network address. You can add multiple entries to refine the match criteria for addresses. Select address-matching criteria. For example: 1. From the Direction list, select **source**. 2. From the Type list, select **host**. 3. In the Address box, type **10.1.40.48**. 4. Click **Add**.

Table 97: Packet Capture Troubleshooting Options *(Continued)*

Field	Description
Protocols	Matches the protocol for which packets are captured. You can choose to capture TCP, UDP, or ICMP packets or a combination of TCP, UDP, and ICMP packets. From the list, select a protocol—for example: 1. Select a protocol from the list. 2. Click **Add**.
Ports	Matches the packet headers containing the specified source or destination TCP or UDP port number or port name. Select a direction and a port. For example: 1. From the Direction list, select **src**. 2. In the Port box, type **23**. 3. Click **Add**.
Advanced Options	
Absolute TCP Sequence	Displays the absolute TCP sequence numbers for the packet headers. • To display absolute TCP sequence numbers in the packet headers, select this check box. • To stop displaying absolute TCP sequence numbers in the packet headers, clear this check box.
Layer 2 Headers	Displays the link-layer packet headers. • To include link-layer packet headers while capturing packets, select this check box. • To exclude link-layer packet headers while capturing packets, clear this check box.

Table 97: Packet Capture Troubleshooting Options *(Continued)*

Field	Description
Non-Promiscuous	Does not place the interface in promiscuous mode so that the interface reads only packets addressed to it. In promiscuous mode, the interface reads every packet that reaches it. • To read all packets that reach the interface, select this check box. • To read only packets addressed to the interface, clear this check box.
Display Hex	Displays packet headers, except link-layer headers, in hexadecimal format. • To display the packet headers in hexadecimal format, select this check box. • To stop displaying the packet headers in hexadecimal format, clear this check box.
Display ASCII and Hex	Displays packet headers in hexadecimal and ASCII formats. • To display the packet headers in ASCII and hexadecimal formats, select this check box. • To stop displaying the packet headers in ASCII and hexadecimal formats, clear this check box.

Table 97: Packet Capture Troubleshooting Options *(Continued)*

Field	Description
Header Expression	Specifies the match condition for the packets to be captured. The match conditions you specify for Addresses, Protocols, and Ports are displayed in expression format in this field. Enter match conditions directly in this field in expression format or modify the expression composed from the match conditions you specified for Addresses, Protocols, and Ports. If you change the match conditions specified for Addresses, Protocols, and Ports again, packet capture overwrites your changes with the new match conditions.
Packet Size	Specifies the number of bytes to be displayed for each packet. If a packet header exceeds this size, the display is truncated for the packet header. The default value is 96 bytes. Type the number of bytes you want to capture for each packet header—for example, **256**.
Don't Resolve Addresses	Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed. • To prevent packet capture from resolving IP addresses to hostnames, select this check box. • To resolve IP addresses into hostnames, clear this check box.
No Timestamp	Suppresses the display of packet header timestamps. • To stop displaying timestamps in the captured packet headers, select this check box. • To display the timestamp in the captured packet headers, clear this check box.

Table 97: Packet Capture Troubleshooting Options *(Continued)*

Field	Description
Write Packet Capture File	Writes the captured packets to a file in PCAP format in **/var/tmp**. The files are named with the prefix **jweb-pcap** and the extension **.pcap**. If you select this option, the decoded packet headers are not displayed on the packet capture page. • To save the captured packet headers to a file, select this check box. • To decode and display the packet headers on the J-Web page, clear this check box.

Table 98: Packet Capture Results and Output Summary

Field	Function
timestamp	Displays the time when the packet was captured. The timestamp **00:45:40.823971** means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds. **NOTE**: The time displayed is local time.
direction	Displays the direction of the packet. Specifies whether the packet originated from the Routing Engine (**Out**) or was destined for the Routing Engine (**In**)
protocol	Displays the protocol for the packet. In the sample output, **IP** indicates the Layer 3 protocol.
source address	Displays the hostname, if available, or IP address and the port number of the packet's origin. If the Don't Resolve Addresses check box is selected, only the IP address of the source is displayed. **NOTE**: When a string is defined for the port, the packet capture output displays the string instead of the port number.

Table 98: Packet Capture Results and Output Summary *(Continued)*

Field	Function
destination address	Displays the hostname, if available, or IP address of the packet's destination with the port number. If the Don't Resolve Addresses check box is selected, only the IP address of the destination and the port are displayed. **NOTE**: When a string is defined for the port, the packet capture output displays the string instead of the port number.
protocol	Displays the protocol for the packet. In the sample output, **TCP** indicates the Layer 4 protocol.
data size	Displays the size of the packet (in bytes).

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.3R1	Starting in Junos OS Release 19.3R1, J-Web supports RE3 line cards for SRX5000 line of devices.

RELATED DOCUMENTATION

Troubleshoot Traceroute | 339

Access CLI

IN THIS SECTION

About CLI Terminal Page

IN THIS SECTION

You are here: **Device Administration** > **Tools** > **CLI Terminal**.

The Junos CLI provides a set of commands for monitoring and configuring a routing platform. Use this page to access Junos OS CLI through J-Web interface.

This topic includes the following sections:

CLI Terminal Requirements

To access the CLI through the J-Web interface, your management device requires the following features:

- **SSH access**—Secure shell (SSH) provides a secured method of logging in to the routing platform to encrypt traffic so that it is not intercepted. If SSH is not enabled on your system, the CLI terminal page displays an error and provides a link to the Set Up Quick Configuration page where you can enable SSH.
- **Java applet support**—Your Web browser must support Java applets.
- **JRE installed on the client**—Java Runtime Environment (JRE) version 1.4 or later must be installed on your system to run Java applications. Download the latest JRE version from the Java Software website **http://www.java.com/**. Installing JRE installs Java plug-ins, which once installed, load automatically and transparently to render Java applets.

  NOTE: The CLI terminal is supported on JRE version 1.4 or later only.

CLI Overview

The Junos OS CLI uses industry-standard tools and utilities to provide a set of commands for monitoring and configuring a routing platform. You type commands on a line and press Enter to execute them. The CLI provides online command Help, command completion, and Emacs-style keyboard sequences for moving around on the command line and scrolling through a buffer of recently executed commands.

The commands in the CLI are organized hierarchically, with commands that perform a similar function grouped together under the same level. For example, all commands that display information about the device system and system software are grouped under the **show** command, and all commands that display information about the routing table are grouped under the **show route** command. The hierarchical organization results in commands that have a regular syntax and provides the following features that simplify CLI use:

- Consistent command names—Commands that provide the same type of function have the same name, regardless of the portion of the software they are operating on. For example, all **show** commands display software information and statistics, and all **clear** commands erase various types of system information.
- Lists and short descriptions of available commands—Information about available commands is provided at each level of the CLI command hierarchy. If you type a question mark (?) at any level, you see a list of the available commands along with a short description of each command.
- Command completion—Command completion for command names (keywords) and command options is also available at each level of the hierarchy. In the CLI terminal, you can perform one of the following actions to complete a command:
  - Enter a partial command name followed immediately by a question mark (with no intervening space) to see a list of commands that match the partial name you typed.
  - Press the Spacebar to complete a command or option that you have partially typed. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a prompt indicates that you have entered an ambiguous command, and the possible completions are displayed.

    The Tab key option is currently not available on the CLI terminal.

The CLI has two modes:

- Operational mode—Complete set of commands to control the CLI environment, monitor and troubleshoot network connectivity, manage the device, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the device.

For more information about the Junos OS CLI, see the *Junos OS CLI User Guide*.

RELATED DOCUMENTATION

View CLI Configuration | 352

View CLI Configuration

IN THIS SECTION

About CLI Viewer Page

You are here: **Device Administration** > **Tools** > **CLI Viewer**.

You can view current configuration running on the device.

NOTE:

- The configuration statements appear in a fixed order irrespective of the order in which you configured the routing platform. The top of the configuration displays a timestamp indicating when the configuration was last changed and the current version.
- Each level in the hierarchy is indented to indicate each statement's relative position in the hierarchy. Each level is generally set off with braces, using an open brace ({) at the beginning of each hierarchy level and a closing brace (}) at the end. If the statement at a hierarchy level is empty, the braces are not displayed. Each leaf statement ends with a semicolon (;), as does the last statement in the hierarchy.
- The indented representation is used when the configuration is displayed or saved as an ASCII file. However, when you load an ASCII configuration file, the format of the file is not so strict. The braces and semicolons are required, but the indention and use of new lines are not required in ASCII configuration files.
- Uncommitted configuration changes will also be listed.

To save, commit, or cancel the current configuration:

1. Click one:
   - **OK**—Saves the configuration and returns to the CLI Viewer page.
   - **Commit Options** > **Commit**—Commits the configuration and returns to the CLI Viewer page.
   - **Cancel**—Cancels your entries and returns to the CLI Viewer page.

RELATED DOCUMENTATION

Edit CLI Configuration | 353

Edit CLI Configuration

IN THIS SECTION

About CLI Editor Page

You are here: **Device Administration** > **Tools** > **CLI Editor**.

You can configure all routing platform services that you can configure from the Junos CLI prompt.

To edit the CLI configuration:

1. Navigate to the hierarchy level you want to edit. Edit the candidate configuration using standard text editor operations—insert lines (with the Enter key), delete lines, modify, copy, and paste text.
2. Click **Commit** to load and commit the configuration. This saves the edited configuration, which replaces the existing configuration. The device checks the configuration for the correct syntax before committing it. If any errors occur when the configuration is loading or committed, they are displayed and the previous configuration is restored.
3. Click one:
   - **OK**—Saves the configuration and returns to the CLI Editor page.
   - **Commit Options>Commit**—Commits the configuration and returns to the CLI Editor page.
   - **Cancel**—Cancels your entries and returns to the CLI Editor page.

   NOTE: When you edit the ASCII configuration file, you can add comments of one or more lines. Comments must precede the statement they are associated with. If you place the comments in other places in the file, such as on the same line after a statement or on a separate line following a statement, they are removed when you click Commit. Comments

must begin and end with special characters. For more information, see the *Junos OS CLI User Guide*.

RELATED DOCUMENTATION

Point and Click CLI | 354

Point and Click CLI

IN THIS SECTION

About Point and Click CLI Page

You are here: **Device Administration** > **Tools** > **Point and Click CLI**.

You can edit configuration on a series of pages of clickable options.

1. To edit the configuration on a series of pages of clickable options that step you through the hierarchy, enter the information specified in Table 99 on page 355. Table 100 on page 355 lists key J-Web configuration editor tasks and their functions.

   NOTE: Options changes for each device. For a device, if a feature is not yet configured, you have the option to first configure the feature. If the feature is already configured, you have the option to edit or delete the feature on that particular device.

2. Click one:

   - **Refresh**—Refreshes and updates the display with any changes to the configuration made by other users.
   - **Commit**—Verifies edits and applies them to the current configuration file running on the device.
   - **Discard**—Removes edits applied to, or deletes existing statements or identifiers from, the candidate configuration.

3. Click one:

   - **OK**—Saves the configuration and returns to the main configuration page.
   - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
   - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 99: Point and Click Configuration Details

Field	Description
Configuration	Specifies that you can edit the selected configuration on a series of pages of clickable options that step you through the hierarchy. Click an option: • **Expand all**—Expands the hierarchy of all statements. • **Hide all**—Hides the hierarchy of all statements. • **(+)**—Expands an individual statement in the hierarchy. • **(–)**—Hides an individual statement in the hierarchy.

Table 100: J-Web Configuration Editor Page Details

Field	Function
Access	Specifies that you can edit or delete access and user authentication methods to the device. The options available are: • **Configure**—Configures the feature. • **Edit**—Edits the feature. • **Delete**—Deletes the feature.

Table 100: J-Web Configuration Editor Page Details *(Continued)*

Field	Function
Accounting options	Specifies that you can configure accounting options such as log data about basic system operations and services on the device. The option available is: • **Configure**—Configures the feature.
Applications	Specifies that you can edit or delete applications functions of the Junos OS and their properties on the device. The options available are: • **Edit**—Edits the feature • **Delete**—Deletes the feature.
Chassis	Specifies that you can configure alarms and other chassis properties on the device. The option available is: • **Configure**—Configures the feature. • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Class of service	Specifies that you can edit or delete the Class-of-Service feature. The options available are: • **Edit**—Edits the feature • **Delete**—Deletes the feature.
Ethernet switching options	Specifies that you can configure Ethernet switching options on the device. The option available is: • **Configure**—Configures the feature.

Table 100: J-Web Configuration Editor Page Details *(Continued)*

Field	Function
Event options	Specifies that you can configure diagnostic event policies and actions associated with each policy. The option available is: • **Configure**—Configures the feature.
Firewall	Specifies that you can configure stateless firewall filters—also known as ACLs—on the device. The option available is: • **Configure**—Configures the feature.
Forwarding options	Specifies that you can configure forwarding option protocols, including flow monitoring, accounting properties, and packet capture. The option available is: • **Configure**—Configures the feature.
Interfaces	Specifies that you can edit or delete interfaces on the device. The options available are: • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Multicast snooping options	Specifies that you can configure multicast snooping options. The option available is: • **Configure**—Configures the feature.
Poe	Specifies that you can edit or delete Power over Ethernet options on the device. The options available are: • **Edit**—Edits the feature. • **Delete**—Deletes the feature.

Table 100: J-Web Configuration Editor Page Details *(Continued)*

Field	Function
Policy options	Specifies that you can configure routing policies that control information from routing protocols that the device imports into its routing table and exports to its neighbors. The option available is: • **Configure**—Configures the feature.
Protocols	Specifies that you can edit or delete routing protocols, including Intermediate System-to-Intermediate System (IS-IS), OSPF, RIP, Routing Information Protocol Next Generation (RIPng), and BGP. The options available are: • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Routing instances	Specifies that you can configure a hierarchy to configure routing instances. The options available re: • **Configure**—Configures the feature.
Routing options	Specifies that you can edit or delete protocol-independent routing properties. The options available are: • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Schedulers	Specifies that you can determine the day and time when security policies are in effect. The option available is: • **Configure**—Configures the feature.

Table 100: J-Web Configuration Editor Page Details *(Continued)*

Field	Function
Security	Specifies that you can edit or delete the rules for the transit traffic and the actions that need to take place on the traffic as it passes through the firewall; and to monitor the traffic attempting to cross from one security zone to another. The options available are: • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Services	Specifies that you can configure real-time performance monitoring (RPM) on the device. The option available is: • **Configure**—Configures the feature. • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Smtp	Specifies that you can configure Simple Mail Transfer Protocol. The option available is: • **Configure**—Configures the feature.
Snmp	Specifies that you can configure Simple Network Management Protocol for monitoring router operation and performance. The option available is: • **Configure**—Configures the feature.

Table 100: J-Web Configuration Editor Page Details *(Continued)*

Field	Function
System	Specifies that you can edit or delete system management functions, including the device's hostname, address, and domain name; the addresses of the DNS servers; user login accounts, including user authentication and the root-level user account; time zones and NTP properties; and properties of the device's auxiliary and console ports. The options available are: • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Vlans	Specifies that you can edit or delete a virtual LAN. The options available are: • **Edit**—Edits the feature. • **Delete**—Deletes the feature.
Wlan	Specifies that you can configure a wireless local area network. The option available is: • **Configure**—Configures the feature.
Access profile	
Access profile name	Enter the access profile name.
Advanced	
Add new entry	Click **Add new entry** to add a new identifier.

RELATED DOCUMENTATION

Edit CLI Configuration | 353

CHAPTER 27

Reset Configuration

IN THIS CHAPTER

Reset Configuration and Rerun Setup Wizard

You are here: **Device Administration** > **Reset Configuration**

NOTE: This menu is only available if you have selected Standalone mode when configuring device factory default settings using the J-Web Setup Wizard.

This page allows you to reset the device configuration and rerun the J-Web Setup Wizard. For details on using the setup wizard to perform initial configuration on a device with a factory default configuration, see "Access the J-Web User Interface" on page 3.

On the **Reset Configuration** dialog page:

1. Click **Reset** to proceed.
   The **Reconfigure Setup Wizard** warning dialogue appears.
2. Click **Proceed to Launch** to reset the configuration and rerun the Setup Wizard.
   For details on using the Setup Wizard, see "The J-Web Setup Wizard" on page 8.

RELATED DOCUMENTATION

Access the J-Web User Interface | 3

6

PART

Network

CHAPTER 28

Connectivity—Interfaces

IN THIS CHAPTER

About the Interfaces Page

IN THIS SECTION

You are here: **Network** > **Connectivity** > **Interfaces**.

Use this page to view or configure the logical interfaces to switch to L2 or L3 mode. You can view the interfaces in the ways of interface type, interface state, or zone association.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a logical interface. See "Add a Logical Interface" on page 368.
- Edit a logical interface. See "Edit a Logical Interface" on page 375.
- Delete a logical interface. See "Delete Logical Interface" on page 375.

Field Descriptions

Table 101 on page 365 describes the fields to view interface configuration on the Interfaces page.

NOTE:

- J-Web supports IOC4 line cards for SRX5000 line of devices. You can also view the sub-ports details configured on any or all ports of the SRX5K-IOC4-MRATE line card.
- J-Web supports Wi–Fi Mini-PIM for SRX320, SRX340, SRX345, and SRX550M devices. The physical interface for the Wi-Fi Mini-PIM uses the name wl-*x*/0/0, where x identifies the slot on the services gateway where the Mini-PIM is installed.

  You can also configure the wl-*x*/0/0 interface when adding a zone at **Security Policies & Objects** > **Zones/Screens**.

Table 101: View Interface Configuration Details on the Interfaces Page

Field	Action

Filter	Select an option from the list to view the interfaces configuration details. The available options are:
	• Interface Type—Select an option to display the list of interfaces available on the device.
	• Interface State—Select an option to display the interfaces state of the device. The options are:
	  • Admin Up
	  • Link Up
	  • Admin Up & Link Down
	  • Admin Down
	• Zone Association—Select an option to display the list of available security zones.

Go	Displays the list of interfaces based on the interface type, interface state, or zone association that you have used to filter the interface information.
Clear	Clears the filter options that you have selected and displays all the interfaces.

Table 101: View Interface Configuration Details on the Interfaces Page *(Continued)*

Field	Action
Expand All	Expands the tree under the list of interfaces.
Global Settings	To configure global setting for the interface ports: 1. Click **Global Settings**. The Global Settings window appears. 2. Enter the following details: • MAC Table size—Enter the size of MAC address forwarding table. • MAC Limit—Enter the maximum number of MAC addresses learned per interface. The range is 1 through 65,535. • Packet Action—Select an option from the list for the action taken when MAC limit is reached. The options available are: ◦ drop ◦ drop-and-log ◦ log ◦ none ◦ shutdown
Disable	Disables the selected interface.
Enable	Enables the selected disabled interface.

Table 102 on page 367 describes the fields on the Interfaces page.

Table 102: Fields on the Interfaces Page

Field	Description
Interface	Displays the interface name. Logical interfaces configured under this interface appear in a collapsible list under the physical interface.
Admin status	Displays the administrative status of the interface. Status can be either Up or Down.
Link Status	Displays the operational status of the link. Status can be either Up or Down.
IP Address	Displays the configured IP addresses. Multiple IP addresses configured on one logical interface are displayed in a collapsible list under the logical interface.
Zone	Displays the security zone with which this interface is associated.
Logical System/Tenant	Display the statistics information for the specified logical system or tenant.
MTU	Displays the maximum transmission unit value for this physical interface.
Speed	Displays the Interface speed (10 Mbps, 100 Mbps, 1 Gbps, or Auto).
Link Mode	Displays the link mode status for this interface. Status can be Active, Passive, or None.
Auto Negotiation	Displays the auto negotiation status of the interface. Status can be either Enabled or Disabled.
Media Type	Displays the media type of the operating modes (copper or fiber) for the 2-Port 10 Gigabit Ethernet XPIM.

RELATED DOCUMENTATION

Add a Logical Interface | 368

Add a Logical Interface

You are here: **Network** > **Connectivity** > **Interfaces**.

To add a logical interface:

1. Select an interface and click the add icon (**+**) available on the upper right side of the Interfaces page.
   The Add Interface page appears.
2. Complete the configuration according to the guidelines provided in Table 103 on page 368.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   If you click OK, a new logical interface with the provided configuration is created.

Table 103 on page 368 provides guidelines on using the fields on the Add Interface page.

Table 103: Fields on the Add Interface Page

Field	Description
General	
Unit	Enter the logical unit number.
Description	Enter the description for the interface.
Vlan Id	Enter the VLAN ID
Multi Tenancy Type	Select an option from the list: • None • Logical System • Tenant
Logical System	Select a logical system from the list. **NOTE**: This option is available when you select the multitenancy type as logical system.

Table 103: Fields on the Add Interface Page *(Continued)*

Field	Description
Tenant	Select a tenant from the list. **NOTE**: This option is available when you select the multitenancy type as tenant.
Zone	Select a zone form the list.
Protocol (family)	
IPv4 Address	
IPv4 Address/DHCP configuration	Select the check box to enable this option.
Enable DHCP	Select this option to enable Dynamic Host Configuration Protocol (DHCP).
Enable address configuration	Select this option to add IPv4 address. To add IPv4 address: 1. Click **+**. 2. Enter the following details: • IPv4 Address—Enter an IPv4 address. • Web Auth—Click **Configure** and enable the options, Enable Http, Enable Https, and Redirect to Https. Then, click **OK** to save changes. • ARP—Click **Edit**. In the ARP Address page, click **+** and enter the IPv4 Address, MAC Address, and select **Publish**. Click **OK** to save the changes.
IPv6 Address	

Table 103: Fields on the Add Interface Page *(Continued)*

Field	Description
IPv6 Address/DHCP configuration	Select the check box to enable this option. **NOTE**: Not available for IRB interface
Enable DHCP	Select this option to enable DHCP.
Enable address configuration	Select this option to add IPv6 address. To add IPv6 address: 1. Click **+**. 2. Enter an IPv6 address.
Ethernet Switching	
Ethernet Switching configuration	Select the check box to enable this option. **NOTE**: Not available for IRB interface
Interface Mode	Select an option from the list: • access—Configures a logical interface to accept untagged packets. • trunk—Configures a single logical interface to accept packets tagged with any VLAN ID.
Recovery Timeout	Enter a period of time in seconds that the interface remains in a disabled state due to a port error prior to automatic recovery.
VLAN Member	Select a VLAN member from the list.
VoIP VLAN	Select a VLAN name from the list to be sent from the authenticating server to the IP phone.
Configure Vlan(s)	Select a VLAN from the **Available** column and move it to **Selected** column using the right arrow.

Table 103: Fields on the Add Interface Page *(Continued)*

Field	Description
All Vlans	Select this option to select any available VLANs.
General- ge	
Description	Enter a description for the interface.
MTU (Bytes)	Enter the MTU in bytes.
Speed	Select the speed from the list: 10 Mbps, 100 Mbps, 1 Gbps, or None.
Link Mode	Select the link mode from the list: Half Duplex, Full Duplex, and None.
Loopback	Select this option if you want the interface to loop back.
Flow Control	Select this option to enable flow control, which regulates the flow of packets from the router to the remote side of the connection.
Enable Auto Negotiation	Select this option to enable autonegotiation.
Enable Per Unit Scheduler	Select this option to enable the association of scheduler maps with logical interfaces.
Enable Vlan Tagging	Select this option to enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface.
Source MAC Filter	
Add	Click **+** and enter the MAC address to assign it to the interface.
Delete	Select a MAC address and click **X**.

Table 103: Fields on the Add Interface Page *(Continued)*

Field	Description
MAC Limit	Enter a value for MAC addresses to be associated with a VLAN. Range: 1 through 131071.
Packet Action	Select an option from the list: • drop—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses. • drop-and-log—Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry • log—Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry. • none—Forward packets with new source MAC addresses and learn the new source MAC address. • shutdown—Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.
General- It	
Unit	Enter a logical unit number.
Encapsulation	Select an option from the list: • Ethernet • Ethernet-VPLS
Peer Unit	Enter a peer unit number.

Table 103: Fields on the Add Interface Page *(Continued)*

Field	Description
Multi Tenancy Type	Select an option from the list: • None • Logical System • Tenant
Logical System	Select a logical system from the list. **NOTE**: This option is available when you select the multitenancy type as logical system.
Tenant	Select a tenant from the list. **NOTE**: This option is available when you select the multitenancy type as tenant.
IP Address	Click **Add** and enter an IP address. Select an IP address and click **Delete** to delete the selected IP address.
st0	
Tunnel Interface st0	Enter the logical unit number.
Zone	Select a zone from the list.
Description	Enter the description for the interface.
Unnumbered	Select this option to fetch interface from which an unnumbered interface borrows an IPv4 address.
Numbered	Select this option to fetch interface from which a numbered interface borrows an IPv4 or IPv6 address.
IPv4 Address	Enter an IPv4 address.

Table 103: Fields on the Add Interface Page *(Continued)*

Field	Description
IPv4 Subnet Mask	Enter a subnet mask for the IPv4 address.
IPv6 Address	Enter an IPv4 address.
IPv6 Subnet Mask	Enter a subnet mask for the IPv6 address.
Multipoint	
St Interface Configuration	Select the check box to enable this option.
Automatic	Select this option to automatically fetch next hop tunnel address.
Manual	Click **+** to add next hop tunnel address and VPN name. Select an existing next hop address and click **X** to delete it.
Routing Protocols	
Enable Routing Protocols	Select an option: • all—Select this option to enable all protocols routing on the routing device. • OSPF—Select this option to enable OSPF routing on the routing device. • BGP—Select this option to enable BGP routing on the routing device. • RIP—Select this option to enable RIP routing on the routing device.

RELATED DOCUMENTATION

Edit a Logical Interface | 375

Delete Logical Interface | 375

Edit a Logical Interface

You are here: **Network** > **Connectivity** > **Interfaces**.

To edit a logical interface:

1. Select an existing logical interface that you want to edit on the Interfaces page.
2. Click the pencil icon available on the upper right side of the page.

   The interface options appear with editable fields. For more information on the options, see "Add a Logical Interface" on page 368.
3. Click **OK**.

RELATED DOCUMENTATION

Delete Logical Interface | 375

Delete Logical Interface

You are here: **Network** > **Connectivity** > **Interfaces**.

To delete a logical interface:

1. Select a logical interface that you want to delete from the Interfaces page.
2. Click the delete icon (X) available on the upper right side of the page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

Add a Logical Interface | 368

Edit a Logical Interface | 375

CHAPTER 29

Connectivity—VLAN

IN THIS CHAPTER

About the VLAN Page

IN THIS SECTION

You are here: **Network** > **Connectivity** > **VLAN**.

Use this page to view, add, and remove VLAN configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a VLAN. See "Add a VLAN" on page 378.
- Edit a VLAN. See "Edit a VLAN" on page 380.
- Delete a VLAN. See "Delete VLAN" on page 380.

- Assign Interface. See "Assign an Interface to VLAN" on page 381.
- Show or hide columns in the VLAN table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advanced search for a VLAN. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 104 on page 377 describes the fields on the VLAN page.

Table 104: VLAN Configuration Page

Field	Function
VLAN Name	Displays the name for the VLAN.
VLAN ID/List	Displays the identifier or list for the VLAN.
Interface Assigned	Displays the interfaces assigned for the VLAN.
Description	Displays a brief description for the VLAN.

RELATED DOCUMENTATION

Add a VLAN | 378

Add a VLAN

You are here: **Network** > **Connectivity** > **VLAN**.

To add a VLAN:

1. Click the add icon (**+**) available on the upper right side of the VLAN page.
   The Add VLAN page appears.
2. Complete the configuration according to the guidelines provided in Table 105 on page 378.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 105 on page 378 provides guidelines on using the fields on the Add VLAN page.

Table 105: Fields on the Add VLAN Page

Field	Description
VLAN Details	
VLAN Name	Enter a unique name for the VLAN. **NOTE**: The VLAN text field is disabled when vlan-tagging is not enabled.
VLAN ID Type	Select a type of VLAN ID. The available options are: • Single • Range
VLAN ID	Enter a unique identification number for the VLAN from 1 through 4094. If no value is specified, the default is 1.
Description	Enter a brief description for the VLAN.
Advanced Settings (optional)	

Table 105: Fields on the Add VLAN Page *(Continued)*

Field	Description
L2 Interfaces	Enter the interfaces to be associated with the VLAN. The available options are as follows: • **Add**—Click **+** to add the MAC address and L2 interface details. • **Edit**—Click the pencil icon to edit the selected interface. • **Remove**—Select the interface or interfaces that you do not want associated with the VLAN.
Filter	
Input Filter	To apply an input firewall filter to an interface, select the firewall filter from the list.
Output Filter	To apply an output firewall filter to an interface, select the firewall filter from the list.
IPv4 Address **NOTE**: This option is available only when you select VLAN ID type as Single.	
IPv4 Address	Enter the IPv4 address of the VLAN.
Subnet	Enter the range of logical addresses within the address space that is assigned to an organization. For example, 255.255.255.0. You can also specify the address prefix.
IP Address	Enter the IP address of the VLAN. The available options are as follows: • **Add**—Click **+** to add the IP address, MAC address, and L2 interface details. • **Edit**—Click the pencil icon to edit the selected IPv4 address. • **Delete**—Select the IPv4 address or addresses that you do not want associated with the VLAN.

Table 105: Fields on the Add VLAN Page *(Continued)*

Field	Description
IPv6 Address **NOTE**: This option is available only when you select VLAN ID type as Single.	
IPv6 Address	Enter the IPv6 address of the VLAN.
Prefix	Select the destination prefix of the VLAN.

RELATED DOCUMENTATION

Edit a VLAN | **380**

Edit a VLAN

You are here: **Network** > **Connectivity** > **VLAN**.

To edit a VLAN:

1. Select an existing VLAN that you want to edit on the VLAN page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit VLAN page appears with editable fields. For more information on the options, see "Add a VLAN" on page 378.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete VLAN | **380**

Delete VLAN

You are here: **Network** > **Connectivity** > **VLAN**.

To delete a VLAN:

1. Select one or more VLANs that you want to delete on the VLAN page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Assign an Interface to VLAN | 381

Assign an Interface to VLAN

You are here: **Network** > **Connectivity** > **VLAN**.

To assign an interface to VLAN:

1. Select a VLAN.
2. Click **Assign Interface** on the right side of the VLAN page.
   The Assign Interfaces page appears.
3. Complete the configuration according to the guidelines provided in Table 106 on page 381.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 106: Fields on the Assign Interfaces Page

Field	Description
VLAN Name	Displays the name of the VLAN for which you want to assign the interface.
VLAN ID	Displays the ID of the selected VLAN.
Description	Displays the description of the selected VLAN.
Interfaces	Select the interfaces in the Available column and use the right arrow to move them to the Selected column.
VoIP Interfaces	Select the VoIP interfaces in the Available column and use the right arrow to move them to the Selected column.

RELATED DOCUMENTATION

- Add a VLAN | 378

CHAPTER 30

Connectivity—Link Aggregation

IN THIS CHAPTER

About the Link Aggregation Page

IN THIS SECTION

You are here: **Network** > **Connectivity** > **Link Aggregation**.

Use this page to view, add, and remove link aggregation configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Global Settings. See "Link Aggregation Global Settings" on page 385.
- Add Logical Interface. See "Add a Logical Interface to Link Aggregation" on page 386.

- Enable/Disable LACP link-protection. To do this, select a link aggregation and click **Enable/Disable** available at the upper right side of the Link Aggregation table.

- Add Link Aggregation. See "Add a Link Aggregation" on page 387.
- Edit Link Aggregation. See "Edit an Aggregated Interface" on page 389.
- Delete Link Aggregation. See "Delete Link Aggregation" on page 390.
- Search for text in a link aggregation table. See "Search for Text in the Link Aggregation Table" on page 390.
- Show or hide columns in the Link Aggregation table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

Field Descriptions

Table 107 on page 384 describes the fields on the Link Aggregation page.

Table 107: Fields on the Link Aggregation Page

Field	Description
Name	Displays the name of the select LAG.
Link Status	Displays whether the interface is linked (Up) or not linked (Down).
Admin Status	Displays whether the interface is up or down.
Interfaces	Displays the name of the aggregated interface.
VLAN ID	Displays the Virtual LAN identifier value for IEEE 802.1Q VLAN tags (0.4094).
IP Address	Displays the IP address associated with the interface.
VLAN Tagging Type	Displays whether the interface is enabled with VLAN-tagging, Flexible VLAN Tagging, or Flexible VLAN Tagging along with native VLAN ID.

Table 107: Fields on the Link Aggregation Page *(Continued)*

Field	Description
Enabled/Disabled	Displays whether the LACP link-protection is enabled or disabled.
Description	Provides a description of the LAG.

RELATED DOCUMENTATION

Link Aggregation Global Settings | 385

Link Aggregation Global Settings

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To add link aggregation global settings:

Complete the configuration according to the guidelines provided in Table 108 on page 385.

Table 108: Fields on the Link Aggregation Global Settings page

Field	Action
General	
Device count	Enter the device count. By default, J-Web displays the device count as the same number of created aggregated Ethernet interfaces. Range: 1 through 128.
Link Aggregation Control Protocol (LACP) **NOTE**: This option is not available for SRX5000 line of devices.	
System priority	Click the arrow button to select the priority level that you want to associate with the LAG.

Table 108: Fields on the Link Aggregation Global Settings page *(Continued)*

Field	Action
Link protection mode	Select one of the following options: • Revertive—Enable to switch to a better priority link (if one is available). • Non-revertive—Disable the ability to switch to a better priority link (if one is available) once a link is established as active and collection distribution is enabled.

RELATED DOCUMENTATION

Add a Logical Interface to Link Aggregation | 386

Add a Logical Interface to Link Aggregation

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To add an interface to link aggregation:

1. Select an aggregated interface.
2. Click **Add Logical Interface** on the right side of the Link Aggregation page.
   The Add Logical Interface page appears.
3. Complete the configuration according to the guidelines provided in Table 109 on page 386.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 109: Fields on the Add Logical Interface Page

Field	Action
General	
AE interface name	Displays aggregated interface name.
Logical interface unit	Enter the logical interface unit.

Table 109: Fields on the Add Logical Interface Page *(Continued)*

Field	Action
Description	Enter the description.
VLAN ID	Enter the VLAN ID. VLAN ID is mandatory.
IPv4 Address	
IPv4 Address	Click **+** and enter a valid IPv4 address.
Subnet Mask	Enter a valid subnet mask for IPv4 address.
IPv6 Address	
IPv6 Address	Click **+** and enter a valid IPv6 address.
Subnet Mask	Enter a valid subnet mask for IPv6 address.

RELATED DOCUMENTATION

Add a Link Aggregation | 387

Add a Link Aggregation

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To add a link aggregation:

1. Click the add icon **(+)** on the upper right side of the Link Aggregation page.
   The Create Link Aggregation page appears.
2. Complete the configuration according to the guidelines provided in Table 110 on page 388.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 110: Fields on the Create Link Aggregation Page

Field	Action
General	
Name	Enter the aggregated interface name. The name should be in ae*X* format. Where *X* is a number. **NOTE**: If an aggregated interface already exists, then the field is displayed as read-only.
Description	Enter a description for the LAG.
Interfaces	Select the interface available for aggregation and move to Selected column using right arrow. **NOTE**: Only interfaces that are configured with the same speed can be selected together for a LAG.
VLAN tagging type	Select one of the following VLAN tagging type: • None • VLAN Tagging—Receive and forward single-tag frames, dual-tag frames, or a mixture of single-tag and dual-tag frames. • Flexible VLAN Tagging—Simultaneously supports transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port. **NOTE**: When you edit from None to VLAN tagging or Flexible VLAN tagging or vice versa, all the logical interfaces of the selected interface are deleted.
Native VLAN ID	VLAN identifier to associate with untagged packets received on the physical interface. Range: 0 through 4094.
Link Aggregation Control Protocol (LACP)	

Table 110: Fields on the Create Link Aggregation Page *(Continued)*

Field	Action
LACP mode	Select a mode in which Link Aggregation Control Protocol packets are exchanged between the interfaces. The modes are: • **Active**—Indicates that the interface initiates transmission of LACP packets • **Passive**—Indicates that the interface only responds to LACP packets.
Periodic	Select a periodic transmissions of link aggregation control PDUs occur at different transmission rate. The options available are: • Fast—Transmit link aggregation control PDUs every second. • Slow—Transmit link aggregation control PDUs every 30 seconds.
System priority	Click the arrow button to select the priority level that you want to associate with the LAG.
Link protection	Enable or disable the option to protect the link. **NOTE**: You can configure only two member links for an aggregated Ethernet interface, that is, one active and one standby.
Link protection mode	Select one of the following options: • Revertive—Enable to switch to a better priority link (if one is available). • Non-revertive—Disable the ability to switch to a better priority link (if one is available) once a link is established as active and collection distribution is enabled.

RELATED DOCUMENTATION

Edit an Aggregated Interface | 389

Edit an Aggregated Interface

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To edit an aggregated interface:

1. Select an existing aggregated interface that you want to edit on the Aggregated Interface page.
2. Click the pencil icon available on the upper right side of the page.

   The edit Aggregated Interface page appears with editable fields. For more information on the options, see "Add a Link Aggregation" on page 387.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

Delete Link Aggregation | 390

Delete Link Aggregation

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To delete link aggregation:

1. Select one or more aggregated interfaces that you want to delete on the Link Aggregation page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Link Aggregation Page | 383

Search for Text in the Link Aggregation Table

You are here: **Network** > **Connectivity** > **Link Aggregation**.

You can use the search icon in the top right corner of the Link Aggregation page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.

   The search results are displayed.

2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

About the Link Aggregation Page | 383

CHAPTER 31

Connectivity—Wireless LAN

IN THIS CHAPTER

About the Settings Page

IN THIS SECTION

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

Use this page to configure wireless LAN settings.

NOTE: Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices. You can configure the SRX380 device supported wireless LAN settings.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an access point. See "Create an Access Point" on page 394.
- Edit an access point. See "Edit an Access Point" on page 395.
- Delete an access point. See "Delete Access Point" on page 396.
- Create access point radio settings. See "Create an Access Point Radio Setting" on page 396.
- Edit access point radio settings. See "Edit an Access Point Radio Setting" on page 400.
- Delete access point radio settings. See "Delete Access Point Radio Settings" on page 400.

Field Descriptions

Table 111 on page 393 describes the fields on the Settings page.

Table 111: Fields on the Settings Page

Field	Description
Access Point Name	Displays the access point name.
Description	Displays the description for the access point.
WL Interface	Displays the wireless LAN interface name.
Location	Displays the location of the access point.
MAC Address	Displays the MAC address.
Country	Displays the country of the access point.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
20.1R1	Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices. You can configure the SRX380 device supported wireless LAN settings.

RELATED DOCUMENTATION

Create an Access Point | 394

Create an Access Point

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To create an access point:

1. Click the add icon (**+**) on the upper right side of the Settings page.
   The Create Access Point Configuration page appears.
2. Complete the configuration according to the guidelines provided in Table 112 on page 394.
3. Click **OK** to save the changes.
   An access point is created.

   If you want to discard your changes, click **Cancel**.

Table 112: : Fields on the Create Access Point Configuration Page

Field	Action
Basic Settings	
Name	Enter a unique name for the access point.
Description	Enter the description for the access point.
Interface	Select a wireless LAN interface from the list.

Table 112: : Fields on the Create Access Point Configuration Page *(Continued)*

Field	Action
Location	Enter the location of the access point.
MAC Address	Enter the MAC address.
Access Point Options	
Country	Select a country of the access point from the list.

RELATED DOCUMENTATION

- About the Settings Page | 392
- Edit an Access Point | 395
- Delete Access Point | 396
- Create an Access Point Radio Setting | 396

Edit an Access Point

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To edit an access point:

1. Select an existing access point that you want to edit on the Settings page.
2. Click the pencil icon on the upper right side of the page.

   The Edit Access Point Configuration page appears with editable fields. For more information on the options, see "Create an Access Point" on page 394.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Settings Page | 392
- Delete Access Point | 396

Delete Access Point

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To delete an access point:

1. Select an existing access point that you want to delete on the Settings page.
2. Click the delete icon on the upper right side of the page.
3. Click **Yes** to delete the access point or click **No** to retain the access point.

RELATED DOCUMENTATION

About the Settings Page | 392

Create an Access Point | 394

Edit an Access Point | 395

Create an Access Point Radio Setting

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To create an access point radio setting:

1. Click the add icon (**+**) on the upper right side of the Radio Settings table.

   The Create Access Point Radio Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 113 on page 396.
3. Click **OK** to save the changes.

   The access point radio settings are created.

   If you want to discard your changes, click **Cancel**.

Table 113: Fields on the Create Access Point Radio Settings Page

Field	Action
Radio	
Radio Type	Select a radio type from the list.

Table 113: Fields on the Create Access Point Radio Settings Page *(Continued)*

Field	Action
Radio State	Select the radio state to enable.

Table 113: Fields on the Create Access Point Radio Settings Page *(Continued)*

Field	Action

Virtual Access Points	To add a virtual access point:
	1. Click **Add**.
	The Create VAP Configuration page appears.
	2. Enter the following details:
	Basic Settings:
	• VAP ID—Enter a value using up or down arrows.
	• Description—Enter a description for the virtual access points.
	• SSID—Enter a unique name to broadcast from access points.
	• VLAN ID—Enter a VLAN identifier (VID) using up or down arrows.
	• Download Limit (Kbps)—Enter a value using up or down arrows.
	• Upload Limit (Kbps)—Enter a value using up or down arrows.
	• Broadcast SSID—Select **No** to disable.
	• Maximum Stations—Enter a value using up or down arrows.
	• Station Isolation—Select the check box to enable.
	Security:
	• Security—Select an option from the list.
	• If you have selected WPA Personal, enter the following details:
	  • WPA Version—Select an option from the list.
	  • Cipher Suites—Select an option from the list.
	  • WPA Shared Key—Enter a value for the key.
	  • Key Type—Select an option from the list.
	• If you have selected WPA Enterprise, enter the following details:

Table 113: Fields on the Create Access Point Radio Settings Page *(Continued)*

Field	Action
	• WPA Version—Select an option from the list. • Cipher Suites—Select an option from the list. • Radius Server IP—Enter IP address for the radio server. • Radius Port—Enter a value using up or down arrows. • Radius Key—Enter a value for the key. *Station MAC Filter*: • Allowed List MAC Address—Enter a MAC address that you want to allow and click **Add** to add the address in the MAC addresses list. Select the MAC address click **Delete** to remove it. • Deny List MAC Address—Enter a MAC address that you want to block and click **Add** to add the address in the MAC addresses list. Select the MAC address click **Delete** to remove it. 3. Click **OK** to save VAP configuration. Select the virtual access point and click **Edit** or **Delete** icons to edit or remove it.
Radio Settings—Radio Options	
Mode	Select a radio mode option from the list.
Channel Number	Select a channel number for radio from the list.
Channel Bandwidth	Select a channel bandwidth for radio from the list.
Transmit Power	Enter a value for radio transmit power using up or down arrows.

RELATED DOCUMENTATION

About the Settings Page | 392
Edit an Access Point Radio Setting | 400
Delete Access Point Radio Settings | 400

Edit an Access Point Radio Setting

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To edit an access point radio settings:

1. Select an existing access point radio setting that you want to edit on the Settings page.
2. Click the edit icon on the upper right side of the Radio Settings table.

   The Edit Access Point Radio Settings page appears with editable fields. For more information on the options, see "Create an Access Point Radio Setting" on page 396.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Settings Page | 392
Delete Access Point Radio Settings | 400

Delete Access Point Radio Settings

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To delete an access point radio setting:

1. Select an existing access point radio setting that you want to delete on the Settings page.
2. Click the delete icon available on the upper right side of the Radio Settings table.
3. Click **Yes** to delete the access point radio settings or click **No** to retain the access point radio settings.

RELATED DOCUMENTATION

About the Settings Page | 392

CHAPTER 32

DHCP Client

IN THIS CHAPTER

About the DHCP Client Page

IN THIS SECTION

You are here: **Network** > **DHCP** > **DHCP Client**.

Use this page to view, add, and remove link aggregation configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create DHCP client information. See "Add DHCP Client Information" on page 403.
- Delete DHCP client information. See "Delete DHCP Client Information" on page 405.

Field Descriptions

Table 114 on page 403 describes the fields on the DHCP Client page.

Table 114: Fields on the DHCP Client Page

Field	Description
Interface Name	Displays the interface name.
DHCP Client Identifier	Displays the name of the client used by the DHCP server to index its database of address bindings.
Server	Displays the DHCP server address.
Lease Time	Displays the time in seconds, to negotiate and exchange DHCP messages.
Add	Adds a new DHCP client configuration.
Delete	Deletes the selected DHCP client configuration.

RELATED DOCUMENTATION

Add DHCP Client Information | 403

Add DHCP Client Information

You are here: **Network** > **DHCP** > **DHCP Client**.

To add DHCP Client information:

1. Click **Add** on the DHCP Client page.
   The DHCP Client Information page appears.
2. Complete the configuration according to the guidelines provided in Table 115 on page 404.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 115: Fields on the DHCP Client Information Page

Field	Action
DHCP Client Information	
Interface	Enter the name of the interface on which to configure the DHCP client.
Client Identifier	Specifies the name of the client used by the DHCP server to index its database of address bindings. Select an option from the list: • **ASCII**— ASCII client. • **Hexadecimal**—Hexadecimal client.
Lease Time	Enter a value from 60 through 2,147,483,647. Specifies the time in seconds, to negotiate and exchange DHCP messages.
Retransmission Attempt	Enter a value from 0 through 6. The default value is 4. Specifies the number of attempts the router is allowed to retransmit a DHCP packet fallback.
DHCP Server Address	Enter the IPv4 address of the DHCP server. Specifies the preferred DHCP server that the DHCP clients contact with DHCP queries.
Vendor Class ID	Enter the vendor class ID numbers. Specifies the vendor class identity number for the DHCP client.
Update Server	Select the check box to enable the propagation of TCP/IP settings on the specified interface (if it is acting as a DHCP client) to the DHCP server that is configured on the router.

RELATED DOCUMENTATION

Delete DHCP Client Information | 405

Delete DHCP Client Information

You are here: **Network** > **DHCP** > **DHCP Client**.

To delete a DHCP Client Information:

1. Select a DHCP Client that you want to delete on the DHCP Client page.
2. Click **Delete** available on the DHCP Client page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the DHCP Client Page | 402

Add DHCP Client Information | 403

CHAPTER 33

DHCP Server

IN THIS CHAPTER

About the DHCP Server Page

IN THIS SECTION

You are here: **Network** > **DHCP** > **DHCP Server**.

Use this page to view, add, and remove DHCP server configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a DHCP Pool. See "Add a DHCP Pool" on page 408.

- Edit a DHCP Pool. See "Edit a DHCP Pool" on page 412.
- Delete a DHCP Pool. See "Delete DHCP Pool" on page 413.
- Configure DHCP group global settings. See "DHCP Groups Global Settings" on page 413.
- Add a DHCP group. See "Add a DHCP Group" on page 414.
- Edit a DHCP group. See "Edit a DHCP Group" on page 414.
- Delete a DHCP group. See "Delete DHCP Group" on page 415.

Field Descriptions

Table 116 on page 407 describes the fields on the DHCP Server page.

Table 116: Fields on the DHCP Server Page

Field	Description
Routing Instance	Displays the name of the routing instance selected for DHCP server.
DHCP Pools	
Pool Name	Displays the name of the source pool.
Network Addresses	Displays the IP address in the pool.
Routing Instance	Displays the name of the routing instance selected.
DHCP Groups	
Global Settings	Specifies the global settings of DHCP server.
Group name	Specifies the source name of the group.
Interfaces	Displays name of the interfaces selected.
Routing Instance	Displays the name of the routing instance selected.

Table 116: Fields on the DHCP Server Page *(Continued)*

Field	Description
DHCP Address range for pool	
Address Range Name	Specify the name of the address assignment pool.
Address Range (Low)	Specifies the lowest address in the IP address pool range.
Address Range (High)	Specifies the highest address in the IP address pool range.
DHCP Static Bindings for pool	
Host Name	Specifies the name of the client for the static binding.
MAC Address	Specifies the client MAC address.
Fixed IP Address	Specifies the IP address to reserve for the client.

RELATED DOCUMENTATION

Add a DHCP Pool | **408**

Add a DHCP Pool

You are here: **Network** > **DHCP** > **DHCP Server**.

To add a DHCP Pool:

1. Click the add icon **(+)** on the upper right side of the DHCP Pools table.
   The Add DHCP Pool page appears.
2. Complete the configuration according to the guidelines provided in Table 117 on page 409.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 117 on page 409 describes the Add DHCP Pool Page.

Table 117: Fields on the Add DHCP Pool Page.

Field	Action
General	
Pool Name	Enter a name for DHCP pool.
Routing Instance	Select a routing instance from the list.
Network Addresses	Enter the following details: • IP Address—Enter an IP address. • Subnet Mask—Enter a subnet mask for the IP address.
DHCP Pool Attributes Click **DHCP Attributes** to add DHCP pool attributes. After configuring the attributes, click **OK** to save the changes.	
Pool Name	Displays the DHCP pool name.
Domain Name	Enter the domain name to be assigned to the address pool.
Server Identifier	Enter the name of the server identifier to assign to the DHCP client in the address pool.
Netbios Node Type	Select a NetBIOS node type from the list. This is equivalent to DHCP option 46.
Next Server	Enter the IP address of the next DHCP server that the clients need to contact.
Propagate Settings	Select an interface from the list. Specifies the name of the interface on the router through which the resolved DHCP queries are propagated to the DHCP pool.
TFTP Server	Enter the IP address of the TFTP server.

Table 117: Fields on the Add DHCP Pool Page. ***(Continued)***

Field	Action
Maximum Lease Time (Secs)	Enter a from value 60 through 1,209,600. Specifies the maximum length of time in seconds, a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)
Boot File	Enter the path and filename of the initial boot file to be used by the client.
Boot Server	Enter the IP address or hostname of the TFTP server that provides the initial boot file to the client.
Grace Period (Secs)	Enter a number of seconds the lease is retained. range is 0 through 4,294,967,295. By default, 0 is no grace period.
DNS Name Servers	Specifies the DNS name to assign to the DHCP client in the address pool. Click any one of the following: • **+**—Adds the DNS name in the address pool. • Click the pencil icon to edit a selected DNS name in the address pool. • **X**—Deletes the DNS name in the address pool.
WINS Servers	Specifies the WINS servers to assign to the DHCP client in the address pool. Click any one of the following: • **+**—Adds WINS servers to the address pool. • Click the pencil icon to edit a selected WINS server in the address pool. • **X**—Deletes the WINS servers in the address pool.

Table 117: Fields on the Add DHCP Pool Page. ***(Continued)***

Field	Action
Gateway Routers	Specifies the gateway router to assign client in the address pool. Click any one of the following: • **+**—Adds the gateway router to the address pool. • Click the pencil icon to edit a selected gateway router in the address pool. • **X**—Deletes the gateway router in the address pool.
Options	Click **+** to add DHCP option. Enter the following details: • Code—Type a number. • Type—Select a type from the list that corresponds to the code. • Value—Type a valid option value based on the type. You can select the DHCP option and click the pencil icon to edit or click **X** to delete the DHCP options.
Option-82	Device inserts DHCP option 82 (also known as the DHCP relay agent information option) information. Enter the following details: • Circuit Identifier—Enter circuit ID to identify the circuit (interface or VLAN) on the switching device on which the request was received. • Ranges—Enter a value for the circuit ID. • Remote Identifier—Enter remote ID to identify the remote host. • Ranges—Enter a value for the remote ID.
Address Range Click **+** to add address range. After configuring the attributes, click **OK** to save the changes. Selected an address range and click the pencil icon to edit it or click **X** to delete it.	

Table 117: Fields on the Add DHCP Pool Page. ***(Continued)***

Field	Action
Name	Enter the address range name.
Low	Enter an IP address that is part of the subnet specified in Address Pool subnet.
High	Enter an IP address that is part of the subnet specified in Address Pool Subnet. This address must be greater than the address specified in Address Range Low.
Static Bindings Click **+** to add DHCP static bindings. After configuring the attributes, click **OK** to save the changes. Selected a DHCP static binding and click the pencil icon to edit it or click **X** to delete it.	
Host Name	Enter the hostname to assign the DHCP client to the MAC address.
Mac Address	Enter the MAC address of the DHCP client.
Fixed IP Address	Enter the fixed address to assign the DHCP client to the MAC address.

RELATED DOCUMENTATION

Edit a DHCP Pool | 412

Edit a DHCP Pool

You are here: **Network** > **DHCP** > **DHCP Server**.

To edit a DHCP Pool:

1. Select an existing DHCP Pool that you want to edit on the DHCP Server page.
2. Click the pencil icon available on the upper right side of the DHCP Pools table.

   The Edit DHCP Pool page appears. You can edit the network addresses. For more information on the options, see "Add a DHCP Pool" on page 408.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete DHCP Pool | 413

Delete DHCP Pool

You are here: **Network** > **DHCP** > **DHCP Server**.

To delete a DHCP Pool:

1. Select a DHCP Pool that you want to delete on the DHCP Server page.
2. Click the delete icon available on the upper right side of the DHCP Pools table.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

DHCP Groups Global Settings | 413

DHCP Groups Global Settings

You are here: **Network** > **DHCP** > **DHCP Server**.

To configure DHCP groups global settings:

1. Click **Global Settings** available on the upper right side of the DHCP Groups table.

   The DHCP Global Configuration page appears.
2. Select the options available in the Available column and move them to Selected column using the arrow to configure the order of the DHCP pool match.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

Add a DHCP Group | 414

Edit a DHCP Group | 414

Delete DHCP Group | 415

Add a DHCP Group

You are here: **Network** > **DHCP** > **DHCP Server**.

To add a DHCP Group:

1. Click the add icon **(+)** on the upper right side of the DHCP Groups table.
   The Add DHCP Group page appears.
2. Complete the configuration according to the guidelines provided in Table 118 on page 414.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 118 on page 414 describes the fields on the Add DHCP Group.

Table 118: Fields on the Add DHCP Group Page

Field	Action
Group Name	Enter a name for the DHCP group.
Routing Instance	Select a routing instance from the list.
Interfaces	Select the interfaces available in the Available column and move them to Selected column using the right arrow.

RELATED DOCUMENTATION

Edit a DHCP Group | 414
Delete DHCP Group | 415
DHCP Groups Global Settings | 413

Edit a DHCP Group

You are here: **Network** > **DHCP** > **DHCP Server**.

To edit a DHCP group:

1. Select an existing DHCP group that you want to edit on the DHCP Server page.
2. Click the pencil icon available on the upper right side of the DHCP Groups table.

   The Edit DHCP Group page appears with editable fields. For more information on the options, see "Add a DHCP Group" on page 414.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

DHCP Groups Global Settings | 413

Add a DHCP Group | 414

Delete DHCP Group | 415

Delete DHCP Group

You are here: **Network** > **DHCP** > **DHCP Server**.

To delete a DHCP group:

1. Select a DHCP group that you want to delete on the DHCP Server page.
2. Click the delete icon available on the upper right side of the DHCP Groups table.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

DHCP Groups Global Settings | 413

Add a DHCP Group | 414

Edit a DHCP Group | 414

CHAPTER 34

Firewall Filters—IPv4

IN THIS CHAPTER

About the IPv4 Page

IN THIS SECTION

You are here: **Network** > **Firewall Filters** > **IPV4**.

Use this page to configure IPv4 firewall filters.

Tasks You Can Perform

You can perform the following task from this page:

- Add an IPv4 firewall filter. See "Add IPv4 Firewall Filters" on page 417.

Field Descriptions

Table 119 on page 417 describes the fields on the IPv4 page.

Table 119: Fields on the IPv4 Page

Field	Description
IPv4 Filter Summary	
Filter Name	Displays the name of the filter and when expanded, lists the terms attached to the filter.
Add New IPv4 Filter	
Filter Name	Searches for existing filters by filter name.
Term Name	Searches for existing terms by term name.
Location	Specifies the position of the new filter.

RELATED DOCUMENTATION

Add IPv4 Firewall Filters | 417

Add IPv4 Firewall Filters

You are here: **Network** > **Firewall Filters** > **IPV4**.

To add an IPV4 firewall filter:

1. Complete the configuration according to the guidelines provided in Table 120 on page 418 and Table 121 on page 420.
2. Click **Add** available in the Add New IPv4 Filter section.

   A new IPv4 Firewall Filter is created.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 120: Fields on the Add IPv4 Firewall Filter Page

Field	Action
IPv4 Filter Summary	
Action column	Select an option. The options available are: • **To move an item upward**—Locate the item and click the up arrow from the same row. • **To move an item downward**—Locate the item and click the down arrow from the same row. • **To delete an item**—Locate the item and click the **X** from the same row.
Filter Name	Displays the name of the filter and when expanded, lists the terms attached to the filter. Displays the match conditions and actions that are set for each term. Allows you to add more terms to a filter or modify filter terms. The options available are: • **To display the terms added to a filter**—Click the plus sign next to the filter name. This also displays the match conditions and actions set for the term. • **To edit a filter**—Click the filter name. To edit a term, click the name of the term.
Search	
IPv4 Filter Name	Enter the existing filter name. The options available are: • **To find a specific filter**—Enter the name of the filter in the Filter Name box. • **To list all filters with a common prefix or suffix**—Use the wildcard character (*) when you enter the name of the filter. For example, **te*** lists all filters with a name starting with the characters **te**.

Table 120: Fields on the Add IPv4 Firewall Filter Page *(Continued)*

Field	Action
IPv4 Term Name	Enter the existing terms by term name. The options available are: • **To find a specific term**—Enter the name of the term in the Term Name box. • **To list all terms with a common prefix or suffix**—Use the wildcard character (*) when typing the name of the term. For example, **ra*** lists all terms with a name starting with the characters **ra** .
Number of Items to Display	Enter the number of filters or terms to display on one page. Select the number of items to be displayed on one page.
Add New IPv4 Filter	
Filter Name	Enter the existing filter name. The options available are: • **To find a specific filter**—Enter the name of the filter in the Filter Name box. • **To list all filters with a common prefix or suffix**—Use the wildcard character (*) when you enter the name of the filter. For example, **te*** lists all filters with a name starting with the characters **te**.
Term Name	Enter the existing terms by term name. The options available are: • **To find a specific term**—Enter the name of the term in the Term Name box. • **To list all terms with a common prefix or suffix**—Use the wildcard character (*) when typing the name of the term. For example, **ra*** lists all terms with a name starting with the characters **ra** .

Table 120: Fields on the Add IPv4 Firewall Filter Page *(Continued)*

Field	Action
Location	Positions the new filter in one of the following locations: • **After Final IPv4 Filter**—At the end of all filters. • **After IPv4 Filter**—After a specified filter. **Before IPv4 Filter**—Before a specified filter.
Add	Adds a new filter name. Opens the term summary page for this filter allowing you to add new terms to this filter.
Add New IPv4 Term	
Location	Positions the new term in one of the following locations: • **After Final IPv4 Filter**—At the end of all term. • **After IPv4 Filter**—After a specified term. **Before IPv4 Filter**—Before a specified term.
Add	Opens the Filter Term page allowing you to define the match conditions and the action for this term.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter

Field	Action
Match Source	

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Source Address	Enter IP source addresses to be included in, or excluded from, the match condition. Allows you to remove source IP addresses from the match condition. If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and also search for them. The options available are: • **Add**—To include the address in the match condition. • **Except**—To exclude the address from the match condition and then select Add -To include the address in the match condition. • **Delete**—To remove an IP source address from the match condition. Enter an IP source address and prefix length and select an option.
Source Prefix List	Enter source prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition. Select an option: • **Add**—To include a predefined source prefix list in the match condition, type the prefix list name. • **Except**—To exclude the prefix list from the match condition and then select Add—To include the prefix list in the match condition. • **Delete**—To remove a prefix list from the match condition.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Source Port	Enter the source port type to be included in, or excluded from, the match condition. Allows you to remove a source port type from the match condition. **NOTE**: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term. The options available are: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select Add—To include the port in the match condition. • **Delete**—To remove a port from the match condition. Select the port from the port name list; enter the port name, number, or range and then select an option.
Match Destination	
Destination Address	Enter destination addresses to be included in, or excluded from, the match condition. Allows you to remove a destination IP address from the match condition. If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and also search for them. The options available are: • **Add**—To include the address in the match condition. • **Except**—To exclude the address from the match condition and then select Add—To include the address in the match condition. • **Delete**—To remove an IP address from the match condition. Enter an IP destination address and prefix length and select an option.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Destination Prefix List	Enter destination prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition. Select an option: • **Add**—To include a predefined destination prefix list, enter the prefix list name. • **Except**—To exclude the prefix list from the match condition and then select Add—To include the prefix list in the match condition. • **Delete**—To remove a prefix list from the match condition.
Destination Port	Enter destination port types to be included in, or excluded from, the match condition. Allows you to remove a destination port type from the match condition. **NOTE**: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term. The options available are: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select Add—To include the port in the match condition. • **Delete**—To remove a port type from the match condition. Select the port from the port name list; enter the port name, number, or range; and then select an option.
Match Source or Destination	

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Address	Enter IP addresses to be included in, or excluded from, the match condition for a source or destination. Allows you to remove an IP address from the match condition. If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses and also search for them. **NOTE**: This address match condition cannot be specified in conjunction with the source address or destination address match conditions in the same term. The options available are: • **Add**—To include the address in the match condition. • **Except**—To exclude the address from the match condition and then select Add—To include the address in the match condition. • **Delete**—To remove an IP address from the match condition. Enter an IP destination address and prefix length and select an option.
Prefix List	Enter prefix lists, which you have already defined, to be included in the match condition for a source or destination. Allows you to remove a prefix list from the match condition. **NOTE**: This prefix list match condition cannot be specified in conjunction with the source prefix list or destination prefix list match conditions in the same term. Select an option: • **Add**—To include a predefined destination prefix list, type the prefix list name. • **Delete**—To remove a prefix list from the match condition.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Port	Enter a port type to be included in, or excluded from, a match condition for a source or destination. Allows you to remove a destination port type from the match condition. **NOTE**: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term. Also, this port match condition cannot be specified in conjunction with the source port or destination port match conditions in the same term. The options available are: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select Add—To include the port in the match condition. • **Delete**—To remove a port type from the match condition. Select the port from the port name list; enter the port name, number, or range; and then select an option.
Match Interface	
Interface	Enter interfaces to be included in a match condition. Allows you to remove an interface from the match condition. The options available are: • **Add**—To include an interface in a match condition. • **Delete**—To remove an interface from the match condition. Select a name from the interface name list or Enter the interface name and select an option.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Interface Set	Enter interface sets, which you have already defined, to be included in a match condition. Allows you to remove an interface set from the match condition. The options available are: • **Add**—To include the group in the match condition. • **Delete**—To remove an interface group from the match condition. Enter the interface set name and select an option.
Interface Group	Enter interface groups, which you have already defined, to be included in, or excluded from, a match condition. Allows you to remove an interface group from the match condition. The options available are: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select Add—To include the port in the match condition. • **Delete—** To remove a port type from the match condition. Enter the name of the group and select an option.
Match Packet and Network	
First Fragment	Select the check box. Matches the first fragment of a fragmented packet.
Is Fragment	Select the check box. Matches trailing fragments (all but the first fragment) of a fragmented packet.
Fragment Flags	Enter fragmentation flags to be included in the match condition. Enter a text or numeric string defining the flag.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
TCP Established	Select the check box. Matches all Transmission Control Protocol packets other than the first packet of a connection. **NOTE**: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.
TCP Initial	Select the check box. Matches the first Transmission Control Protocol packet of a connection. **NOTE**: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.
TCP Flags	Enter Transmission Control Protocol flags to be included in the match condition. **NOTE**: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.
Protocol	Enter IPv4 protocol types to be included in, or excluded from, the match condition. Allows you to remove an IPv4 protocol type from the match condition. The options available are: • **Add**—To include the protocol in the match condition. • **Except**—To exclude the protocol from the match condition and then select Add—To include the protocol in the match condition. • **Delete**—To remove an IPv4 protocol type from the match condition. Select a protocol name from the list or enter a protocol name or number and then select an option.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
ICMP Type	Select a packet type from the list or enter a packet type name or number and then select an option. **NOTE**: This protocol does not verify that ICMP is used on the port. Make sure to specify an ICMP type match condition in the same term. The options available are: • **Add**—To include the packet type in the match condition. • **Except**—To exclude the packet type from the match condition and then select. **Add**—To include the packet type in the match condition. • **Delete**—To remove an ICMP packet type from the match condition.
ICMP Code	Select a packet code from the list or enter the packet code as text or a number and select an option. **NOTE**: The ICMP code is dependent on the ICMP type. Make sure to specify an ICMP type match condition in the same term. The options available are: • **Add**—To include the packet type in the match condition. • **Except**—To exclude the packet type from the match condition and then select **Add**—To include the packet type in the match condition. • **Delete**—To remove an ICMP packet type from the match condition.
Fragment Offset	Enter a fragment offset number or range and then select an option. The options available are: • **Add**—To include the offset in the match condition. • **Except**—To exclude the offset from the match condition and then select Add—To include the offset in the match condition. • **Delete**—To remove a fragment offset value from the match condition.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Precedence	Enter IP precedence to be included in, or excluded from, the match condition. Allows you to remove an IP precedence entry from the match condition. The options available are: • **Add**—To include the precedence in the match condition. • **Except**—To exclude the precedence from the match condition and then select **Add**—To include the precedence in the match condition. • **Delete**—To remove an IP precedence from the match condition.
DSCP	Select DSCP from the list; or enter the DSCP value as a keyword, a decimal integer from 0 through 7, or a binary string; and then select an option. The options available are: • **Add**—To include the DSCP in the match condition. • **Except**—To exclude the DSCP from the match condition and then select Add—To include the DSCP in the match condition. • **Delete**—To remove a DSCP from the match condition.
TTL	Enter an IPv4 TTL value by entering a number from 1 through 255 and select an option. **NOTE**: This option is not available in SRX5600 device. The options available are: • **Add**—To include the TTL in the match condition. • **Except**—To exclude the TTL from the match condition and then select Add—To include the TTL in the match condition . • **Delete**—To remove an IPv4 TTL type from the match condition.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Packet Length	Specify a packet length, enter a value or range. Select an option. The options available are: • **Add**—To include the packet length in the match condition. • **Except**—To exclude the packet length from the match condition and then select **Add**—To include the packet length in the match condition. • **Delete**—To remove a packet length value from the match condition.
Forwarding Class	Specify a forwarding class by selecting a forwarding class from the list or entering a forwarding class, and then select an option. The options available are: • **Add**—To include the forwarding class in the match condition. • **Except**—To exclude the forwarding class from the match condition and then select **Add**—To include the forwarding class in the match condition. • **Delete**—To remove a forwarding class from the match condition.
IP Options	Enter option by selecting an IP option from the list or entering a text or numeric string identifying the option, and then select an option. The options available are: • **Add**—To include the IP option in the match condition. • **Except**—To exclude the IP option from the match condition and then select **Add**—To include the IP option in the match condition. • **Delete**—To remove an IP option from the match condition.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
IPsec ESP SPI	Enter an ESP SPI value by entering a binary, hexadecimal, or decimal SPI value or range, and then select an option. The options available are: • **Add**—To include the value in the match condition. • **Except**—To exclude the value from the match condition and then select **Add**—To include the value in the match condition. • **Delete**—To remove an ESP SPI value from the match condition.
Action	
Nothing	Select **Nothing**. Specifies that no action is performed. By default, a packet is accepted if it meets the match conditions of the term, and packets that do not match any conditions in the firewall filter are dropped.
Accept	Select **Accept**. Accepts a packet that meets the match conditions of the term.
Discard	Select **Discard**. Discards a packet that meets the match conditions of the term. Names a discard collector for packets.
Reject	Select **Reject** and then select a message type from the reason list. Rejects a packet that meets the match conditions of the term and returns a rejection message. Allows you to specify a message type that denotes the reason the packet was rejected. **NOTE**: To log and sample rejected packets, specify log and sample action modifiers in conjunction with this action.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Next Term	Select **Next Term**. Evaluates a packet with the next term in the filter if the packet meets the match conditions in this term. This action makes sure that the next term is used for evaluation even when the packet matches the conditions of a term. When this action is not specified, the filter stops evaluating the packet after it matches the conditions of a term and takes the associated action.
Routing Instance	Accepts a packet that meets the match conditions, and forwards it to the specified routing instance. Select **Routing Instance** and enter the routing instance name in the box next to **Routing Instance**.
Action Modifiers	
Forwarding Class	Classifies the packet as a specific forwarding class. Select **Forwarding Class** from the list.
Count	Counts the packets passing this term. Allows you to name a counter that is specific to this filter. This means that every time a packet transits any interface that uses this filter, it increments the specified counter. Select **Count** and enter a 24-character string containing letters, numbers, or hyphens to specify a counter name.
Virtual Channel	Enter a string identifying the virtual channel. **NOTE**: This option is not available in SRX345 of devices.
Prefix Action	Enter the prefix action. **NOTE**: This option is not available in SRX4100 and SRX345 devices.
Log	Select **Log**. Logs the packet header information in the routing engine.

Table 121: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

Field	Action
Syslog	Select **Syslog**. Records packet information in the system log.
Port Mirror	Select **Port Mirror**. Port mirrors the packet. **NOTE**: This option is not available in SRX5600 and SRX345 devices.
Loss Priority	Sets the loss priority of the packet. This is the priority of dropping a packet before it is sent, and it affects the scheduling priority of the packet. Select the range of priority from the list.

RELATED DOCUMENTATION

About the IPv4 Page | 416

CHAPTER 35

Firewall Filters—IPv6

IN THIS CHAPTER

About the IPv6 Page

IN THIS SECTION

You are here: **Network** > **Firewall Filters** > **IPV6**.

Use this page to configure IPv6 firewall filter.

Tasks You Can Perform

You can perform the following task from this page:

- Add an IPv6 Firewall Filters. See "Add IPv6 Firewall Filters" on page 435.

Field Descriptions

Table 122 on page 435 describes the fields on IPv6 page.

Table 122: Fields on the IPv6 Page

Field	Description
IPv6 Filter Summary	
Filter Name	Displays the name of the filter and when expanded, lists the terms attached to the filter.
Add New IPv6 Filter	
Filter Name	Searches for existing filters by filter name.
Term Name	Searches for existing terms by term name.
Location	Specifies the position of the new filter.

RELATED DOCUMENTATION

Add IPv6 Firewall Filters | 435

Add IPv6 Firewall Filters

You are here: **Network** > **Firewall Filters** > **IPV6**.

To add an IPV6 firewall filter:

1. Complete the configuration according to the guidelines provided in Table 123 on page 436 and Table 124 on page 439.
2. Click **Add** available in the Add New IPv6 Filter section.

   A new IPv6 Firewall Filter is created.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 123 on page 436 describes the fields on the Add IPv6 page.

Table 123: Fields on the Add IPv6 Firewall Filter Page

Field	Action
IPv6 Filter Summary	
Action column	Select an option: • **To move an item upward**—Locate the item and click the up arrow from the same row. • **To move an item downward**—Locate the item and click the down arrow from the same row. • **To delete an item**—Locate the item and click **X** from the same row.
Filter Name	Enter the name of the filter and, when expanded, lists the terms attached to the filter. Displays the match conditions and actions that are set for each term. Allows you to add more terms to a filter or to modify filter terms. The options available are: • **To display the terms added to a filter**—Click the plus sign next to the filter name. This also displays the match conditions and actions set for the term. • **To edit a filter**—Click the filter name. To edit a term, click the name of the term.
Search	

Table 123: Fields on the Add IPv6 Firewall Filter Page *(Continued)*

Field	Action
Filter Name	Searches for existing filters by filter name. The options available are: • **To find a specific filter**—Enter the name of the filter in the Filter Name box. • **To list all filters with a common prefix or suffix**—Use the wildcard character (*) when you enter the name of the filter. For example, **te*** lists all filters with a name starting with the characters **te**.
Term Name	Searches for existing terms by name. The options available are: • **To find a specific term**—Enter the name of the term in the Term Name box. • **To list all terms with a common prefix or suffix**—Use the wildcard character (*) when typing the name of the term. For example, **ra*** lists all terms with a name starting with the characters **ra**.
Number of Items to Display	Specifies the number of filters or terms to display on one page. Selects the number of items to be displayed on one page.
Add New IPv6 Filter	

Table 123: Fields on the Add IPv6 Firewall Filter Page *(Continued)*

Field	Action
Filter Name	Enter the name of the filter and when expanded, lists the terms attached to the filter. Displays the match conditions and actions that are set for each term. Allows you to add more terms to a filter or modify filter terms. Select an option: • **To display the terms added to a filter**—Click the plus sign next to the filter name. This also displays the match conditions and actions set for the term. • **To edit a filter**—Click the filter name. To edit a term, click the name of the term.
Term Name	Searches for existing terms by term name. Select an option: • **To find a specific term**—Enter the name of the term in the Term Name box. • **To list all terms with a common prefix or suffix**—Use the wildcard character (*) when typing the name of the term. For example, **ra*** lists all terms with a name starting with the characters **ra**.
Location	Positions the new filter in one of the following locations: • **After Final IPv4 Filter**—At the end of all filters. • **After IPv6 Filter**—After a specified filter. **Before IPv6 Filter**—Before a specified filter.

Table 123: Fields on the Add IPv6 Firewall Filter Page *(Continued)*

Field	Action
Add	Click **Add**. Opens the Filter Term page allowing you to define the match conditions and the action for this term.
Add New IPv6 Term	
Location	Positions the new filter in one of the following locations: • **After Final IPv4 Filter**—At the end of all filters. • **After IPv6 Filter**—After a specified filter. **Before IPv6 Filter**—Before a specified filter.
Add	Click **Add**. Opens the Filter Term page allowing you to define the match conditions and the action for this term.

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter

Field	Action
Match Source	

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Source Address	Specifies IP source addresses to be included in, or excluded from, the match condition. Allows you to remove source IP addresses from the match condition. If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and also search for them. Enter an IP source address and prefix length, and select an option: • **Add**—To include the address in the match condition. • **Except**—To exclude the address from the match condition and then select Add -To include the address in the match condition. • **Delete**—To remove an IP source address from the match condition.
Source Prefix List	Specifies source prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition. Select an option: • **Add**—To include a predefined source prefix list in the match condition, type the prefix list name. • **Delete**—To remove a prefix list from the match condition.
Source Port	Specifies the source port type to be included in, or excluded from, the match condition. Allows you to remove a source port type from the match condition. **NOTE**: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term. Select the port from the port name list; enter the port name, number, or range and then select an option: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select Add—To include the port in the match condition. • **Delete**—To remove a port from the match condition.
Match Destination	

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Destination Address	Specifies destination addresses to be included in, or excluded from, the match condition. Allows you to remove a destination IP address from the match condition. If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and also search for them. Enter an IP destination address and prefix length and select an option: • **Add**—To include the address in the match condition. • **Except**—To exclude the address from the match condition and then select Add—To include the address in the match condition. • **Delete**—To remove an IP address from the match condition.
Destination Prefix List	Specifies destination prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition. Select an option: • **Add**—To include a predefined destination prefix list, enter the prefix list name. • **Delete**—To remove a prefix list from the match condition.
Destination Port	Specifies destination port types to be included in, or excluded from, the match condition. Allows you to remove a destination port type from the match condition. **NOTE**: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term. Select the port from the port name list; enter the port name, number, or range; and then select an option: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select Add—To include the port in the match condition. • **Delete**—To remove a port type from the match condition.
Match Source or Destination	

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Address	Specifies IP addresses to be included in, or excluded from, the match condition for a source or destination. Allows you to remove an IP address from the match condition. If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses and also search for them. **NOTE**: This address match condition cannot be specified in conjunction with the source address or destination address match conditions in the same term. Enter an IP destination address and prefix length and select an option: • **Add**—To include the address in the match condition. • **Except**—To exclude the address from the match condition and then select **Add**—To include the address in the match condition. • **Delete**—To remove an IP address from the match condition.
Prefix List	Specifies prefix lists, which you have already defined, to be included in the match condition for a source or destination. Allows you to remove a prefix list from the match condition. **NOTE**: This prefix list match condition cannot be specified in conjunction with the source prefix list or destination prefix list match conditions in the same term. Select an option: • **Add**—To include a predefined destination prefix list, type the prefix list name. • **Delete**—To remove a prefix list from the match condition.

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Port	Specifies a port type to be included in, or excluded from, a match condition for a source or destination. Allows you to remove a destination port type from the match condition. **NOTE**: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term. Also, this port match condition cannot be specified in conjunction with the source port or destination port match conditions in the same term. Select the port from the port name list; enter the port name, number, or range; and then select an option: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select **Add**—To include the port in the match condition. • **Delete**—To remove a port type from the match condition.
Match Interface	
Interface	Specifies interfaces to be included in a match condition. Allows you to remove an interface from the match condition. Select a name from the interface name list or Enter the interface name and select an option: • **Add**—To include an interface in a match condition. • **Delete**—To remove an interface from the match condition.
Interface Set	Specifies interface sets, which you have already defined, to be included in a match condition. Allows you to remove an interface set from the match condition. Enter the interface set name and select an option: • **Add**—To include the group in the match condition. • **Delete**—To remove an interface group from the match condition.

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Interface Group	Specifies interface groups, which you have already defined, to be included in, or excluded from, a match condition. Allows you to remove an interface group from the match condition. Enter the name of the group and select an option: • **Add**—To include the port in the match condition. • **Except**—To exclude the port from the match condition and then select Add—To include the port in the match condition. • **Delete**—To remove a port type from the match condition.
Match Packet and Network	
TCP Established	Matches all Transmission Control Protocol packets other than the first packet of a connection. **NOTE**: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term. Select the check box.
TCP Initial	Matches the first Transmission Control Protocol packet of a connection. **NOTE**: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term. Select the check box.
TCP Flags	Specifies Transmission Control Protocol flags to be included in the match condition. **NOTE**: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term. Enter a text or numeric string defining the flag.

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Next Header	Specifies IPv6 protocol types to be included in, or excluded from, the match condition. Allows you to remove an IPv6 protocol type from the match condition. Select a protocol name from the list or enter a protocol name or number and then select an option: • **Add**—To include the protocol in the match condition. • **Except**—To exclude the protocol from the match condition and then select Add—To include the protocol in the match condition. • **Delete**—To remove an IPv6 protocol type from the match condition.
ICMP Type	Specifies ICMP packet types to be included in, or excluded from, the match condition. Allows you to remove an ICMP packet type from the match condition. **NOTE**: This protocol does not verify that ICMP is used on the port. Make sure to specify an ICMP type match condition in the same term. Select a packet type from the list or enter a packet type name or number and then select an option: • **Add**—To include the packet type in the match condition. • **Except**—To exclude the packet type from the match condition and then select. **Add**—To include the packet type in the match condition. • **Delete**—To remove an ICMP packet type from the match condition.

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
ICMP Code	Specifies the ICMP code to be included in, or excluded from, the match condition. Allows you to remove an ICMP code from the match condition. **NOTE**: The ICMP code is dependent on the ICMP type. Make sure to specify an ICMP type match condition in the same term. Select a packet code from the list or enter the packet code as text or a number and select an option: • **Add**—To include the packet type in the match condition. • **Except**—To exclude the packet type from the match condition and then select **Add**—To include the packet type in the match condition. • **Delete**—To remove an ICMP packet type from the match condition.
Traffic Class	Specifies the traffic class to be included in, or excluded from, the match condition. Allows you to remove a traffic class value from the match condition. The options available are: • **Add**—To include the traffic class in the match condition. • **Except**—To exclude the traffic class from the match condition and then select **Add**—To include the traffic class in the match condition. • **Delete**—To remove a traffic class value from the match condition.
Packet Length	Specifies the length of received packets, in bytes, to be included in, or excluded from, the match condition. Allows you to remove a packet length value from the match condition. Specify a packet length, enter a value or range. Select an option: • **Add**—To include the packet length in the match condition. • **Except**—To exclude the packet length from the match condition and then select **Add**—To include the packet length in the match condition. • **Delete**—To remove a packet length value from the match condition.

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Forwarding Class	Specifies forwarding classes to be included in, or excluded from, the match condition. Allows you to a remove forwarding class entry from the match condition. Specify a forwarding class by selecting a forwarding class from the list or entering a forwarding class, and then select an option: • **Add**—To include the forwarding class in the match condition. • **Except**—To exclude the forwarding class from the match condition and then select **Add**—To include the forwarding class in the match condition. • **Delete**—To remove a forwarding class from the match condition.
Action	
Nothing	Select **Nothing**. Specifies that no action is performed. By default, a packet is accepted if it meets the match conditions of the term, and packets that do not match any conditions in the firewall filter are dropped.
Accept	Select **Accept**. Accepts a packet that meets the match conditions of the term.
Discard	Select **Discard**. Discards a packet that meets the match conditions of the term. Names a discard collector for packets.
Reject	Select **Reject** and then select a message type from the reason list. Rejects a packet that meets the match conditions of the term and returns a rejection message. Allows you to specify a message type that denotes the reason the packet was rejected. **NOTE**: To log and sample rejected packets, specify log and sample action modifiers in conjunction with this action.

Table 124: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

Field	Action
Next Term	Select **Next Term**. Evaluates a packet with the next term in the filter if the packet meets the match conditions in this term. This action makes sure that the next term is used for evaluation even when the packet matches the conditions of a term. When this action is not specified, the filter stops evaluating the packet after it matches the conditions of a term and takes the associated action.
Routing Instance	Accepts a packet that meets the match conditions, and forwards it to the specified routing instance. Select **Routing Instance** and enter the routing instance name in the box next to **Routing Instance**.
Action Modifiers	
Forwarding Class	Classifies the packet as a specific forwarding class. Select **Forwarding Class** from the list.
Count	Counts the packets passing this term. Allows you to name a counter that is specific to this filter. This means that every time a packet transits any interface that uses this filter, it increments the specified counter. Select **Count** and enter a 24-character string containing letters, numbers, or hyphens to specify a counter name.
Log	Select **Log**. Logs the packet header information in the routing engine.
Syslog	Select **Syslog**. Records packet information in the system log.
Loss Priority	Sets the loss priority of the packet. This is the priority of dropping a packet before it is sent, and it affects the scheduling priority of the packet. Select the range of priority from the list.

RELATED DOCUMENTATION

About the IPv6 Page | 434

CHAPTER 36

Firewall Filters—Assign to Interfaces

IN THIS CHAPTER

About the Assign to Interfaces Page

IN THIS SECTION

You are here: You are here: **Network** > **Firewall Filters** > **Assign To Interfaces**.

Use this page to configure interface for firewall filters.

Field Descriptions

Table 125 on page 451 describes the fields on the Assign Interfaces page.

Table 125: Fields on the Assign Interfaces Page

Field	Description

Logical Interface Name	Displays the logical interfaces on a router. Allows you to apply IPv4 and IPv6 firewall filters to packets received on the interface and packets transmitted from the interface.
	The options available are:
	• **Input firewall filter**:
	  • IPv4 Input Filter—Enter the name of IPv4 filter applied to received packets.
	  • IPv6 Input Filter—Enter the name of IPv6 filter applied to received packets.
	• **Output firewall filter**:
	  • IPv4 Output Filter—Enter the name of IPv4 filter applied to transmitted packets.
	  • IPv6 Output Filter—Enter the name of IPv6 filter applied to transmitted packets.
	Click **OK** to save the changes.

Link State	Displays the status of the logical interface.
Input Firewall Filters	Displays the input firewall filter applied on an interface. This filter evaluates all packets received on the interface.
Output Firewall Filters	Displays the output firewall filter applied on an interface. This filter evaluates all packets transmitted from the interface.

RELATED DOCUMENTATION

Add IPv4 Firewall Filters | 417

Add IPv6 Firewall Filters | 435

CHAPTER 37

NAT Policies

IN THIS CHAPTER

About the NAT Policies Page

IN THIS SECTION

You are here: **Network** > **NAT** > **Policies**.

Network Address Translation (NAT) is a form of network masquerading where you can hide devices between the zones or interfaces. A trust zone is a segment of the network where security measures are applied. It is usually assigned to the internal LAN. An untrust zone is the Internet. NAT modifies the IP addresses of the packets moving between the trust and untrust zones.

Whenever a packet arrives at the NAT device, the device performs a translation on the packet's IP address by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This helps you hide internal IP addresses from the other networks and keep your network secure.

Use this page to configure source, destination, and static NAT.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a source NAT. See "Create a Source NAT" on page 454.
- Edit a source NAT. See "Edit a Source NAT" on page 460.
- Delete a source NAT. See "Delete Source NAT" on page 460.
- View destination NAT rules. For more information on destination NAT, see "About the Destination Page" on page 472.
- View static NAT rules. For more information on static NAT, see "About the Static Page" on page 478.

Field Descriptions

Table 126 on page 453 describes the fields on the NAT Policies Page.

Table 126: Fields on the NAT Policies Page.

Field	Description
Seq	Displays the sequence number of rules in a context. Drag and drop the policies within the same context to reorder your NAT policy among the existing policies.
Hits	Displays the number of hits the rule has encountered.
Rule Name	Displays the rule name.
NAT Type	Displays whether the NAT is source, destination, or static.
Source Ingress	Displays the source ingress type. For example: zone, interface, or routing instance.
Source Address	Displays the match source address of the NAT policy.
Source Port	Displays the match source port of the NAT policy.
Destination Egress	Displays the match destination egress type. For example: zone, interface, or routing instance.

Table 126: Fields on the NAT Policies Page. ***(Continued)***

Field	Description
Destination Address	Displays the match destination address of the NAT policy.
Destination Port	Displays the match destination port of the NAT policy.
Applications	Displays the match application for the NAT policy.
Protocol	Displays the match IP protocol for the NAT policy.
Actions	Displays the action of the NAT policy.
Description	Displays the description for the NAT policy.

Create a Source NAT

You are here: **Network** > **NAT** > **Policies**.

To create a source NAT:

1. Click **Create** > **Source NAT** on the upper right-side of the Policies page.
   The inline creation fields will appear.
2. Complete the configuration according to the guidelines provided in Table 127 on page 454.
3. Click the tick icon on the right-side of the row once done with the configuration.

Table 127: Fields on the Policies Page—Create Source NAT

Field	Description
Rule Name > Name	Enter a unique source NAT rule name.
Source Ingress	

Table 127: Fields on the Policies Page—Create Source NAT *(Continued)*

Field	Description
Select Sources	
Source ingress type	Select an option from the list for ingress traffic that originates from inside the network: • Zone • Interface • Routing Instance
Zone	Select the source zones in the **Available** column and use the right arrow to move them to the **Selected** column. **NOTE**: This option is available only if you select source ingress type as Zone.
Interface	Select the source interfaces in the **Available** column and use the right arrow to move them to the **Selected** column. **NOTE**: This option is available only if you select source ingress type as Interface.
Routing instance	Select the source routing instances in the **Available** column and use the right arrow to move them to the **Selected** column. **NOTE**: This option is available only if you select source ingress type as Routing Instance.
Addresses	Select the source addresses in the **Available** column and use the right arrow to move them to the **Selected** column. To create a new address: 1. Click **+**. The Create Address page appears. 2. Enter the following details: • **Name**—Optional. Enter a unique name for source address. • **Description**—Enter the description for source address. • **Host IP**—Enter IPv4 or IPv6 host address.

Table 127: Fields on the Policies Page—Create Source NAT *(Continued)*

Field	Description
Ports/Port range	Click **+** to enter port number or port range (for example, 1-5) with minimum and maximum values for source. Range: 0 through 65535. To edit a port number or port range, select it and click the pencil icon. To delete a port number or port range, select it and click the delete icon.
Destination Egress	
Select Destination	
Destination egress type	Select an option from the list for outgoing traffic that originates from inside of the device network: • Zone • Interface • Routing Instance
Zone	Select the destination zones in the **Available** column and use the right arrow to move them to the **Selected** column. **NOTE**: This option is available only if you select destination egress type as Zone.
Interface	Select the destination interfaces in the **Available** column and use the right arrow to move them to the **Selected** column. **NOTE**: This option is available only if you select destination egress type as Interface.
Routing instance	Select the destination routing instances in the **Available** column and use the right arrow to move them to the **Selected** column. **NOTE**: This option is available only if you select destination egress type as Routing Instance.

Table 127: Fields on the Policies Page—Create Source NAT *(Continued)*

Field	Description
Addresses	Select the destination addresses in the **Available** column and use the right arrow to move them to the **Selected** column. To create a new address: 1. Click **+**. The Create Address page appears. 2. Enter the following details: • **Name**—Optional. Enter a unique name for destination address. • **Description**—Enter the description for destination address. • **Host IP**—Enter IPv4 or IPv6 host address.
Ports/Port range	Click **+** to enter port number or port range (for example, 1-5) with minimum and maximum values for destination. Range: 0 through 65535. To edit a port number or port range, select it and click the pencil icon. To delete a port number or port range, select it and click the delete icon.
Applications	
Select Applications	
Applications	Select an application option: • Any—Any applications you want to associate with the NAT policy. • Specific—Select the applications in the **Available** column and use the right arrow to move them to the **Selected** column. • None—No applications selected to associate with the NAT policy.
Protocols	
Select Protocols	

Table 127: Fields on the Policies Page—Create Source NAT *(Continued)*

Field	Description
Protocols	Select the protocols in the **Available** column and use the right arrow to move them to the **Selected** column.
Add Protocol	Click + and enter a protocol number to associate with the NAT policy. Range is 0 through 255.
Actions	
Actions	
Translation type	Select an option: • **None**—No translation is performed for the incoming traffic. • **Interface**—Performs interface-based translations on the source traffic. • **Pool**—Performs pool-based translations on the source traffic.
Source pool	Select a source pool from the list. Click **Add New** to create a new source NAT pool. For more information on field options, see "Create a Source NAT Pool" on page 464.
Persistent	Enable this option for mapping all requests from the same internal transport address to the same reflexive transport address.

Table 127: Fields on the Policies Page—Create Source NAT *(Continued)*

Field	Description
Persistent NAT type	Select an option from the list: • **any-remote-host**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. Any external host can send a packet to the internal host by sending the packet to the reflexive transport address. • **target-host**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external hosts IP address. • **target-host-port**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external hosts IP address and port.
Inactivity timeout	Enter the amount of time that the persistent NAT binding remains in the sites memory when all the sessions of the binding entry have ended. Range is 60 through 7200 seconds.
Maximum session number	Enter the maximum number of sessions with which a persistent NAT binding can be associated. Range is 8 through 65536
Description	Enter the description for the source NAT.

RELATED DOCUMENTATION

Edit a Source NAT | 460

Delete Source NAT | 460

Edit a Source NAT

You are here: **Network** > **NAT** > **Policies**.

To edit a source NAT:

1. Double-click an existing source NAT that you want to edit on the Policies page.
2. Complete the configuration according to the guidelines provided in "Create a Source NAT" on page 454.
3. Click the tick icon on the right-side of the row once done with the configuration.

RELATED DOCUMENTATION

Delete Source NAT | 460

Delete Source NAT

You are here: **Network** > **NAT** > **Policies**.

To delete a source NAT:

1. Select one or more source NATs that you want to delete on the Policies page.
2. Click the delete icon available on the upper right-side of the page.

   A confirmation message window appears.
3. Click **Yes** to delete or click **No** to retain the source NAT.

RELATED DOCUMENTATION

Create a Source NAT | 454

Edit a Source NAT | 460

CHAPTER 38

NAT Pools

IN THIS CHAPTER

About the NAT Pools Page

IN THIS SECTION

You are here: **Network** > **NAT** > **Pools**.

A NAT pool is a set of IP addresses that you can define and use for translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Unlike static NAT, where there is a one-to-one mapping that includes destination IP address translation in one direction and source IP address translation in the reverse direction, with source NAT, you translate the original source IP address to an IP address in the address pool. With destination NAT, you translate the original destination address to an IP address in the address pool.

Use this page to configure source and destination NAT pools.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a global option. See "Global Options" on page 463.
- Create a source NAT pool. See "Create a Source NAT Pool" on page 464.
- Edit a source NAT pool. See "Edit a Source NAT Pool" on page 468.
- Delete a source NAT pool. See "Delete Source NAT Pool" on page 469.
- Add a destination NAT pool. See "Add a Destination NAT Pool" on page 469.
- Edit a destination NAT pool. See "Edit a Destination NAT Pool" on page 471.
- Delete a destination NAT pool. See "Delete Destination NAT Pool" on page 471.

Field Descriptions

Table 128 on page 462 describes the fields on the NAT Pools Page.

Table 128: Fields on the NAT Pools Page.

Field	Description
Pool Name	Displays the NAT pool name.
Pool Type	Displays whether the NAT pool is either source or destination.
Pool Address	Displays the NAT pool address.
Proxy ARP/ND	Displays the Address Resolution Protocol (ARP) proxy or Neighbor Discovery Protocol (NDP) proxy for the NAT pool.
Description	Displays the description for the NAT pool.

Global Options

You are here: **Network** > **NAT** > **Pools**.

To add global options for a NAT pool:

1. Click the **Global Options** available on the upper right side of the page.

   The Global Options page appears.
2. Complete the configuration according to the guidelines provided in Table 129 on page 463.
3. Click **OK** to save the changes.

Table 129: Fields on the Global Options Page

Field	Action
Persistent address	Enable this option to ensure that the same IP address is assigned from the source NAT pool to a specific host for multiple concurrent sessions.
Port randomization	Enable port randomization. The device performs NAT translation choosing the IP address by round robin, then chooses the port used for that IP address by randomization.
Interface port overloading	Enable this option to set the port range for NAT interface overload mapping. It also allows you to block a specific port from being used in interface overload mapping.
Overloading factor	Enter a value for the port overloading capacity for the source NAT interface. For example, if overloading factor is set to 2, and it is multiplied by a maximum port capacity of 63,486, the port overloading threshold is 126,972. If the configured setting exceeds the maximum port capacity of the interface, an error message is generated during the configuration commit.

RELATED DOCUMENTATION

About the NAT Pools Page | **461**

Create a Source NAT Pool | **464**

Add a Destination NAT Pool | **469**

Create a Source NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To add a source NAT pool:

1. Click **Create** > **Source NAT Pool** on the upper right side of the Pools page.
   The Create Source NAT Pool page appears.
2. Complete the configuration according to the guidelines provided in Table 130 on page 464.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 130 on page 464 describes the fields on the Create Source NAT Pool page.

Table 130: Fields on the Create Source NAT Pool Page

Field	Description
Name	Enter a unique string of alphanumeric characters, hyphens and underscores; maximum length 63-character.
Description	Enter a description for the source NAT pool.
Basic	
Routing instance	Select a routing instance from the list.

Table 130: Fields on the Create Source NAT Pool Page *(Continued)*

Field	Description
Pool addresses	Select the source NAT pool addresses in the Available column and the use the right arrow to move them to the Selected column. To add a new pool address: **1.** Click **+**. The Add Pool Address page appears. **2.** Enter the following details: • **Name**—Enter a name for the pool address. • **Description**—Enter a description for the pool address. • **Pool address type**—Select either IP address or address range for the pool. • **IP address**—Enter IPv4 or IPv6 address of the host. **NOTE**: This option is available only when you select IP address as pool address type. • **Start Address**—Enter the starting range of IPv4 or IPv6 address for the source NAT pool. **NOTE**: This option is available only when you select Address Range as pool address type. • **End Address**—Enter the ending range of IPv4 or IPv6 address for the source NAT pool. **NOTE**: This option is available only when you select Address Range as pool address type.
Advanced	
Port Translation	

Table 130: Fields on the Create Source NAT Pool Page *(Continued)*

Field	Description
Port translation	Select a port translation option from the list: • **No Translation** • **Translation with port range**—Port range from low to high. Range is 1024 through 65535. • **Translation with port overloading factor**—Port overloading capacity for the source NAT interface.
Shared Address	Enable this option to map many-to-one external IP addresses. This increases NAT resources and improves traffic. **NOTE**: This option is available only when you select No Translation.
Host address base	Enter IPv4 or IPv6 address used as the host address base. For example, if the host address base is 198.51.100.30 and the NAT pool uses the range 203.0.113.10 to 203.0.113.20, then 198.51.100.30 translates to 203.0.113.10, 198.51.100.31 translates to 203.0.113.11, and so on.
Port range from	Enter the lower limit of the port range. Range: 1024 through 65535. **NOTE**: This option is available only when you select Translation with port range.
Port range to	Enter the upper limit of the port range. Range: 1024 through 65535. **NOTE**: This option is available only when you select Translation with port range.
Overloading factor	Enter the port overloading factor value. Range: 2 through 32. **NOTE**: This option is available only when you select Translation with port overloading factor.

Table 130: Fields on the Create Source NAT Pool Page *(Continued)*

Field	Description
Address pooling	Specifies that multiple internal IP addresses can be mapped to the same external IP address. Use this option only when the source NAT pool is configured with no port translation.
Paired	Select this option to use in source NAT pools with port translation for applications that require all sessions associated with one internal IP address to be translated to the same external IP address for multiple sessions. **NOTE**: This option is available only when you enable Address Pooling.
Non-paired	Select this option to use in source NAT pools without port translation for assigning IP addresses using a round-robin fashion. **NOTE**: This option is available only when you enable Address Pooling.
Overflow pool type	Specify a source pool to use when the current address pool is exhausted: • **None**—No support for overflow. • **Interface**—Allow the interface to support overflow. • **Pool**—Name of the source address pool. **NOTE**: This option is available only when you select No Translation.
Overflow pool	Select a source address pool from the list.
Utilization Alarm	
Upper threshold	Enter an upper threshold percentage for pool address utilization at which an SNMP trap is triggered. Range: 50 through 100.

Table 130: Fields on the Create Source NAT Pool Page *(Continued)*

Field	Description
Lower threshold	Enter a lower threshold percentage for pool address utilization at which an SNMP trap is triggered. Range: 40 through 100. **NOTE**: This option can be set only if you configure the upper threshold value.

RELATED DOCUMENTATION

- About the NAT Pools Page | **461**
- Edit a Source NAT Pool | **468**
- Delete Source NAT Pool | **469**

Edit a Source NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To edit a source NAT pool:

1. Select an existing source NAT pool that you want to edit on the Pools page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Source NAT Pool page appears with editable fields. For more information on the options, see "Create a Source NAT Pool" on page 464.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- Delete Source NAT Pool | **469**

Delete Source NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To delete a source NAT pool:

1. Select one or more source NAT pools that you want to delete on the Pools page.
2. Click the delete icon available on the upper right side of the page.

   A confirmation message window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the NAT Pools Page | **461**
- Create a Source NAT Pool | **464**
- Edit a Source NAT Pool | **468**

Add a Destination NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To add a destination NAT pool:

1. Click **Create** > **Destination NAT Pool** on the upper right side of the Pools page.

   The Create Destination NAT Pool page appears.
2. Complete the configuration according to the guidelines provided in Table 131 on page 469.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 131 on page 469 describes the fields on the Create Destination NAT Pool page.

Table 131: Fields on the Create Destination NAT Pool Page

Field	Action
Name	Enter the destination pool name.
Description	Enter a description for the destination pool.

Table 131: Fields on the Create Destination NAT Pool Page *(Continued)*

Field	Action
Routing instance	Select a routing instance from the list.
Pool address type	Select one of the following pool address type: • **Address & Port**—Translate destination IP address or addresses and port number(s) to a specific IP address and one port number. • **Address Range**—Translate a range of destination IP addresses to another range of IP addresses. This mapping is one-to-one.
Pool address	Enter IPv4 or IPv6 address for destination pool. **NOTE**: This option is available only when you select Address & Port as pool address type.
Pool port	Enter a destination port value. Range: 0 through 65535. **NOTE**: This option is available only when you select Address & Port as pool address type.
Start address	Enter starting address (IPv4 or IPv6) of the destination address range. **NOTE**: This option is available only when you select Address Range as pool address type.
End address	Enter ending address (IPv4 or IPv6) of the destination address range. **NOTE**: This option is available only when you select Address Range as pool address type.

RELATED DOCUMENTATION

Edit a Destination NAT Pool | **471**

Delete Destination NAT Pool | **471**

About the NAT Pools Page | **461**

Create a Source NAT Pool | **464**

Edit a Destination NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To edit a destination NAT pool:

1. Select an existing destination NAT pool that you want to edit on the Pools page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Destination NAT Pool page appears with editable fields. For more information on the options, see "Add a Destination NAT Pool" on page 469.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Destination NAT Pool | **471**

About the NAT Pools Page | **461**

Delete Destination NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To delete a destination NAT pool:

1. Select one or more destination NAT pools that you want to delete on the Pools page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Add a Destination NAT Pool | **469**

Edit a Destination NAT Pool | **471**

CHAPTER 39

Destination NAT

IN THIS CHAPTER

About the Destination Page

IN THIS SECTION

You are here: **Network** > **NAT** > **Destination**.

Use this page to add, edit, or delete destination NAT configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Destination Rule Set. See "Add a Destination Rule Set" on page 474.
- Edit a Destination Rule Set. See "Edit a Destination Rule Set" on page 477.
- Delete a Destination Rule Set. See "Delete Destination Rule Set" on page 477.

Field Descriptions

Table 132 on page 473 describes the fields on the Destination Page.

Table 132: Fields on the Destination Page.

Field	Description
Destination NAT Rule Set	
From	Displays the destination NAT sort options from which the packets flow. The options available are: • Routing Instance • Zone • Interface
Filter	Displays the filter option.
Name	Displays the name of the destination NAT rule set.
From	Displays the name of the routing instance/zone/interface from which the packets flow.
Rule	Displays the name of the rule in the selected destination NAT rule set.
Description	Displays a description of the destination NAT rule set.
Rules in Selected Rule-Set	
Rule Name	Displays the name of the rule in the selected destination NAT rule set.
Match Source	Displays the match source address.
Match Destination	Displays the match destination address.
Match IP Protocol	Displays the match IP protocol.

Table 132: Fields on the Destination Page. ***(Continued)***

Field	Description
Match Destination Port	Displays the match destination port.
Action	Displays the action of the rule in the selected rule set.
Upper Threshold	Displays upper threshold at which an SNMP trap is triggered.
Lower Threshold	Displays lower threshold at which an SNMP trap is triggered.
Description	Displays a description of the rule in the selected destination NAT rule set.

RELATED DOCUMENTATION

Add a Destination Rule Set | 474

Add a Destination Rule Set

You are here: **Network** > **NAT** > **Destination**.

To add a destination Rule Set:

1. Click the add icon **(+)** on the upper right side of the Destination page.
   The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in Table 133 on page 474.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 133 on page 474 describes the fields on the Add Rule Set page.

Table 133: Fields on the Add Rule Set page.

Field	Action
Add Rule Set	

Table 133: Fields on the Add Rule Set page. ***(Continued)***

Field	Action
Rule Set Name	Enter the rule set name.
Rule Set Description	Enter a description for the rule set.
From	Specifies the filter options. Select an option: • Routing Instance • Zone • Interface Select the routing instances/zones/interfaces in the **Available** column and the use the right arrow to move them to the **Selected** column.
Add Rule	
Rule Name	Enter the rule name.
Rule Description	Enter a description for the rule.
Match	
Source Address	Search and select the source addresses in the **Available** column and the use the right arrow to move them to the **Selected** column. You can also enter a source address in the **New** text box in the **Selected** column and click **Add** to add the source address to the lower pane of the **Selected** column.
Destination Address	Enter the destination IP address.
Port	Enter the destination port number.
IP Protocol	Enter the protocol name in the text box and click **+** to add the protocol to the **IP Protocol** column.

Table 133: Fields on the Add Rule Set page. ***(Continued)***

Field	Action
Actions	Specifies the actions for the destination NAT pool. Select an option: • No Destination NAT. • Do Destination NAT With Pool.
Do Destination NAT With Pool	
Add New Pool	Select a pool from the list or click **+**.
Add Destination Pool	
Pool Name	Enter the destination pool name.
Pool Description	Enter a description for the destination pool.
Routing Instance	Specifies the routing instance available. Select an option.
Pool Addresses and Port	
Address/Port	Enter the destination pool address.
Port	Enter the destination pool port number.
Address Range	Enter the destination pool address range.
Upper Threshold	Enter upper threshold at which an SNMP trap is triggered. Session count hit alarm range: 1 through 4294967295
Lower Threshold	Enter lower threshold at which an SNMP trap is triggered. Rule session count alarm range: 1 through 4294967295

RELATED DOCUMENTATION

Edit a Destination Rule Set | 477

Edit a Destination Rule Set

You are here: **Network** > **NAT** > **Destination**.

To edit a destination rule set:

1. Select an existing destination rule set that you want to edit on the Destination page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Rule Set page appears with editable fields. For more information on the options, see "Add a Destination Rule Set" on page 474.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Destination Rule Set | 477

Delete Destination Rule Set

You are here: **Network** > **NAT** > **Destination**.

To delete destination rule set:

1. Select one or more destination rule sets that you want to delete on Destination page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Add a Destination NAT Pool | 469

CHAPTER 40

Static NAT

IN THIS CHAPTER

About the Static Page

IN THIS SECTION

You are here: **Network** > **NAT** > **Static**.

Use tis page to configure static NAT.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a static rule set and rules to it. See "Add a Static Rule Set" on page 480.
- Edit a static rule set and its rules. See "Edit a Static Rule Set" on page 484.
- Delete a static rule set and its rules. See "Delete Static Rule Set" on page 484.
- Move the rules in the rules table. To do this, select a rule which you want to move and select the following options according to your choice:

- Move Up—Enables you to move the rule up in the list.
- Move Down—Enables you to move the rule down in the list.
- Move to Top—Enables you to move the rule to top of the list
- Move to Bottom—Enables you to move the rule to the bottom of the list

Field Descriptions

Table 134 on page 479 describes the fields on the Static page.

Table 134: Fields on the Static Page

Field	Description
Static NAT Rule Set	
From	Displays the destination NAT sort options from which the packets flow. The options available are: • Routing Instance • Zone • Interface
Filter	Displays the filter options.
Name	Displays the name of the static NAT rule set.
From	Displays the name of the routing instance, zone, or interface from which the packets flow.
Rule	Displays the name of the rule in the selected static NAT rule set.
Description	Displays a description of the static NAT rule set.
Rules in Selected Rule-Set	

Table 134: Fields on the Static Page *(Continued)*

Field	Description
Rule Name	Displays the name of the routing instance, zone, or interface to which the packet flows.
Source Addresses	Displays the source address to match the rule.
Source Ports	Displays the source port number.
Destination Addresses	Displays the destination address to match the rule.
Destination Ports	Displays the destination port number.
Prefix	Displays the static IP address prefix.
Mapped Port	Displays the destination port or port range to allow static NAT to map ports.
Upper Threshold	Displays the upper threshold value of the at which an SNMP trap is triggered.
Lower Threshold	Displays the lower threshold value of the at which an SNMP trap is triggered.
Description	Displays the description of the rule in the selected static NAT rule set.

RELATED DOCUMENTATION

Add a Static Rule Set | 480
Edit a Static Rule Set | 484
Delete Static Rule Set | 484

Add a Static Rule Set

You are here: **Network** > **NAT** > **Static**.

To add a static rule set:

1. Click the add icon (**+**) on the upper right side of the Static page.

   The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in Table 135 on page 481.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 135: Fields on the Add Static Rule Set Page

Field	Action
Rule Set Name	Enter a rule set name.
Rule Set Description	Enter a description for the rule set.
From	Select a filter option from the list: • Routing Instance • Zone • Interface Select the routing instances, zones, or interfaces in the **Available** column and use the right arrow to move them to the **Selected** column.
Rules	
Rules	Specifies the rules added to the selected static rule set.

Table 135: Fields on the Add Static Rule Set Page *(Continued)*

Field	Action
Add	To add a rule to the selected static rule set: 1. Click **+** available at the upper right of the Rules table. The Add Rule page appears. 2. Enter the following details: • Rule Name—Enter a rule name. • Rule Description—Enter a description for the rule. • Match—Displays the match destination address. • Source Address—Select an IPv4 or IPv6 address from the list or enter the address and click **+** to add it. Select an existing IPv4 or IPv6 address and click **X** to delete it. • Source Port—Enter a port number or port range from low to high and click **+** to add it. Port Range: 0 through 65535. Select an existing port and click **X** to delete it. • Destination Address—Select **IPv4** or **IPv6** and then select an address from the list. • Destination Port—Select one of the following options: • Any—Selects available port. • Port—Enter a port number. • Port Range—Enter a port range from low to high. • Then—Enter the following details: • Host Address—Enter the static prefix address. **NOTE**: You can select **Translate to ipv4 address** if you have selected IPv6 in the destination address.

Table 135: Fields on the Add Static Rule Set Page *(Continued)*

Field	Action

	• Mapped Port—Select one of the following options:
	  • Any—Selects available port.
	  • Port—Enter a port number.
	  • Port Range—Enter a port range from low to high.
	• Routing Instance—Select a routing instance from the list.
	• Upper Threshold—Enter an upper threshold value at which an SNMP trap is triggered.
	  Range: 1 through 4294967295.
	• Lower Threshold—Enter a lower threshold value at which an SNMP trap is triggered.
	  Range: 1 through 4294967295.
	  NOTE: This option can be set only if you configure the upper threshold value.
	3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Edit	Select an existing rule and click the edit icon at the top right corner of the Rules table. The Edit Interface page appears with editable fields.
Delete	Select an interface and click the delete icon at the top right corner of the Rules table. A confirmation window appears. Click **Yes** to delete the selected interface or click **No** to discard.

RELATED DOCUMENTATION

About the Static Page | **478**

Edit a Static Rule Set | **484**

Delete Static Rule Set | **484**

Edit a Static Rule Set

You are here: **Network** > **NAT** > **Static**.

To edit a static rule set and its rules:

1. Select an existing static rule set that you want to edit on the Static page.
2. Click the pencil icon available on the upper right side of the Static page.

   The Edit Static Rule Set page appears with editable fields. For more information on the options, see "Add a Static Rule Set" on page 480.

   > **NOTE**: Alternatively, you can select the rule directly and click the pencil icon available on the upper right side of the Rules table to edit a rule for the selected rule set.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Static Page | **478**

Add a Static Rule Set | **480**

Delete Static Rule Set | **484**

Delete Static Rule Set

You are here: **Network** > **NAT** > **Static**.

To delete a static rule set and its rules:

1. Select one or more static rules sets that you want to delete on the Static page.
2. Click the delete icon available on the upper right side of the page.

   A confirmation window appears.

   > **NOTE**: Alternatively, you can select the rule directly and click the delete (**X**) icon available on the upper right side of the Rules table to delete a rule for the selected rule set.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Static Page | **478**
- Add a Static Rule Set | **480**
- Edit a Static Rule Set | **484**

CHAPTER 41

NAT Proxy ARP/ND

IN THIS CHAPTER

About the Proxy ARP/ND Page

IN THIS SECTION

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

You can add, edit, and delete proxy ARP or proxy ND configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a proxy ARP. See "Add a Proxy ARP" on page 487.
- Edit a proxy ARP. See "Edit a Proxy ARP" on page 489.

- Delete a proxy ARP. See "Delete a Proxy ARP" on page 489.
- Create a proxy ND. See "Add a Proxy ND" on page 490.
- Edit a proxy ND. See "Edit a Proxy ND" on page 491.
- Delete a proxy ND. See "Delete Proxy ND" on page 491.
- Launch NAT wizard. To do this, click **Launch Wizard** option at the right side of the page. The NAT wizard leads you through the basic required steps to configure NAT for the SRX Series security device.

Field Descriptions

Table 136 on page 487 describes the fields on the Proxy ARP/ND Configuration page.

Table 136: Fields on the Proxy ARP/ND Configuration Page

Field	Description
Interface	Displays the interface type.
Address	Displays the IPv4 or IPv6 address.

RELATED DOCUMENTATION

- Add a Proxy ARP | **487**
- Edit a Proxy ARP | **489**
- Delete a Proxy ARP | **489**
- Add a Proxy ND | **490**
- Edit a Proxy ND | **491**
- Delete Proxy ND | **491**

Add a Proxy ARP

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To add a proxy ARP:

1. Click the add icon (**+**) on the upper right side of the proxy ARP/ND page.

   Select the Proxy ARP page. The Add Proxy ARP page appears.
2. Complete the configuration according to the guidelines provided in Table 137 on page 488.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 137: Fields on the Add Proxy ARP Page

Field	Action
Interface	Enter the interface type. Select an option: • ge-0/0/0.0 • ge-0/0/2.0 • lo0.0 • vlan0.0
Addresses	Dislays the proxy ARP IP address. Click **Delete** to deleted the proxy ARP address.
IPv4 Address/Range	Enter the source IP address range and the end IP address that the device can be assigned to. Click **+** to add to the addresses.

RELATED DOCUMENTATION

- About the Proxy ARP/ND Page | **486**
- Edit a Proxy ARP | **489**
- Delete a Proxy ARP | **489**
- Add a Proxy ND | **490**
- Edit a Proxy ND | **491**
- Delete Proxy ND | **491**

Edit a Proxy ARP

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To edit a proxy ARP:

1. Select an existing proxy ARP that you want to edit on the Proxy ARP/ND page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Proxy ARP page appears with editable fields. For more information on the options, see "Add a Proxy ARP" on page 487.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

- About the Proxy ARP/ND Page | **486**
- Add a Proxy ARP | **487**
- Delete a Proxy ARP | **489**
- Add a Proxy ND | **490**
- Edit a Proxy ND | **491**
- Delete Proxy ND | **491**

Delete a Proxy ARP

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To delete proxy ARP:

1. Select one or more proxy ARPs that you want to delete on the Proxy ARP page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Proxy ARP/ND Page | **486**
- Add a Proxy ARP | **487**
- Edit a Proxy ARP | **489**

Add a Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To add a proxy ND:

1. Click the add icon (**+**) on the upper right side of the proxy ARP/ND page.
   The Add Proxy ND page appears.
2. Complete the configuration according to the guidelines provided in Table 138 on page 490.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 138: Fields on the Add Proxy ND Page

Field	Action
Interface	Enter the interface type. Select an option: • ge-0/0/0.0 • ge-0/0/1.0 • ge-0/0/3.0 • lo0.0
Addresses	Displays the proxy ND IP address. Click **Delete** to deleted the proxy ND address.
IPv6 Address/Range	Enter the source IPv6 address range and the end IPv6 address that the device can be assigned to. Click **+** to add to the addresses.

RELATED DOCUMENTATION

- About the Proxy ARP/ND Page | 486
- Add a Proxy ARP | 487
- Edit a Proxy ARP | 489
- Delete a Proxy ARP | 489
- Edit a Proxy ND | 491
- Delete Proxy ND | 491

Edit a Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To edit a proxy ND:

1. Select an existing proxy ND that you want to edit on the Proxy ARP/ND page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Proxy ND page appears with editable fields. For more information on the options, see "Add a Proxy ND" on page 490.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

- About the Proxy ARP/ND Page | 486
- Add a Proxy ARP | 487
- Edit a Proxy ARP | 489
- Delete a Proxy ARP | 489
- Add a Proxy ND | 490
- Delete Proxy ND | 491

Delete Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To delete a proxy ND:

1. Select one or more proxy NDs that you want to delete on the Proxy ND page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Proxy ARP/ND Page | **486**
- Add a Proxy ARP | **487**
- Edit a Proxy ARP | **489**
- Delete a Proxy ARP | **489**
- Add a Proxy ND | **490**
- Edit a Proxy ND | **491**

CHAPTER 42

Static Routing

IN THIS CHAPTER

About the Static Routing Page

IN THIS SECTION

You are here: **Network** > **Routing** > **Static Routing**.

Use this page to view, add, and remove link aggregation configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a static route. See "Add a Static Route" on page 494.
- Edit a static route. See "Edit a Static Route" on page 496.
- Delete a static route. See "Delete Static Route" on page 496.

Field Descriptions

Table 139 on page 494 describes the fields on the Static Routing page.

Table 139: Fields on the Static Routing Page

Field	Description
Route	Displays the static route selected.
Next-hop	Displays the selected next-hop address.
Routing Instance	Displays the routing instance selected for this route.

RELATED DOCUMENTATION

Add a Static Route | 494

Add a Static Route

You are here: **Network** > **Routing** > **Static Routing**.

To add a static route:

1. Click the add icon (**+**) on the upper right side of the Static Routing page.
   The Add Static Route page appears.
2. Complete the configuration according to the guidelines provided in Table 140 on page 495.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   If you click **OK**, a new static route is added with the provided configuration.

Table 140: Fields on the Add Static Route Page

Field	Description
Routing Instance	Select the routing instance from the list. The selected destination routing instance that points to the routing table containing the tunnel destination address. **NOTE**: If you log in as a tenant user, routing instance is not displayed as tenant context supports only one routing instance.
IPv4	Click the **IPv4** button.
IP address	Enter the static route IPv4 address.
Subnet mask	Enter the subnet mask. For example, 24 bits represents the 255.255.255.0 address.
IPv6	Click the **IPv6** button.
IPv6 address	Enter the static route IPv6 address.
Prefix	Enter the prefix for IPv6 address.

Next-hop	Displays the next-hop address created.
	
	Click any one of the following
	
	• **+**—To add the next-hop, enter the following details and click **OK**:
	  • IP Address/IPv6 Address—Enter the IPv4 or IPv6 address based on the selected static route address type.
	  • **Interface Name**—Select an interface from the list.
	• **Delete**—Select one or more next-hop addresses and click **X**. Then, click **Yes** to delete it.

RELATED DOCUMENTATION

Edit a Static Route | 496

Edit a Static Route

You are here: **Network** > **Routing** > **Static Routing**.

To edit a static route:

1. Select the existing static route that you want to edit on the Static Routing page.
2. Click the pencil icon available on the upper right side of the Static Routing page.

   The Edit Static Route page appears with editable fields. For more information on the options, see "Add a Static Route" on page 494.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Static Route | 496

Delete Static Route

You are here: **Network** > **Routing** > **Static Routing**.

To delete a static route:

1. Select the existing static route that you want to delete on the Static Routing page.
2. Click the delete icon available on the upper right side of the Static Routing page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the Static Routing Page | 493

CHAPTER 43

RIP Routing

IN THIS CHAPTER

About the RIP Page

IN THIS SECTION

You are here: **Network** > **Routing** > **RIP**.

Use this page to configure RIP.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a RIP instance. See "Add a RIP Instance" on page 499.
- Edit a RIP instance. See "Edit a RIP Instance" on page 501.
- Delete a RIP instance. See "Delete RIP Instance" on page 501.

- Edit RIP global settings. See "Edit RIP Global Settings" on page 501.
- Delete RIP global settings. See "Delete RIP Global Settings" on page 505.

Field Descriptions

Table 141 on page 498 describes the fields on the RIP page.

Table 141: Fields on the RIP Page

Field	Description
Routing Instance	Select a routing instance from the list.
RIP Instances	
RIP Instances	Displays the RIP instance selected.
Neighbors	Displays the neighbors selected.
Routing Instance	Displays the routing instance.
Export Policies	Displays the export policies selected.
Import Policies	Displays the import policies selected.
Preference	Displays the preference selected.
Update Interval	Displays the update interval selected.
Metric-out	Displays the metric-out value selected.
RIP Global Settings	
Name	Displays the name of the RIP.
Value	Displays the values for RIP.

RELATED DOCUMENTATION

Add a RIP Instance | 499

Add a RIP Instance

You are here: **Network** > **Routing** > **RIP**.

To add a RIP instance:

1. Click the add icon (**+**) on the upper right side of the RIP page.
   The Add page appears.
2. Complete the configuration according to the guidelines provided in Table 142 on page 499.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   If you click **OK**, a new RIP instance is added with the provided configuration.

Table 142: Fields on the Add Page

Field	Action
General	
Routing Instance	Select a routing instance from the list to display only the default routing instance or all routing instances.
RIP Instance Name	Enter the RIP instance name.
Preference	Enter the preference of the external routes learned by RIP as compared to those learned from other routing protocols.
Metric out	Enter the metric value to add to routes transmitted to the neighbor.
Update Interval	Enter the update time interval to periodically send out routes learned by RIP to neighbors.
Route Timeout	Enter the route timeout interval for RIP.
Policy	

Table 142: Fields on the Add Page *(Continued)*

Field	Action
Import Policy	Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas. Click one of the following options: • **+**—Adds an import policy. • **Move up arrow**—Moves the selected policy up the list of policies. • **Move down arrow**—Moves the selected policy down the list of policies. • **X**—Removes an import policy.
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area. Click one of the following options: • **+**—Adds an export policy. • **Move up arrow**—Moves the selected policy up the list of policies. • **Move down arrow**—Moves the selected policy down the list of policies. • **X**—Removes an export policy.
Neighbor Displays the RIP-enabled interfaces, its port, metric-in, and update interval.	
Associate	Select interface(s) to associate with the RIP. Select the box next to the interface name to enable RIP on an interface. Click the edit icon to modify one or more selected interfaces settings. **NOTE**: Only logical interfaces for RIP are displayed.

RELATED DOCUMENTATION

Edit a RIP Instance | **501**

Edit a RIP Instance

You are here: **Network** > **Routing** > **RIP**.

To edit a RIP instance:

1. Select the existing logical system profile that you want to edit on the RIP page.
2. Click the pencil icon available on the upper right side of the RIP page.

   The Edit page appears with editable fields. For more information on the options, see "Add a RIP Instance" on page 499.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete RIP Instance | **501**

Delete RIP Instance

You are here: **Network** > **Routing** > **RIP**.

To delete a RIP instance:

1. Select the existing logical system profile that you want to delete on the RIP page.
2. Click the delete icon available on the upper right side of the RIP page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

Edit RIP Global Settings | **501**

Edit RIP Global Settings

You are here: **Network** > **Routing** > **RIP**.

To edit RIP global settings:

1. Click the pencil icon on the upper right side of the RIP Global Settings table.
   The Edit RIP Global Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 143 on page 502.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 143: Fields on the Edit RIP Global Settings Page

Field	Action
General	
Send	Select a RIP send options from the list: • Broadcast • Multicast • None • Version-1
Receive	Select a RIP receive options from the list: • Both • None • Version-1 • Version-2
Route timeout (sec)	Enter the route timeout interval value for RIP.
Update interval (sec)	Enter the update time interval value to periodically send out routes learned by RIP to neighbors.
Hold timeout (sec)	Enter the hold timeout interval period for which the expired route is retained in the routing table before being removed.
Metric in	Enter the metric-in value to add to incoming routes when advertising into RIP routes that were learned from other protocols.

Table 143: Fields on the Edit RIP Global Settings Page *(Continued)*

Field	Action
RIB Group	Select a routing table group to install RIP routes into multiple routing tables.
Message size	Enter the number of route entries to be included in every RIP update message.
Check Zero	Specifies whether the reserved fields in a RIP packet are set to zero. Select an option: • **True**—Discards version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements check-zero the RIP version 1 and version 2 specifications. • **False**—Receives RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero. This behavior violates the specifications in RFC 1058 and RFC 2453.
Graceful switchover	Specifies graceful switch over for RIP. Enter the following: • **Disable**—Select the check box to disable graceful switchover. • **Restart time (sec)**—Enter the time in seconds for the restart to complete.

Authentication	Enter the following:
	
	• **Authentication Type**—Select the type of authentication for RIP route queries received on an interface. The options available are:
	
	  • None
	
	  • MD5
	
	  • Simple
	
	• **Authentication key**—Enter the authentication key for MD5.

Policy	

Table 143: Fields on the Edit RIP Global Settings Page *(Continued)*

Field	Action
Import Policy	Specifies one or more policies to routes being imported into the local routing device from the neighbors. Click one of the following options: • **+**—Adds an import policy. • **Move up arrow**—Moves the selected policy up the list of policies. • **Move down arrow**—Moves the selected policy down the list of policies. • **X**—Removes an import policy.
Trace Options	
File Name	Enter the filename to receive the output of the trace operation.
Number of Files	Enter the maximum number of trace files.
File Size	Enter the maximum size for each trace file.
World-readable	Specifies whether or not the trace file can be read by any user or not. Select an option: • **True**—Allows any user to read the file. • **False**—Restricts all users being able to read the file.
Flags	Select one or more flags from the Available Flags column and move it to the Configured Flags column using the arrow.

RELATED DOCUMENTATION

Delete RIP Global Settings | 505

Delete RIP Global Settings

You are here: **Network** > **Routing** > **RIP**.

To delete RIP global settings:

1. Select an information that you want to delete on the RIP Global settings table.
2. Click the delete icon available on the upper right side of the RIP Global settings table.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the RIP Page | **497**

CHAPTER 44

OSPF Routing

IN THIS CHAPTER

About the OSPF Page

IN THIS SECTION

You are here: **Network** > **Routing** > **OSPF**.

Use this page to configure OSPF routing.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an OSPF. See "Add an OSPF" on page 508.
- Edit an OSPF. See "Edit an OSPF" on page 517.
- Delete OSPF. See "Delete OSPF" on page 517.
- Advanced search for an OSPF. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you

hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

   Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

   NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

- Show or hide columns in the OSPF table. To do this, click the Show Hide Columns icon in the top right corner of the OSPF table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 144 on page 507 describes the fields on the OSPF page.

Table 144: Fields on the OSPF Page

Field	Description
Filter	Select an instance for OSPF from the list.
Area ID	Displays the area ID selected.
Area Type	Displays the area type selected.
Member Interfaces	Displays the member interface selected.
Version	Displays the version of the interface selected (OSPF for IPv4 and OSPFv3 for IPv6).

Table 144: Fields on the OSPF Page *(Continued)*

Field	Description
Routing Instance	Displays the routing instance of the interface selected. **NOTE**: This option is not available for tenant users.
Import Policy	Displays the import policy selected. **NOTE**: This option is not available for tenant users.
Export Policy	Displays the export policy selected. **NOTE**: This option is not available for tenant users.

RELATED DOCUMENTATION

Add an OSPF | 508

Add an OSPF

You are here: **Network** > **Routing** > **OSPF**.

To add an OSPF routing:

1. Click the add icon (**+**) on the upper right side of the OSPF page.
   The Create OSPF page appears.
2. Complete the configuration according to the guidelines provided in Table 145 on page 508.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   If you click **OK**, a new OSPF routing is added with the provided configuration.

Table 145: Fields on the Add an OSPF Page

Field	Action
Basic Settings	

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
Routing Instance	Select the routing instance from the list or create a new routing instance inline. **NOTE**: This option is not available for tenant users. To add a new routing instance inline: **1.** Click **Add**. The Create Routing Instance page appears. **2.** Enter the following details: • **General Settings** • Name—Enter a unique name for the routing instance that contains a corresponding IP unicast table; no special characters are allowed and the keyword default cannot be used. • Description—Enter a description for the routing instance. We recommend that you enter a maximum of 255 characters. • Instance Type—Select a type of routing instance from the list: • Virtual Router—Used for non-VPN related applications. • VPLS—This instance is applicable only for root or super admin. This option will not be applicable for LSYS admin. Interfaces with Encapsulation Ethernet-VPLS will be listed when VPLS instance type is selected. • **Interfaces**—Select one or more interfaces to associate with the routing instance from the Available column and move it to the Selected column using arrow. To search for specific interface, click the search icon and enter partial text or full text of the keyword in the search bar. **3.** Click **OK** to save changes.
Routing Options	
Router ID	Enter the ID of the routing device.

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
Traffic Engineering **NOTE**: This option is not available for OSPFv3.	Enable this option if you want the traffic to be managed or engineered.
Area Details	
Area Id	Specifies the uniquely identified area within its AS. Type a 32-bit numeric identifier for the area. Type an integer or select and edit the value. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3, the value assigned to the area is **0.0.0.3.**

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
Area Range	Displays a range of IP addresses for the summary link state advertisements (LSAs) to be sent within an area. Select an option: **1.** To add an area range form: **a.** Click **+**. The Create Area Range Form page appears. **b.** Enter the following details: • Area Range—Enter the area range address. **NOTE**: For OSPF, enter an IPv4 address and for OSPFv3 enter an IPv6 address. • Subnet mask—Enter the subnet mask area address. **NOTE**: This option is available only for IPv4 address. • Override metric—Select a value to override the metric for the IP address range. Range: 1025 through 65534. **c.** Select **Restrict Advertisements of this area range** to specify that the routes contained within a summary must not be displayed. **d.** Select **Enforce exact match for advertisements of this area range** to specify that the summary of a route must be advertised only when an exact match is made within the configured summary range. **e.** Click **OK**. **2.** To edit the selected are range: **a.** Select the existing area range. **b.** Click the pencil icon to edit the selected area range. The Edit Area Range Form page appears with editable fields.

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
	c. Click **OK** to save the changes. 3. To delete an area range: a. Select the area range that you want to delete. b. Click the delete icon. A confirmation message appears. c. Click **Yes** to delete the selected area range.
Version	Select the version of the OSPF: • ospf—Enables OSPF routing on the routing device. • ospf3—Enables OSPFv3 routing on the routing device.
Area Type **NOTE**: This option is not applicable for area zero.	Specifies the type of OSPF area. Select an option from the list: • **None**—A regular OSPF area, including the backbone area. • **stub**—A stub area. • **nssa**—A not-so-stubby area (NSSA).
No Summaries (Totally Stubby area) **NOTE**: This option is applicable for non-zero area and it is not applicable for area zero.	Enable or disable the summaries. **NOTE**: This option can be configured when area-type is nssa or stub.
Virtual Link **NOTE**: This option is applicable for area zero and it is not applicable for non-zero area.	Select whether you want the virtual link to be established. If you select virtual link to be created, then enter the Neighbor ID and Transit area. Transit area is the area that has virtual link connecting two or more ABRs attached to this area.

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
Interface Details	
Select Interface	Select one or more interfaces to associate with the routing instance from the Available column and move it to the Selected column using arrow.
Interface type	Specifies the interfaces to be associated with the OSPF configuration. Select an option from the list: • None—No interface. • nbma—Non broadcast multiaccess (NBMA) interface. **NOTE**: This option is not available for OSPFv3. • p2mp—Point-to-multipoint interface. • p2p—Point-to-point interface. • p2mp-over-lan—Point-to-multipoint over LAN mode. **NOTE**: This option is not available for OSPF.
Interface Metric	Type the metric that you want for measuring the interface.
Passive mode	Enable this option for the passive mode. **NOTE**: You can enable this option only if Secondary option is disabled and vice-versa.
Advanced	

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action

Bidirectional Forward Detection	Enable this option for the bidirectional forward detection (BFD) protocol version that you want to detect.
	
	If you enable, enter the following details:
	
	• BFD Version—Select the bidirectional forward detection version form the list:
	  • None—No BFD version is used.
	  • automatic—Autodetects the BFD protocol version.
	  • BFD Version 0—Uses BFD protocol version 0.
	  • BFD Version 1—Uses BFD protocol version 1.
	• Minimum Interval—Enter the minimum interval value for BFD in milliseconds. Range: 1 through 255,000.
	• Minimum Receive Interval—Enter the minimum receive interval value. Range: 1 through 255,000.

IPsec security association	Select a number of one of the security associations from the list. By default, no security keys are configured. **NOTE**: You can configure this option only if Secondary option is disabled and vice-versa.
Link protection	Enable this option. Creates a backup loop-free alternate path to the primary next hop for all destination routes that traverse the protected interface. **NOTE**: You can either enable Link protection or Node Link protection at a time. For example, if you enable Link protection, then Node Link protection is automatically disabled.
Node Link protection	Enable this option. Creates an alternate loop-free path to the primary next hop for all destination routes that traverse a protected interface. **NOTE**: You can either enable Link protection or Node Link protection at a time. For example, if you enable Link protection, then Node Link protection is automatically disabled.

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
Secondary	Enable this option. Specifies an interface to belong to another OSPF area. **NOTE**: You can enable this option only if Passive Mode is disabled and IPsec security association is not configured and vice-versa.
Authentication **NOTE**: This option is not available for OSPFv3.	Select an authentication key (password) from the list: • None • md5 • simplepassword
MD5 Authentication Key **NOTE**: This option is not available for OSPFv3.	Specifies an MD5 authentication key (password). Click **+** and enter the following details: • MD5 ID—MD5 key identifier. Range: 0 through 255. • Key—One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. Characters can include ASCII strings. If you include spaces, enclose all characters in quotation marks (“ ”). • Start Time—MD5 start time. Then, click tick mark to save the changes.
Simple Password **NOTE**: This option is not available for OSPFv3.	Enter a simple authentication key (password).
Advanced Settings	
Policy **NOTE**: This option is not available for tenant users.	

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
Import Policy	Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas. Click one of the following options: • **+**—Adds an import policy. • **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy up the list of policies down. • **X**—Removes the import policy.
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area. Click one of the following options: • **+**—Adds an import policy. • **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy up the list of policies down. • **X**—Removes the import policy.
Trace Options	
File Name	Enter the name of the file to receive the output of the trace operation.
Number of files	Enter the maximum number of trace files.
File Size	Enter the maximum size for each trace file.
World Readable	Enable this option to allow any user to read the file. Disable this option to prevent all users from reading the file.

Table 145: Fields on the Add an OSPF Page *(Continued)*

Field	Action
Flags	Specifies the trace operation to be performed. Select one or more flags in the Available column and move them to the Selected column using the right arrow.

RELATED DOCUMENTATION

Edit an OSPF | **517**

Edit an OSPF

You are here: **Network** > **Routing** > **OSPF**.

To edit an OSPF routing:

1. Select an existing OSPF routing that you want to edit on the OSPF page.
2. Click the pencil icon available on the upper right side of the OSPF page.

   The Create OSPF page appears with editable fields. For more information on the options, see "Add an OSPF" on page 508.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete OSPF | **517**

Delete OSPF

You are here: **Network** > **Routing** > **OSPF**.

To delete an OSPF routing:

1. Select an existing OSPF routing that you want to delete on the OSPF page.

2. Click the delete icon available on the upper right side of the OSPF page.

   A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the OSPF Page | **506**

CHAPTER 45

BGP Routing

IN THIS CHAPTER

About the BGP Page

IN THIS SECTION

You are here: **Network** > **Routing** > **BGP**.

Use this page to configure BGP routing.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a routing instance. See "Add a BGP Group" on page 523.
- Edit a routing instance. See "Edit a BGP Group" on page 528.
- Delete a routing instance. See "Delete a BGP Group" on page 529.

- Disable group information. To do this, select an existing group information and click **Disable**.
- Edit global information. See "Edit Global Information" on page 529.
- Disable global information. To do this, select an existing global information and click **Disable**.

Field Descriptions

Table 146 on page 520 describes the fields on the BGP page.

Table 146: Fields on the BGP Page

Field	Description
Routing Instance **NOTE**: If you log in as a tenant user, the Routing Instance is not displayed as tenant context supports only one routing instance.	Select routing instances from the list. Example: default or all routing instances.
Group Name	Displays the name of the group.
Status	Displays the status of the group.
Peer ASN	Displays the peer ASN.
Type	Displays the group type.
Dynamic Peers	Displays the dynamic peers selected.
Static Peers	Displays the static peers selected.
Routing Instance	Displays the routing instance selected.
Import Policy	Displays the import policy selected. **NOTE**: If you log in as a tenant user, Routing Instance, Import Policy, and Export Policy are not displayed.

Table 146: Fields on the BGP Page *(Continued)*

Field	Description
Export Policy	Displays the export policy selected. **NOTE**: If you log in as a tenant user, Routing Instance, Import Policy, and Export Policy are not displayed.
Global Information The global information values corresponding to the routing instance that you selected will be displayed in the Global Information section. Based on the routing instance that you select, the values in the Global information.	
Edit	Edits the Global settings which lists the following fields. See "Edit Global Information" on page 529.

Table 146: Fields on the BGP Page *(Continued)*

Field	Description
Name	Displays the following names: • Router Identifier—Specifies the routing device's IP address. • BGP Status—Enables or disables BGP. • Router ASN—Specifies the routing device's AS number. • Preference—Specifies the route preference. • Confederation—Specifies the routing device's confederation AS number. **NOTE**: If you log in as a tenant user, Confederation is not displayed. • Confederation Members—Specifies the AS numbers for the confederation members. **NOTE**: If you log in as a tenant user, Confederation Members is not displayed. • Description—Specifies the text description of the global, group, or neighbor configuration. • Import Policy—Specifies one or more routing policies for routes being imported into the routing table from BGP. **NOTE**: If you log in as a tenant user, Import Policy is not displayed. • Export Policy—Specifies one or more policies to routes being exported from the routing table into BGP. **NOTE**: If you log in as a tenant user, Export Policy is not displayed.

RELATED DOCUMENTATION

Add a BGP Group | 523

Add a BGP Group

You are here: **Network** > **Routing** > **BGP**.

To add a BGP Group:

1. Click the add icon (**+**) on the upper right side of the BGP Group page.

   The Add a Group page appears.
2. Complete the configuration according to the guidelines provided in Table 147 on page 523.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 147: Fields on the Add a Group Page

Field	Action
General	
Routing Instance **NOTE**: If you log in as a tenant user, the Routing Instance is not displayed as tenant context supports only one routing instance.	Select a routing instance from the list.
Group Name	Enter a new group name.
ASN	Specifies the unique numeric identifier of the AS in which the routing device is configured. Enter the routing device's 32-bit AS number, in dotted decimal notation. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter **3**, the value assigned to the AS is **0.0.0.3**.
Preference	Enter the degree of preference value for an external route. The route with the highest local preference value is preferred.

Table 147: Fields on the Add a Group Page *(Continued)*

Field	Action
Cluster Id	Enter the IPv6 or IPv4 address to be used as the cluster identifier. The cluster identifier is used by the route reflector cluster in an internal BGP group.
Description	Enter the text description for the global, group, or neighbor configuration.
Damping	Select the check box to enable route flap damping.
Advertise Inactive Routes	Select the check box to enable advertising of inactive routes.
Advertise Peer AS Routes	Select the check box to advertising of peer AS routes.
Neighbors	

Table 147: Fields on the Add a Group Page *(Continued)*

Field	Action
Dynamic Neighbors	Configures a dynamic neighbor (peer). Select one of the following options: **1.** To add a dynamic neighbor: **a.** Click **+**. The Add Dynamic Neighbor window appears. **b.** Select one of the following options in the Addresses field: • All • IPv4 • IPv6 **c.** Enter the following details if you select IPv4 in the Addresses field: • IP Address—Enter the IPv4 address for dynamic neighbor. • Subnet Mask—Enter the subnet mask for the IPv4 address. **d.** Enter the following details if you select IPv6 in the Addresses field: • IPv6 Address—Enter the IPv6 address for dynamic neighbor. • Prefix—Enter the prefix length using up and down arrows for the IPv6 address. **e.** Click **OK** to save changes. **2.** To edit a dynamic neighbor: **a.** Select the existing dynamic neighbor address. **b.** Click the pencil icon to edit the selected dynamic neighbor address. The Edit Dynamic Neighbor window appears with editable fields. **c.** Click **OK** to save changes. **3.** To delete a dynamic neighbor: **a.** Select the existing dynamic neighbor address. **b.** Click the delete icon (**X**) to delete the selected dynamic neighbor address.

Table 147: Fields on the Add a Group Page *(Continued)*

Field	Action
Static Neighbors	Configures a static neighbor (peer). Select one of the following options: **1.** To add a static neighbor: **a.** Click **+**. The Add Static Neighbor window appears. **b.** Enter the following details: • Addresses—Select IPv4 or IPv6. • IP Address—Enter the IPv4 address for static neighbor. • Local Address—Enter the IP address for static neighbor. • Preference—Enter the preference value for an external route. The route with the highest local preference value is preferred. • Description—Enter a description. • Hold Time—Enter the hold timeout interval period. • Out Delay—Enter the output delay time. Range: 0 through 65,535 seconds. • Passive—Select the check box to enable the device to be passive. The routing device will wait for the peer to issue an open request before a message is sent. • As Override—Select the check box to replace all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer. • Import Policy—Select one of the following options: • **+**—Adds an import policy.

Table 147: Fields on the Add a Group Page *(Continued)*

Field	Action
	• **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy down. • **X**—Removes an import policy. • Export Policy—Select one of the following options: • **+**—Adds an import policy. • **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy down. • **X**—Removes an import policy. **c.** Click **OK** to save changes. **2.** To edit a static neighbor: **a.** Select the existing static neighbor address. **b.** Click the pencil icon to edit the selected static neighbor address. The Edit Static Neighbor window appears with editable fields. **c.** Click **OK** to save changes. **3.** To delete a static neighbor: **a.** Select the existing static neighbor address. **b.** Click the delete icon (**X**) to delete the selected static neighbor address.
Policies Tab	

Table 147: Fields on the Add a Group Page *(Continued)*

Field	Action
Import Policy	Specifies one or more routing policies for routes being imported into the routing table from BGP. Select one of the following options: • **+**—Adds an import policy. • **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy down. • **X**—Removes an import policy.
Export Policy	Specifies one or more policies to routes being exported from the routing table into BGP. Select one of the following options: • **+**—Adds an import policy. • **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy down. • **X**—Removes an import policy.

RELATED DOCUMENTATION

Edit a BGP Group | 528

Edit a BGP Group

You are here: **Network** > **Routing** > **BGP**.

To edit a BGP group :

1. Select an existing BGP group that you want to edit on the BGP page.
2. Click the pencil icon available on the upper right side of the BGP page.

The Edit a Group page appears with editable fields. For more information on the fields, see "Add a BGP Group" on page 523.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete a BGP Group | 529

Delete a BGP Group

You are here: **Network** > **Routing** > **BGP**.

To delete a BGP group:

1. Select an existing BGP group that you want to delete on the BGP page.
2. Click the delete icon available on the upper right side of the BGP page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

Edit Global Information | 529

Edit Global Information

You are here: **Network** > **Routing** > **BGP**.

To edit BGP global information:

1. Select an existing global information that you want to edit on the BGP page.
2. Click the pencil icon available on the upper right side of the Global Information table.

   The Edit Global Settings page appears.
3. Complete the configuration according to the guidelines provided in Table 148 on page 530.
4. Click **OK** to save the changes.

Table 148: Fields on the Edit Global Settings Page

Field	Action
General	
Router ASN	Enter the router ASN value.
Router Identifier	Enter the router identification IP address.
BGP Status	Select an option from the list: Enable or Disable.
Preference	Enter the degree of preference value for an external route. The route with the highest local preference value is preferred.
Description	Enter the description.
Confederation Number	Enter the router confederation ASN value.

Table 148: Fields on the Edit Global Settings Page *(Continued)*

Field	Action
Confederation Members	Specifies the AS numbers for the confederation members. Select one of the following options: **1.** To add a member ASN: **a.** Click **+**. The Confederation Members window appears. **b.** Enter member ASN value in the Member ASN field. **c.** Click **OK** to save changes. **2.** To edit a member ASN: **a.** Select an existing member ASN value and click the pencil icon. The Confederation Members window appears. **b.** Edit member ASN value in the Member ASN field. **c.** Click **OK** to save changes. **3.** To delete a member ASN: **a.** Select an existing member ASN value. The Confederation Members window appears. **b.** Click the delete icon to delete the member ASN value.
Advance Options	
Keep Route	Specifies whether routes learned from a BGP peer must be retained in the routing table even if they contain an AS number that was exported from the local AS. Select **All** or **None** to configure keep routes.
TCP MSS	Enter the maximum segment size (MSS) for the TCP connection. Range: 1 through 4096.
MTU Discovery	Select the check box to enable MTU discovery.

Table 148: Fields on the Edit Global Settings Page *(Continued)*

Field	Action
Remove Private ASN	Select the check box to enable removal of private ASNs.
Graceful Restart	Enter the following details: • Restart Time—Enter the period of time after which a restart is expected to be complete. • Stale Routes Time—Enter the maximum time that stale routes are kept during restart.
Multihop	Specifies the maximum time-to-live (TTL) value for the TTL in the IP header of BGP packets. Enter the following details: • Nexthop Change—Select the check box to allow unconnected third-party next hops. • TTL—Enter a TTL value.
Authentication	Enter the following details: • Authentication Algorithm—Select an option from the list: None, MD5, or SHA1. • Authentication Key—Enter an MD5 authentication key (password). This option is available if you select MD5 as authentication algorithm.
Policies Tab **NOTE**: If you log in as a tenant user, Policy tab is not displayed.	

Table 148: Fields on the Edit Global Settings Page *(Continued)*

Field	Action
Import Policy	Applies one or more policies to routes being imported into the local routing device from the neighbors. Select one of the following options: • **+**—Adds an import policy. • **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy down. • **X**—Removes an import policy.
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area. Select one of the following options: • **+**—Adds an import policy. • **Move up**—Moves the selected policy up the list of policies. • **Move down**—Moves the selected policy down. • **X**—Removes an import policy.
Trace Options Tab	
File Name	Enter the name of the file to receive the output of the trace operation.
Number of Files	Enter the maximum number of trace files.
File Size	Enter the maximum size for each trace file.

Table 148: Fields on the Edit Global Settings Page *(Continued)*

Field	Action
World Readable	Specifies whether the trace file can be read by any user. Select an option: • **True**—Allows any user to read the file. • **False**—Prevents all users from reading.
Flags	Select one or more flags from the Available Flags column and move it to the Configured Flags column using the arrow.

RELATED DOCUMENTATION

About the BGP Page | 519

CHAPTER 46

Routing Instances

IN THIS CHAPTER

About the Routing Instances Page

IN THIS SECTION

You are here: **Network** > **Routing** > **Routing Instances**.

Use this page to configure routing instances.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a routing instance. See "Add a Routing Instance" on page 537.
- Edit a routing instance. See "Edit a Routing Instance" on page 538.
- Delete a routing instance. See "Delete Routing Instance" on page 539.

- Show or hide columns in the Routing Instance table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advance search for a routing instance. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 149 on page 536 describes the fields on the Routing Instances page.

Table 149: Fields on the Routing Instances Page

Field	Description
Name	Name of the routing instance.
Type	Identifies the routing instance type.
Assigned Interfaces	Displays the selected interfaces assigned to the routing instance.
Description	Displays the description of the routing instances.

RELATED DOCUMENTATION

Add a Routing Instance | 537

Add a Routing Instance

You are here: **Network** > **Routing** > **Routing Instances**.

To add a routing interface:

1. Click the add icon (+) available on the upper right side of the Routing Instances page.
   The Create Routing Instance page appears.
2. Complete the configuration according to the guidelines provided in Table 150 on page 537.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
   If you click **OK**, a new routing instance is added with the provided configuration.

Table 150: Fields on the Add Routing Instance

Field	Description
General Settings	
Name	Enter a unique name for the routing instance that contains a corresponding IP unicast table; no special characters are allowed and the keyword default cannot be used.
Description	Enter a description for the routing instance. We recommend that you enter a maximum of 255 characters.
Instance Type	Select the type of routing instance from the list: • Virtual Router—Used for non-VPN related applications. • VPLS—This instance is applicable only for root or super admin. This option will not be applicable for LSYS admin. Interfaces with Encapsulation Ethernet-VPLS will be listed when VPLS instance type is selected.

Table 150: Fields on the Add Routing Instance *(Continued)*

Field	Description
Interfaces	Select interfaces from the Available column and move it to the Selected column using the arrow. • Name—Displays the interface name. • Zone—Displays the zone name corresponding to the interface name. This is used to validate that all the interfaces of the selected zone(s) must belong to the same routing instance.

RELATED DOCUMENTATION

About the Routing Instances Page | 535
Edit a Routing Instance | 538

Edit a Routing Instance

You are here: **Network** > **Routing** > **Routing Instances**.

To edit a routing instance:

1. Select a routing instance that you want to edit on the Routing Instances page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Routing Instance page appears with editable fields. For more information on the fields, see "Add a Routing Instance" on page 537.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

About the Routing Instances Page | 535
Delete Routing Instance | 539

Delete Routing Instance

You are here: **Network** > **Routing** > **Routing Instances**.

To delete a routing instance:

1. Select one or more routing instance that you want to delete on the Routing Instances page.
2. Click the delete icon available on the upper right side of the page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

- About the Routing Instances Page | **535**
- Add a Routing Instance | **537**
- Edit a Routing Instance | **538**

CHAPTER 47

Routing—Policies

IN THIS CHAPTER

About the Policies Page

IN THIS SECTION

You are here: **Network** > **Routing** > **Policies**.

Use this page to configure policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create global options. See "Global Options" on page 542.
- Create a policy. See "Add a Policy" on page 543.

- Clone a policy. See "Clone a Policy" on page 555.
- Edit a policy. See "Edit a Policy" on page 555.
- Delete a policy. See "Delete Policy" on page 555.
- Term Up—Moves a term up in a selected list policies configuration.
- Term Down—Moves a term down in a selected list policies configuration.
- Test a policy. See "Test a Policy" on page 556.

Field Descriptions

Table 151 on page 541 describes the fields on the Policies page.

Table 151: Fields on the Policies Page

Field	Description
Name	Displays the name of the policy.
From: Prefix	Displays the policy prefix.
From: Protocol	Displays the selected source protocol.
From: Interface or Address	Displays the selected source interface or IP address.
To: Protocol	Displays the source destination protocol.
To: Interface or Address	Displays the selected interface or address.
Action	Displays the selected action.
Move To	Displays if the action is to move to next policy or term.

RELATED DOCUMENTATION

Global Options | 542

Global Options

You are here: **Network** > **Routing** > **Policies**.

To edit global options:

1. Select an existing configuration that you want to edit on the Global Options page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Global Options page appears. You can modify any previous changes done. For more information on the options, see Table 152 on page 542.
3. Click **OK** to save the changes.

Table 152: Fields on the Global Options Page

Field	Action
Add Prefix List	
Name	Enter the name of the prefix list. Select an option from the list: • **Add**—Adds the prefix list. • **Edit**—Edits the prefix list. • **X**—Removes the prefix list.
Members	
IP Address	To add prefix list members: 1. Click **+**. The Add Prefix List Members page appears. 2. Enter the following details: • IP Address—Enter the prefix list IP address. • Subnet Mask—Enter the subnet mask IP address 3. Click **OK** to save changes. Click the pencil icon to edit the IP address. You can click **X** to delete the IP address.

Table 152: Fields on the Global Options Page *(Continued)*

Field	Action
As Path	
As Path	Click **+** to add As path. As Path Name—Enter the name of the As path. Regular Expression—Enter the regular expression of the As path. Click the pencil icon to edit the As path. You can click **X** to delete the As path.
BGP Community	
BGP Community	Click **+** to add a BGP community. Name—Enter the BGP community name. Click the pencil icon to edit the As path. You can click **X** to delete the As path.
Members	Click **+** to add a BGP community member. Community ID—Enter the BGP community ID.

RELATED DOCUMENTATION

Add a Policy | 543

Add a Policy

You are here: **Network** > **Routing** > **Policies**.

To add a policy:

1. Click **+** > **New** on the right side of the Policies page.
   The Add Policy page appears.
2. Complete the configuration according to the guidelines provided in Table 153 on page 544.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, a new policy is added with the provided configuration.

Table 153: Fields on the Policy Page

Field	Description
Policy Name	Enter the policy name.
Terms	Click one of the following: • **+**—Adds the term. • **Edit**—Edits the term. • **X**—Deletes the term,
Add Term	
Term Name	Enter the term name.
Source	
Family	Select a family protocol address from the list.
Routing Instance	Select a routing instance from the list.
RIB	Select a routing table from the list.
Preference	Enter a preference value for the route.
Metric	Enter the metric value. You can specify up to four metric values.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
Interface	Specifies the name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP). Choose one of the following options: **1.** To add an interface **a.** Click **+** and select **Interface**. The Available Interfaces page appears. **b.** Select an interface from the list and click **OK**. The selected interface is added. **2.** To add an IP address **a.** Click **+** and select **Address**. The Add IP Address page appears. **b.** Enter IP address from the list and click **OK**. The selected IP address is added. **3.** To delete an interface or an IP address: **a.** Select an existing interface or address from Interfaces. **b.** Click **X**. The selected interface or IP address is deleted.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
Prefix List	Specifies a named list of IP addresses. You can specify an exact match with incoming routes. Choose one of the following options: **1.** To add a prefix list: **a.** Click **+**. The Available Prefix List page appears. **b.** Select a prefix list from the list and click **OK**. The selected prefix list is added. **2.** To delete a prefix list: **a.** Select an existing prefix list. **b.** Click **X**. The selected prefix list is deleted.
Protocol	Specifies the name of the protocol from which the route was learned or to which the route is being advertised. Choose one of the following options: **1.** To add a protocol: **a.** Click **+**. The Available Protocols page appears. **b.** Select a protocol from the list and click **OK**. The selected protocol is added. **2.** To delete a protocol: **a.** Select an existing protocol. **b.** Click **X**. The selected protocol is deleted.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
Policy	Specifies the name of a policy to evaluate as a subroutine. Choose one of the following options: 1. To add a policy: a. Click **+**. The Available Policies page appears. b. Select a policy from the list and click **OK**. The selected policy is added. 2. To delete a policy: a. Select an existing policy. b. Click **X**. The selected policy is deleted.
More	Click **More** for advanced configuration options for policies. The More Options page appears. Click **OK** to save changes after the configuration is complete.
More Options	
OSPF Area ID	Enter the IP address for the area identifier.
BGP Origin	Select a value from the list to specify the origin of the AS path information.
Local Preference	Type a BGP local preference value.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
AS Path	Specifies the name of an AS path regular expression. Choose one of the following options: **1.** To add an As path: **a.** Click **+**. The Available AS Paths page appears. **b.** Select an As path from the list and click **OK**. The selected As path is added. **2.** To delete an As path: **a.** Select an existing As path. **b.** Click **X**. The selected As path is deleted.
Route	Enter the following details: • External—Select the check box to enable external routing. • OSPF Type—Select an OSPF type from the list.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
Community	Specifies the name of one or more communities. Choose one of the following options: 1. To add a community: a. Click **+**. The Available Communities page appears. b. Select a community from the list and click **OK**. The selected community is added. 2. To delete a community: a. Select an existing community. b. Click **X**. The selected community is deleted.
Destination	
Family	Select a value for address family protocol from the list.
Routing Instance	Select a routing instance from the list.
RIB	Select a name of a routing table from the list.
Preference	Type a preference value for the route.
Metric	Type a metric value.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
Interface	Specifies the name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP). Choose one of the following options: **1.** To add an interface: **a.** Click **+** and select **Interface**. The Available Interfaces page appears. **b.** Select an interface from the list and click **OK**. The selected interface is added. **2.** To add an IP address: **a.** Click **+** and select **Address**. The Add IP Address page appears. **b.** Enter IP address from the list and click **OK**. The selected IP address is added. **3.** To delete an interface or an IP address: **a.** Select an existing interface or address from Interfaces. **b.** Click **X**. The selected interface or IP address is deleted.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
Protocol	Specifies the name of the protocol from which the route was learned or to which the route is being advertised. Choose one of the following options: **1.** To add a protocol: **a.** Click **+**. The Available Protocols page appears. **b.** Select a protocol from the list and click **OK**. The selected protocol is added. **2.** To delete a protocol: **a.** Select an existing protocol. **b.** Click **X**. The selected protocol is deleted.
Policy	Displays the name of the policy. Choose one of the following options: **1.** To add a policy: **a.** Click **+**. The Available Policies page appears. **b.** Select a policy from the list and click **OK**. The selected policy is added. **2.** To delete a policy: **a.** Select an existing policy. **b.** Click **X**. The selected policy is deleted.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
More	Click **More** for advanced configuration options for policies. The More Options page appears. Click **OK** to save changes after the configuration is complete.
Action	
Action	Select an action value from the list.
Default Action	Select a value from the list. Specifies that any action that is intrinsic to the protocol is overridden. This action is also non terminating so that various policy terms can be evaluated before the policy is terminated.
Next	Select a value from the list. Specifies the default control action if a match occurs, and there are no further terms in the current routing policy.
Priority	Select a value from the list. Specifies a priority for prefixes included in an OSPF import policy. Prefixes learned through OSPF are installed in the routing table based on the priority assigned to the prefixes.
BGP Origin	Select a value from the list. Specifies the BGP origin attribute.
AS Path Prepend	Enter AS path prepend value. Affixes an AS number at the beginning of the AS path. AS numbers are added after the local AS number has been added to the path. This action adds an AS number to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS number is placed within a confederation sequence. Otherwise, the affixed AS number is placed with a non confederation sequence.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
AS Path Expand	Enter the following details: • Type—Select the type and type a value. Extracts the last AS number in the existing AS path and affixes that AS number to the beginning of the AS path n times, where n is a number from 1 through 32. The AS number is added before the local AS number has been added to the path. This action adds AS numbers to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS numbers are placed within a confederation sequence. Otherwise, the affixed AS numbers are placed within a non confederation sequence. This option is typically used in non-IBGP export policies. • Value—Enter the As path value.
Preference	Enter the following details: • Action—Select the preference action and type a value. • Value—Enter the preference value.
Local Preference	Enter the following details: • Action—Select the preference action and type a value. • Value—Enter the preference value.
Load Balance Per Packet	Select the check box to enable this option. Specifies that all next-hop addresses in the forwarding table must be installed and have the forwarding table perform per-packet load balancing. This policy action allows you to optimize VPLS traffic flows across multiple paths.
Tag	Enter the following details: • Action—Select the action and type a value. Changes the metric (MED) value by the specified negative or positive offset. This action is useful only in an external BGP (EBGP) export policy. • Value—Enter the tag value.

Table 153: Fields on the Policy Page *(Continued)*

Field	Description
Metric	Enter the following details: • Action—Select the action and type a value. Specifies the tag value. The tag action sets the 32-bit tag field in OSPF external link-state advertisement (LSA) packets. • Value—Enter the metric value.
Route	Enter the following details: • External—Select the check box to enable this option. • OSPF Type—Select an option from the list.
Class of Service	Enter the following details: • Class—Select **None** from the list. Specifies the class-of-service parameters to be applied to routes installed into the routing table. • Source Class—Enter the source class. Specifies that the value entered here maintains the packet counts for a route passing through your network, based on the source address. • Destination Class—Enter the destination class. Specifies the value entered here maintains packet counts for a route passing through your network, based on the destination address in the packet. • Forwarding Class—Enter the forwarding class. Specifies that the value of queue number entered here maintains packet counts for a route passing through your network, based on the internal queue number assigned in the packet.

RELATED DOCUMENTATION

Clone a Policy | 555

Clone a Policy

You are here: **Network** > **Routing** > **Policies**.

To clone a policy:

1. Select a policy that you want to clone and select **Clone** from the More link.

   The Clone Policy page appears with editable fields. For more information on the fields, see "Add a Policy" on page 543.
2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

Edit a Policy | 555

Edit a Policy

You are here: **Network** > **Routing** > **Policies**.

To edit a policy:

1. Select a policy that you want to edit on the Policies page.
2. Click the pencil icon available on the upper right side of the Policies page.

   The Edit Policy page appears with editable fields. For more information on the options, see "Add a Policy" on page 543.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Policy | 555

Delete Policy

You are here: **Network** > **Routing** > **Policies**.

To delete a policy configuration:

1. Select one or more policies that you want to delete from the Policies page.
2. Click the delete icon available on the upper right side of the Policies page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

Test a Policy | 556

Test a Policy

You are here: **Network** > **Routing** > **Policies**.

To test a policy:

1. Select a policy you want to test.
2. Click **Test Policy** at the upper right side of the Policies page.

   The Test Policy page appears.
3. Click **Start** to test the policy.

   You can click **Generate Report** to get the test reports.

RELATED DOCUMENTATION

Add a Policy | 543
Edit a Policy | 555
Delete Policy | 555

CHAPTER 48

Routing—Forwarding Mode

IN THIS CHAPTER

About the Forwarding Mode Page

IN THIS SECTION

You are here: **Network** > **Routing** > **Forwarding Mode**.

Use this page to view the forwarding configuration details.

Field Descriptions

Table 154 on page 558 describes the fields on the Forwarding Mode page.

Once the configuration is complete, click **Save** to save the changes or click **Cancel** to discard the changes.

Table 154: Fields on the Forwarding Mode Page

Field	Description
Family IPv6	Supports IPv6 protocol traffic, including Routing Information Protocol for IPv6 (RIPng). Select an option from the list: • None • drop—Drop IPv6 packets. • flow-based—Perform flow-based packet forwarding. • packet-based—Perform simple packet forwarding. **NOTE**: For SRX5000 line of devices, only drop and flow-based options are available.
Family ISO **NOTE**: This option is not available for SRX5000 line of devices.	Supports IS-IS traffic. Select an option from the list: • None • packet-based
Family MPLS **NOTE**: This option is not available for SRX5000 line of devices.	Supports MPLS traffic. Select an option from the list: • None • flow-based • packet-based

CHAPTER 49

CoS—Value Aliases

IN THIS CHAPTER

About the Value Aliases Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

Use this page to view, add, and remove value aliases details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a code point alias. See "Add a Code Point Alias" on page 560.
- Edit a code point alias. See "Edit a Code Point Alias" on page 561.
- Delete a code point alias. See "Delete Code Point Alias" on page 562.

Field Descriptions

Table 155 on page 560 describes the fields on the Value Alias page.

Table 155: Fields on the Value Alias Page

Field	Description
Alias name	Displays the name given to CoS values. For example, af11 or be.
Alias type	Displays the code point type. The following types of code points are supported: • **DSCP**—Defines aliases for Differentiated Services code point (DSCP) for IPv4 values. You can refer to these aliases when you configure classes and define classifiers. • **DSCP-IPv6**—Defines aliases for DSCP IPv6 values. You can refer to these aliases when you configure classes and define classifiers. • **EXP**—Defines aliases for MPLS experimental (EXP) bits. You can map MPLS EXP bits to the device forwarding classes. • **inet-precedence**—Defines aliases for IPv4 precedence values. Precedence values are modified in the IPv4 TOS field and mapped to values that correspond to levels of service.
CoS Value bits	Displays the CoS value for which an alias is defined. **NOTE**: Changing this value alters the behavior of all classifiers that refer to this alias.

RELATED DOCUMENTATION

Add a Code Point Alias | 560

Add a Code Point Alias

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

To add a code point alias:

1. Click the add icon (**+**) available on the right side of the Value Aliases page.

The Add Code Point Alias page appears.

2. Complete the configuration according to the guidelines provided in Table 156 on page 561.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 156: Fields on the Add Code Point Alias Page

Field	Description
Code point name	Enter a name for the CoS point alias.
Code point type	Select a code point type from the list.
Code point value bits	Select a COS value for which an alias is defined.

RELATED DOCUMENTATION

Edit a Code Point Alias | **561**

Edit a Code Point Alias

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

To edit a code point alias:

1. Select a code point alias that you want to edit on the Value Aliases page.
2. Click the pencil icon available on the upper right side of the Value Aliases page.

   The Code Point options appears with editable fields. For more information on the options, see "Add a Code Point Alias" on page 560.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Code Point Alias | **562**

Delete Code Point Alias

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

To delete a code point alias:

1. Select a code point alias that you want to delete on the Value Aliases page.
2. Click the delete icon available on the upper right side of the Value Aliases page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the Value Aliases Page | 559

CHAPTER 50

CoS—Forwarding Classes

IN THIS CHAPTER

About the Forwarding Classes Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

Use this page to view, add, and delete Forwarding Classes.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a forwarding class. See "Add a Forwarding Class" on page 564.
- Edit a forwarding class. See "Edit a Forwarding Class" on page 565.
- Delete forwarding class. See "Delete Forwarding Class" on page 565.

Field Descriptions

Table 157 on page 564 describes the fields on the Forwarding Classes page.

Table 157: Fields on the Forwarding Classes Page

Field	Description
Forwarding class name	Displays the forwarding class name assigned to the internal queue number. By default, four forwarding classes are assigned to queue numbers: 0 (best-effort), 1 (assured-forwarding), 5 (expedited-forwarding), and 7 (network-connect).
Queue number	Displays the internal queue numbers to which forwarding classes are assigned. By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can have more than one forwarding class assigned to a queue number.
Queue characteristics	Displays the queue characteristics, for example, video or voice.

RELATED DOCUMENTATION

Add a Forwarding Class | 564

Add a Forwarding Class

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

To add a forwarding class:

1. Click the add icon (**+**) available on the right side of the Forwarding Class page.
   The Add Forwarding Class page appears.
2. Complete the configuration according to the guidelines provided in Table 158 on page 565.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 158: Fields on the Add Forwarding Class page

Field	Description
Queue number	Select the internal queue number to which a forwarding class is assigned.
Forwarding class name	Enter the forwarding class name assigned to the internal queue number.

RELATED DOCUMENTATION

Edit a Forwarding Class | 565

Edit a Forwarding Class

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

To edit a forwarding class:

1. Select an existing forwarding class that you want to edit on the Forwarding Classes page.
2. Click the pencil icon available on the upper right side of the Forwarding Classes page.

   The Edit Forwarding Class options appears with editable fields. For more information on the options, see "Add a Forwarding Class" on page 564 for options available for editing.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Forwarding Class | 565

Delete Forwarding Class

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

To delete a forwarding class:

1. Select an existing forwarding class that you want to delete on the Forwarding Classes page.

2. Click the delete icon available on the upper right side of the Forwarding Classes page.

   A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the Forwarding Classes Page | 563

CHAPTER 51

CoS Classifiers

IN THIS CHAPTER

About the Classifiers Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

Use this page to view, add, and delete Classifier Page configuration.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a classifier. See "Add a Classifier" on page 569.
- Edit a classifier. See "Edit a Classifier" on page 570.
- Delete classifier. See "Delete Classifier" on page 571.

Field Descriptions

Table 159 on page 568 describes the fields on the Classifiers page.

Table 159: Fields on the Classifiers Page

Field	Description
Classifier name	Displays the name of a classifier.
Classifier type	Displays the classifier type. The following type of classifiers are available: • **dscp**—Differentiated Services code point classifier for IPv4. • **dscp-ipv6**—Differentiated Services code point classifier for IPv6 (default and compatibility). **NOTE**: This option is not available on SRX4000 lines of devices. • **exp**—MPLS experimental (EXP) bits classifier **NOTE**: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices. • **ieee-802.1**—IEEE-802.1 classifier • **ieee-802.1ad**—IEEE-802.1ad classifier **NOTE**: This option is not available on SRX4000 lines of devices. • **inet-precedence**—IPv4 precedence classifier (default and compatibility)
Details of classifiers	
Incoming code point	Displays CoS values and the aliases to which the forwarding class and loss priority are mapped.
Forwarding class name	Displays forwarding class names that are assigned to specific CoS values and aliases of a classifier.
Loss priority	Displays loss priorities that are assigned to specific CoS values and aliases of a classifier.

RELATED DOCUMENTATION

Add a Classifier | 569

Add a Classifier

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

To add a classifier:

1. Click the add icon (**+**) available on the right side of the Classifiers page.

   The Add Classifier page appears.
2. Complete the configuration according to the guidelines provided in Table 160 on page 569.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 160: Fields on the Add Classifier Page

Field	Description
Classifier name	Enter the classifier name.
Classifier type	Select a classifier type from the list. • **dscp**—Differentiated Services code point classifier for IPv4. • **dscp-ipv6**—Differentiated Services code point classifier for IPv6 (default and compatibility). **NOTE**: This option is not available on SRX4000 lines of devices. • **exp**—MPLS experimental (EXP) bits classifier **NOTE**: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices. • **ieee-802.1**—IEEE-802.1 classifier • **ieee-802.1ad**—IEEE-802.1ad classifier **NOTE**: This option is not available on SRX4000 lines of devices. • **inet-precedence**—IPv4 precedence classifier (default and compatibility)

Table 160: Fields on the Add Classifier Page *(Continued)*

Field	Description
Code point mapping	Specifies the code point mapping created. The available options are as follows: • **Add**—Click **+** to add a code point mapping. • **Edit**—Click pencil icon to edit the selected code point mapping. • **Delete**—Deletes the code point mapping.
Code point	Select the CoS value in bits and the alias of a classifier from the list.
Forwarding class	Select the forwarding class for the specified CoS value and alias from the list.
Loss priority	Select the loss priority for the specified CoS value and alias from the list.

RELATED DOCUMENTATION

Edit a Classifier | 570

Edit a Classifier

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

To edit a classifier:

1. Select an existing classifier configuration that you want to edit on the Classifiers page.
2. Click the pencil icon available on the upper right side of the Classifiers page.

   The Edit Classifiers page appears with editable fields. For more information on the options, see "Add a Classifier" on page 569.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Classifier | 571

Delete Classifier

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

To delete a classifier:

1. Select a classifier that you want to delete on the Classifiers Page.
2. Click the delete icon available on the upper right side of the Classifiers page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Classifiers Page | 567

CHAPTER 52

CoS—Rewrite Rules

IN THIS CHAPTER

About the Rewrite Rules Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

Use this page to add, edit, or delete rewrite rule configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a rewrite rule. See "Add a Rewrite Rule" on page 573.
- Edit a rewrite rule. See "Edit a Rewrite Rule" on page 575.
- Delete rewrite rule. See "Delete Rewrite Rule" on page 575.

Field Descriptions

Table 161 on page 573 describes the fields on the Rewrite Rules page.

Table 161: Fields on the Rewrite Rules Page

Field	Description
Rewrite rule name	Displays the names of defined rewrite rules.
Rewrite rule type	Displays the rewrite rule type.
Code Point Details	
Egress/Outgoing Code point	Displays the CoS values and aliases that a specific rewrite rule has set for a specific forwarding class and loss priority.
Forwarding class name	Displays the forwarding classes associated with a specific rewrite rule.
Loss priority	Displays the loss priority values associated with a specific rewrite rule.

RELATED DOCUMENTATION

Add a Rewrite Rule | 573

Add a Rewrite Rule

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

To add a rule configuration:

1. Click the add icon (**+**) available on the right side of the Forwarding Class page.
   The Add Rewrite Rule page appears.
2. Complete the configuration according to the guidelines provided in Table 162 on page 574.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 162: Fields on the Add Rewrite Rule Page

Field	Action
Rewrite rule name	Enter the name of a defined rewrite rule.
Rewrite rule type	Select a rewrite rule type from the list. • **dscp**—Defines the Differentiated Services code point rewrite rule. • **ieee-802.1**—Defines the IEEE-802.1 rewrite rule. • **inet-precedence**—Defines the precedence rewrite rule for IPv4. • **exp**—Defines the MPLS EXP rewrite rule. **NOTE**: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices. • **dscp-ipv6**—Defines the Differentiated Services code point rewrite rule for IPv6. **NOTE**: This option is not available on SRX4000 lines of devices. • **ieee-802.1ad**—Defines the IEEE-802.1ad rewrite rule. **NOTE**: This option is not available on SRX4000 lines of devices. • **frame-relay-de**—Defines the frame relay discard eligible bit rewrite rule. **NOTE**: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices.
Code point mapping	Specifies the code point mapping created. Click one: • **Add**—Click **+** to add a code point mapping. • **Edit**—Click pencil icon to edit the selected code point mapping. • **Delete**—Deletes the code point mapping.
Egress/Outgoing Code point	Select a CoS value and alias from the list.

Table 162: Fields on the Add Rewrite Rule Page *(Continued)*

Field	Action
Forwarding class	Select the forwarding class of the rewrite rule from the list.
Loss priority	Select the loss priority of the rewrite rule from the list.

RELATED DOCUMENTATION

Edit a Rewrite Rule | 575

Edit a Rewrite Rule

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

To edit a rewrite rule:

1. Select an existing rule configuration you want to edit on the Rewrite Rules page.
2. Click the pencil icon available on the upper right side of the Rewrite Rules page.

   The Edit Rewrite Rule page appears with editable fields. For more information on the options, see "Add a Rewrite Rule" on page 573.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Rewrite Rule | 575

Delete Rewrite Rule

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

To delete a rewrite rule:

1. Select an existing rule configuration you want to delete on the Rewrite Rules page.

2. Click the delete icon available on the upper right side of the Rewrite Rules page.

   A confirmation window appears.

3. Click **Yes** to delete or click **No** to retain the previous configuration.

RELATED DOCUMENTATION

About the Rewrite Rules Page | 572

CHAPTER 53

CoS—Schedulers

IN THIS CHAPTER

About the Schedulers Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

Use this page to add, edit or delete configuration of schedulers and enable or disable global settings.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a scheduler. See "Add a Scheduler" on page 578.
- Edit a scheduler. See "Edit a Scheduler" on page 580.
- Delete scheduler. See "Delete Scheduler" on page 581.

Field Descriptions

Table 163 on page 578 describes the fields on the Schedulers page.

Table 163: Fields on the Schedulers Page

Field	Description
Schedulers Global Setting	
Enable Non Strict Priority	Applies non-strict priority policy to all the schedulers.
Schedulers Configuration	
Scheduler name	Displays the names of defined schedulers.
Scheduler priority	Displays the scheduler transmission priority, which determines the order in which an output interface transmits traffic from the queues.
Details of scheduler	
Name	Displays the scheduler name.
Value	Displays the CoS value.

RELATED DOCUMENTATION

Add a Scheduler | 578

Add a Scheduler

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

To add a scheduler:

1. Click the add icon (**+**) available on the right side of the Scheduler page.

   The Add Scheduler page appears.

2. Complete the configuration according to the guidelines provided in Table 164 on page 579.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 164: Fields on the Add Scheduler Page

Field	Action
Scheduler name	Enter the scheduler name.
Scheduler priority	Select an option from the list: • **high**—Packets in this queue have high priority. • **low**—Packets in this queue are transmitted last. • **medium-low**—Packets in this queue have medium-low priority. • **medium-high**—Packets in this queue have medium-high priority. • **strict-high**—Packets in this queue are transmitted first.
Buffer size	Select an option from the list: • **exact**—Exact buffer size. • **percent**—Percentage of the total buffer. Select and type an integer from 1 through 100. • **remainder**—Remaining available buffer size. • **temporal**—Temporal value in microseconds.
Shaping rate	Enter the minimum bandwidth allocated to a queue. Select an option from the list: • **rate**—Shaping rate as an absolute number of bits per second. Select and type an integer from 3200 through 160,000,000,000 bits per second. • **percent**—Shaping rate as a percentage. Select and type an integer from 0 through 100.

Table 164: Fields on the Add Scheduler Page *(Continued)*

Field	Action
Transmit rate	Enter the transmission rate of a scheduler. Select an option from the list: • **rate**—Transmit rate. Select and type an integer from 3200 through 160,000,000,000 bits per second. • **exact**—Exact transmit rate. • **percent**—Percentage of transmission capacity. Select and type an integer from 1 through 100. • **remainder**—Remaining transmission capacity.

RELATED DOCUMENTATION

Edit a Scheduler | 580

Edit a Scheduler

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

To edit a scheduler:

1. Select an existing scheduler that you want to edit on the Schedulers page.
2. Click the pencil icon available on the upper right side of the Schedulers page.

   The Edit Scheduler appears with editable fields. For more information on the options, see "Add a Scheduler" on page 578.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Scheduler | 581

Delete Scheduler

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

To delete a scheduler:

1. Select an existing scheduler that you want to delete on the Schedulers page.
2. Click the delete icon available on the upper right side of the Schedulers page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the Schedulers Page | 577

CHAPTER 54

CoS—Scheduler Maps

IN THIS CHAPTER

About the Scheduler Maps Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

Use this page to add, edit, or delete schedulers maps configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a scheduler map. See "Add a Scheduler Map" on page 583.
- Edit a scheduler map. See "Edit a Scheduler Map" on page 584.
- Delete a scheduler map. See "Delete Scheduler Map" on page 585.

Field Descriptions

Table 165 on page 583 describes the fields on the Scheduler Maps page.

Table 165: Fields on the Scheduler Maps Page

Field	Description
Scheduler map name	Displays the names of defined scheduler maps. Scheduler maps link schedulers to forwarding classes.
Schedulers	Displays the schedulers assigned for each map.
Forwarding classes	Displays the forwarding classes assigned for each map.
Details of Schedulers	
Name	Displays the scheduler assigned to the selected scheduler map.
Value	Displays the CoS values.

RELATED DOCUMENTATION

Add a Scheduler Map | 583

Add a Scheduler Map

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

To add a scheduler map:

1. Click the add icon (**+**) available on the right side of the Scheduler Map page.
   The Add Scheduler Map page appears.
2. Complete the configuration according to the guidelines provided in Table 166 on page 584.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 166: Fields on the Add Scheduler Map Page

Field	Action
Scheduler map name	Enter a name for the scheduler map.
best-effort	Select an option from the list. Specifies no service profile. Loss priority is typically not carried in a CoS value.
expedited-forwarding	Select an option from the list. Specifies end-to-end service with low loss, low latency, low jitter, and assured bandwidth.
assured-forwarding	Select an option from the list. Specifies the group of defined values.
network-control	Select an option from the list. Specifies CoS packet forwarding class of high priority.

RELATED DOCUMENTATION

Edit a Scheduler Map | 584

Edit a Scheduler Map

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

To edit a scheduler map:

1. Select an existing scheduler map that you want to edit on the Schedulers page.
2. Click the pencil icon available on the upper right side of the Schedulers page.

   The Edit Scheduler Map page appears with editable fields. For more information on the options, see "Add a Scheduler Map" on page 583.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Scheduler Map | 585

Delete Scheduler Map

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

To delete a scheduler map:

1. Select an existing scheduler map that you want to delete on the Schedulers page.
2. Click the delete icon available on the upper right side of the Schedulers page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the Scheduler Maps Page | 582

CHAPTER 55

CoS—Drop Profile

IN THIS CHAPTER

About the Drop Profile Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

Use this page to configure drop profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a drop profile. See "Add a Drop Profile" on page 587.
- Edit a drop profile. See "Edit a Drop Profile" on page 589.
- Delete a drop profile. See "Delete Drop Profile" on page 589.

Field Descriptions

Table 167 on page 587 describes the fields on the Drop Profile page.

Table 167: Fields on the Drop Profile Page

Field	Description
Drop profile name	Displays the configured random early detection (RED) drop profile names.
Profile type	Displays whether a RED drop profile type is interpolated or segmented.
Data points	Displays information about the data point types.

RELATED DOCUMENTATION

About the Drop Profile Page | 586

Add a Drop Profile

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

To add a drop profile:

1. Click the add icon (**+**) available on the right side of the Drop Profile page.
   The Add Drop Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 168 on page 587.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 168: Fields on the Add Drop Profile Page

Field	Action
Drop Profile Name	Enter a drop profile name.

Table 168: Fields on the Add Drop Profile Page *(Continued)*

Field	Action
Interpolated	Select the option to specify whether the value pairs are interpolated to produce a smooth profile.
Segmented	Select the option to specify whether the value pairs are represented by line fragments, which connect each data point on the graph to produce a segmented profile.
Data point	To add a data point: 1. Click **+**. The Add Data Point page appears. 2. Enter the following details: • Fill Level—Enter a percentage value for queue buffer fullness for the X-coordinate. For example, 95. • Drop Probability—Enter a percentage value for drop probability for the Y-coordinate. For example, 85. 3. Click **OK** to save changes. To edit a data point: 1. Select the existing data point and click the pencil icon. The Edit Data Point page appears. 2. Enter a percentage value for Drop Probability. 3. Click **OK** to save changes. To delete a data point, select the existing data point and click the delete (**X**) icon. Then, click **Yes** to delete it.

RELATED DOCUMENTATION

Edit a Drop Profile | 589

Edit a Drop Profile

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

To edit a drop profile:

1. Select an existing drop profile that you want to edit on the Drop Profile page.
2. Click the pencil icon available on the upper right side of the Drop Profile page.

   The Edit Drop Profile page appears with editable fields. For more information on the options, see "Add a Drop Profile" on page 587.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Drop Profile | 589

Delete Drop Profile

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

To delete a drop profile:

1. Select an existing drop profile that you want to delete on the Drop Profile page.
2. Click the delete icon available on the upper right side of the Drop Profile page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the Drop Profile Page | 586

CHAPTER 56

CoS—Virtual Channel Groups

IN THIS CHAPTER

About the Virtual Channel Groups Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Virtual Channel Groups**.

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

Use this page to configure virtual channel group.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a virtual channel. See "Add a Virtual Channel" on page 591.
- Edit a virtual channel. See "Edit a Virtual Channel" on page 592.

- Delete a virtual channel. See "Delete Virtual Channel" on page 593.

Field Descriptions

Table 169 on page 591 describes the fields on the Virtual Channel Groups page.

Table 169: Fields on the Virtual Channel Groups Page

Field	Description
Virtual Channel Group Name	Displays the name of defined virtual channel groups.
Virtual Channel Name	Displays the name of defined virtual channels.
Default	Displays the default virtual channel of a group marking.
Scheduler Map	Displays the scheduler map assigned to a particular virtual channel.
Shaping Rate	Displays the shaping rate configured for a virtual channel.

RELATED DOCUMENTATION

Add a Virtual Channel | 591

Add a Virtual Channel

You are here: **Network** > **Class of Service(CoS)** > **Virtual Channel Groups**.

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

To add a virtual channel to the virtual channel group:

1. Click **Add** on the Virtual Channel page.
   The Virtual Channel Information page appears.
2. Complete the configuration according to the guidelines provided in Table 170 on page 592.

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 170: Fields on the Virtual Channel Information Page

Field	Action
Virtual Channel Name	Select a predefined name from the list or enter a new virtual channel name.
Scheduler Map	Select a scheduler map from the list. Specifies a predefined scheduler map to assign to a virtual channel. The scheduler maps associate schedulers with forwarding classes.
Shaping Rate	Enter the shaping rate for a virtual channel. Configuring a shaping rate is optional. If no shaping rate is configured, a virtual channel without a shaper can use the full logical interface bandwidth. The options available are: Select an option from the list: • Unconfigured—Select the option for no shaping rate. • Absolute Rate—Configures a shaping rate as an absolute number of bits per second. Range: 3200 through 320000000000. • Percent—Configures a shaping rate as a percentage. Range: 0 through 100.

RELATED DOCUMENTATION

Edit a Virtual Channel | 592

Edit a Virtual Channel

You are here: **Network** > **Class of Service(CoS)** > **Virtual Channel Groups**.

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

To edit a virtual channel in the virtual channel group:

1. Click on the existing virtual channel name that you want to edit on the Virtual Channel Groups page.

   The Virtual Channel Information page appears with editable fields. For more information on the options, see "Add a Virtual Channel" on page 591.
2. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Virtual Channel | 593

Delete Virtual Channel

You are here: **Network** > **Class of Service(CoS)** > **Virtual Channel Groups**.

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

To delete a virtual channel:

1. Select an existing virtual channel name that you want to delete on the Virtual Channel Groups page.
2. Click **Delete** on the Virtual Channel Groups page.

RELATED DOCUMENTATION

About the Virtual Channel Groups Page | 590

CHAPTER 57

CoS—Assign To Interface

IN THIS CHAPTER

About the Assign To Interface Page

IN THIS SECTION

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

Use this page to add, edit, or delete interface configuration.

Tasks You Can Perform

You can perform the following tasks from this page:

- Edit a port. See "Edit a Port" on page 596.
- Add a Logical Interface. See "Add a Logical Interface" on page 596.
- Edit a Logical Interface. See "Edit a Logical Interface" on page 598.

- Delete Logical Interface. See "Delete Logical Interface" on page 599.

Field Descriptions

Table 171 on page 595 describes the fields on the Assign To Interface page.

Table 171: Fields on the Assign To Interface Page

Field	Description
Port	Displays the port and interface name.
Scheduler map	Displays the predefined scheduler maps for the physical interface.
Details of Logical Interfaces	
Unit	Displays the name of a logical interface.
Forwarding class	Displays the forwarding classes assigned to a particular interface.
Scheduler map	Displays the scheduler maps assigned to a particular interface.
Virtual channel group	Displays the virtual channel groups assigned to a particular interface.
Classifier[dscp,dscpv6,exp,inet]	Displays the classifiers assigned to a particular interface—for example, information about DSCP and DSCPv6, EXP, and IPv4 (inet precedence) classifiers.
Rewrite rule[dscp,dscpv6,exp,inet]	Displays the rewrite rules assigned to a particular interface—for example, information about Differentiated Services Code Point (DSCP and DSCPv6), EXP, and IPv4 (inet precedence) rewrite rules.

RELATED DOCUMENTATION

Edit a Port | 596

Edit a Port

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To edit a port:

1. Select an existing port profile that you want to edit on the Assign To Interface page.
2. The Edit page appears with editable fields. For more information on the options, see Table 172 on page 596.
3. Click **OK** to save the changes.

Table 172: Fields on the Edit Port Page

Field	Action
Interface Name	Displays the selected interface name.
Associate system default scheduler map	Select **Associate system default scheduler map**. Specifies that you can associate the system default scheduler map with the selected interface.
Select the scheduler map	Select **Select the scheduler map** and select a value from the list. Specifies the scheduler map to the selected interface.

RELATED DOCUMENTATION

Add a Logical Interface | 596

Add a Logical Interface

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To add a logical interface:

1. Click the add icon (**+**) available on the right side of the Logical Interface page.
   The Add Logical Interface page appears.
2. Complete the configuration according to the guidelines provided in Table 173 on page 597.

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 173: Fields on the Add Logical Interface

Field	Action
Unit	Enter a logical interface name.
Scheduler map	Select a scheduler map from the list.
Forwarding class	Select a forwarding class from the list.
Virtual channel group	Select a virtual channel group from the list.
Classifiers	
dscp	Select a classifier DSCP value from the list. Specifies the Differentiated Services Code Point of the classifier type assigned to a particular interface.
dscp v6	Select a classifier DSCPv6 value from the list. Specifies the Differentiated Services Code Point version 6 of the classifier type assigned to a particular interface.
exp	Select an EXP classifier value from the list. Specifies the EXP classifier type assigned to a particular interface.
inet precedence	Select an IPv4 precedence classifier value from the list. Specifies the IPv4 precedence classifier type assigned to a particular interface.
Rewrite rules	
dscp	Select a rewrite rule DSCP value from the list. Specifies the Differentiated Services Code Point of the rewrite rule type assigned to a particular interface

Table 173: Fields on the Add Logical Interface *(Continued)*

Field	Action
dscp v6	Select a rewrite rule DSCPv6 value from the list. Specifies the Differentiated Services Code Point version 6 of the rewrite rule type assigned to a particular interface.
exp	Select an EXP rewrite rule value from the list. Specifies the EXP rewrite rule type assigned to a particular interface.
inet precedence	Select an IPv4 precedence rewrite rule value from the list. Specifies the IPv4 precedence rewrite rule type assigned to a particular interface.

RELATED DOCUMENTATION

Edit a Logical Interface | 598

Edit a Logical Interface

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To edit a logical interface:

1. Select an existing logical interface that you want to edit on the Logical Interface page.
2. Click the pencil icon available on the upper right side of the Logical Interface page.

   The Edit Logical Interface page appears with editable fields. For more information on the options, see "Add a Logical Interface" on page 596.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Logical Interface | 599

Delete Logical Interface

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To delete a logical interface:

1. Select an existing logical interface that you want to delete on the Logical Interface page.
2. Click the delete icon available on the upper right side of the Logical Interface page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

About the Assign To Interface Page | **594**

CHAPTER 58

Application QoS

IN THIS CHAPTER

About the Application QoS Page

IN THIS SECTION

You are here: **Network** > **Application QoS**.

Application quality of service (AppQoS) provides the ability to prioritize and meter application traffic to provide better service to business-critical or high-priority application traffic.

The AppQoS feature expands the capability of Junos OS class of service (CoS) to include marking DSCP values based on Layer-7 application types, honoring application-based traffic through loss priority

settings, and controlling transfer rates on egress Physical Interface Cards (PICs) based on Layer-7 application types.

Use this page to add, edit, clone, and delete an AppQoS profile and a rate limiter profile.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an AppQoS profile. See "Add an Application QoS Profile" on page 603.
- Edit an AppQoS profile. See "Edit an Application QoS Profile" on page 605.
- Clone an AppQoS profile. See "Clone an Application QoS Profile" on page 605.
- Delete AppQoS profile. See "Delete Application QoS Profile" on page 606.
- Add a rate limiter profile. See "Add a Rate Limiter Profile" on page 606.
- Edit a rate limiter profile. See "Edit a Rate Limiter Profile" on page 607.
- Clone a rate limiter profile. See "Clone a Rate Limiter Profile" on page 608.
- Delete rate limiter profile. See "Delete Rate Limiter Profile" on page 608.
- Show or hide columns in the AppQoS Profile or Rate Limiter Profile table. To do this, click Show Hide Columns icon in the top right corner of the page and select the columns you want to display or deselect to hide columns on the page.
- Advanced search for an AppQoS or rate limiter profile. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 174 on page 602 describes the fields on the Application QoS page.

Table 174: Fields on the Application QoS Page

Field	Description
AppQoS Profile	
Name	Displays the AppQoS profile name.
Traffic Direction	Displays whether the traffic direction is client-to-server and server-to-client. **NOTE**: If the same rate limiter profile is associated with client-to-server and server-to-client traffic, then **Both** status will be displayed.
Rate Limiter	Displays the rate limiter profile name.
Forwarding Class	Displays the forwarding class name.
Rate Limiter Profile	
Name	Displays the rate limiter profile name.
Maximum Bandwidth	Displays the maximum bandwidth (in Mbps) to be transmitted for the rate limiter.
Maximum Burst Size	Displays maximum burst size (in MB) to be transferred in a single burst or time-slice.
Associated AppQoS Profile	Displays the AppQoS profile name associated with the rate limiter profile.

Add an Application QoS Profile

You are here: **Network** > **Application QoS**.

To add an AppQoS profile:

1. Click the add icon **(+)** on the upper right side of the Application QoS page.

   The Add AppQoS Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 175 on page 603 through Table 176 on page 604.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 175: Fields on the Add AppQoS Profile Page

Field	Action
Name	Enter a name for the AppQoS profile. The name must be a string beginning with a letter or underscore and consisting of letters, numbers, dashes and underscores, and length should be maximum 53 characters.
Rate Limiter	
Traffic Direction	
Client to Server	Select a rate limiter from the list to be associated with client-to-server traffic for this application. Click **Add New** to add a new rate limiter profile. For more information on creating a new rate limiter, see "Add a Rate Limiter Profile" on page 606.
Server to Client	Select a rate limiter from the list to be associated with server-to-client traffic for this application. Click **Add New** to add a new rate limiter profile. For fields information, see "Add a Rate Limiter Profile" on page 606.

Table 175: Fields on the Add AppQoS Profile Page *(Continued)*

Field	Action
Action	Select one of the following actions to configure the AppQoS rules: • Drop—Drops out-of-profile packets. • Loss Priority High—Elevates the loss priority to maximum. **NOTE**: This option is not supported for SRX4600 and SRX5000 line of devices.
QoS Marking	
DSCP	Select an option from the list to mark Differentiated Services code point (DSCP) alias or bit map with matching applications to establish the output queue.
Forwarding Class	Select an option from the list to mark the AppQoS class with matching applications. Click **Add New** to add a new forwarding class. For more information in adding a new forwarding class, see Table 176 on page 604. **NOTE**: **Add New** is not supported for the logical systems and tenants. You can only select the predefined value.
Packet Loss Priority	Select an option from the list to mark loss priority with matching applications. Possible values are none, high, low, medium-high, and medium-low. A high loss priority means that there is an 80% chance of packet loss in congestion.
Logs	Enable this option to log AppQoS events.

Table 176: Fields on the Add Forwarding Class page

Field	Action
Name	Enter a name for the forwarding class.
Queue Number	Enter an output queue number to associate with the forwarding class. Range is 0 through 7.

Table 176: Fields on the Add Forwarding Class page *(Continued)*

Field	Action
Priority	Select the forwarding class queuing priority from the list.

RELATED DOCUMENTATION

- About the Application QoS Page | **600**
- Edit an Application QoS Profile | **605**
- Clone an Application QoS Profile | **605**
- Delete Application QoS Profile | **606**

Edit an Application QoS Profile

You are here: **Network** > **Application QoS**.

To edit an AppQoS profile:

1. Select an existing AppQoS profile that you want to edit on the Application QoS page.
2. Click the pencil icon available on the upper right-side of the page.

   The Edit AppQoS Profile page appears with editable fields. For more information on editing the fields, see "Add an Application QoS Profile" on page 603.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

- About the Application QoS Page | **600**
- Clone an Application QoS Profile | **605**
- Delete Application QoS Profile | **606**

Clone an Application QoS Profile

You are here: **Network** > **Application QoS**.

To clone an AppQoS profile:

1. Select an existing AppQoS profile that you want to clone on the Application QoS page.
2. Click **More** > **Clone** available on the upper right-side of the page.

   The Clone AppQoS Profile page appears with editable fields. For more information on editing the fields, see "Add an Application QoS Profile" on page 603.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

About the Application QoS Page | 600
Edit an Application QoS Profile | 605
Delete Application QoS Profile | 606

Delete Application QoS Profile

You are here: **Network** > **Application QoS**.

To delete AppQoS profiles:

1. Select one or more AppQoS profiles that you want to delete on the Application QoS page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete the selected AppQoS profiles or click **No** to retain the profiles.

RELATED DOCUMENTATION

About the Application QoS Page | 600
Add an Application QoS Profile | 603
Edit an Application QoS Profile | 605
Clone an Application QoS Profile | 605

Add a Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To add a rate limiter profile:

1. Click the add icon **(+)** on the upper right side of the Application QoS page.

   The Add Rate Limiter Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 177 on page 607.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 177: Fields on the Add Rate Limiter Profile Page

Field	Action
Name	Enter a name for the rate limiter profile. It is applied in AppQoS rules to share device resources based on quality-of-service requirements. Name must be a string beginning with a letter or underscore and consisting of letters, numbers, dashes and underscores and length should be maximum 63 characters.
Maximum Bandwidth	Enter the maximum bandwidth to be transmitted in Mbps, for this rate limiter. You can provision up to 10240 Mbps of bandwidth among multiple rate limiters to share the resource proportionally. Range is 64 kbps through 10240 Mbps.
Maximum Burst Size	Enter the maximum burst size (in MB) to be transferred in a single burst or time-slice. This limit ensures that a high-priority transmission does not keep a lower priority transmission from transmitting. Range is 1 byte through 1280 MB.

RELATED DOCUMENTATION

- About the Application QoS Page | 600
- Edit a Rate Limiter Profile | 607
- Clone a Rate Limiter Profile | 608
- Delete Rate Limiter Profile | 608

Edit a Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To edit a rate limiter profile:

1. Select an existing rate limiter profile that you want to edit on the Application QoS page.
2. Click the pencil icon available on the upper right-side of the page.

   The Edit Rate Limiter Profile page appears with editable fields. For more information on editing the fields, see "Add a Rate Limiter Profile" on page 606.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

About the Application QoS Page | 600

Clone a Rate Limiter Profile | 608

Delete Rate Limiter Profile | 608

Clone a Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To clone a rate limiter profile:

1. Select an existing rate limiter profile that you want to clone on the Application QoS page.
2. Click **More** > **Clone** available on the upper right-side of the page.

   The Clone Rate Limiter Profile page appears with editable fields. For more information on editing the fields, see "Add a Rate Limiter Profile" on page 606.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

About the Application QoS Page | 600

Edit a Rate Limiter Profile | 607

Delete Rate Limiter Profile | 608

Delete Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To delete rate limiter profiles:

1. Select one or more rate limiter profiles that you want to delete on the Application QoS page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete rate limiter profiles or click **No** to retain the profiles.

RELATED DOCUMENTATION

- About the Application QoS Page | **600**
- Add a Rate Limiter Profile | **606**
- Edit a Rate Limiter Profile | **607**
- Clone a Rate Limiter Profile | **608**

CHAPTER 59

IPsec VPN

IN THIS CHAPTER

About the IPsec VPN Page

IN THIS SECTION

You are here: **Network** > **VPN** > **IPsec VPN**.

A VPN is a private network that uses a public network to connect two or more remote sites. Instead of using dedicated connections between networks, VPNs use virtual connections routed (tunneled) through public networks. IPsec VPN is a protocol, consists of set of standards used to establish a VPN connection. Use this page to configure IPsec VPN.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure IPsec VPN global settings. See "IPsec VPN Global Settings" on page 613.
- Create a Site-to-Site VPN. See "Create a Site-to-Site VPN" on page 616.
- Create a remote access VPN. See "Create a Remote Access VPN—Juniper Secure Connect" on page 633 and "Create a Remote Access VPN—NCP Exclusive Client" on page 651.
- Edit an IPsec VPN configuration. See "Edit an IPsec VPN" on page 664.
- Delete an IPsec VPN configuration. See "Delete an IPsec VPN" on page 665.
- Show or hide columns in the IPsec VPN table. To do this, click the Show Hide Columns icon in the top right corner of the page and select the columns you want to display or deselect to hide columns on the page.
- Advance search for an IPsec VPN. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and choose a valid operator for your advanced search.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 178 on page 611 describes the fields on the IPsec VPN page.

Table 178: Fields on the IPsec VPN Page

Field	Description
Name	Displays the name of the IPsec VPN.

Table 178: Fields on the IPsec VPN Page *(Continued)*

Field	Description
IKE Status	Displays the Phase I Internet Key Exchange (IKE) status.

VPN Topology	Displays the name of the VPN topology:
	• Site to Site VPN—Connects two sites in an organization together and allows secure communications between the sites.
	• Remote Access VPN—Allows a user who is working at home or traveling to connect to the corporate office and its resources. This topology is sometimes referred to as an end-to-site tunnel.
	The options available are Remote Access VPN (Juniper Secure Connect) and Remote Access VPN (NCP Exclusive Client).
	• Other topologies which are displayed and you cannot add or edit are:
	  • Dynamic VPN—The dynamic VPN feature simplifies remote access by enabling users to create IPsec VPN tunnels without having to manually configure settings on their PCs or laptops. This feature is supported on SRX300, SRX320, SRX340, SRX345, and SRX550HM devices.
	  • Hub-and-spoke VPNs—Connects branch offices to the corporate office in an enterprise network. You can also use this topology to connect spokes together by sending traffic through the hub.
	  • ADVPN Hub—Auto Discovery VPN (ADVPN) dynamically establishes VPN tunnels between spokes to avoid routing traffic through the Hub.
	  • ADVPN Spoke—Allows the spokes to establish a shortcut tunnel between peers.

Dead Peer Detection	Displays if the dead peer detection (DPD) is enabled or disabled.
Routing Mode	Displays the name of the routing mode to send traffic to the IPsec VPN.
Remote Access	Displays the remote URL or address. **NOTE**: This option is applicable only for Remote Access VPNs (Juniper Secure Connect).

RELATED DOCUMENTATION

Create a Site-to-Site VPN | 616

Edit an IPsec VPN | 664

Delete an IPsec VPN | 665

IPsec VPN Global Settings

IN THIS SECTION

You are here: **Network** > **VPN** > **IPsec VPN**.

Use this page to view or add the VPN global configuration details. Click **Global settings** on the IPsec VPN page.

Field Descriptions

Table 179 on page 613 describes the fields on the Global Settings page.

Table 179: Fields on the Global Settings Page

Field	Description
General	
IKE - Respond to bad-spi	Enable this option if you want the device to respond to IPsec packets with invalid IPsec Security Parameter Index (SPI) values.
Max Responses	Enter a value from 1 through 30 to respond to invalid SPI values per gateway. The default is 5. This option is available when Response Bad SPI is selected.
IPsec VPN Monitor Options	Enable this option if you want the device to monitor VPN liveliness.

Table 179: Fields on the Global Settings Page *(Continued)*

Field	Description
Interval (seconds)	Enter a value from 2 through 3600 seconds after which Internet Control Message Protocol (ICMP) requests are sent to the peer.
Threshold	Enter a value from 1 through 65,536 to specify the number of consecutive unsuccessful pings before the peer is declared unreachable.
Remote Access VPN	
Default Profile Name	Select a default profile name from the list. **NOTE**: This option is available when at least one Juniper Secure Connect VPN is created.
SSL VPN Tunnel tracking	Enable this option to track Encapsulated Security Payload (ESP) tunnels.

Table 179: Fields on the Global Settings Page *(Continued)*

Field	Description
SSL VPN Profiles	Lists the SSL VPN profiles. **NOTE**: This option displays associated IPsec VPNs when at least one Juniper Secure Connect VPN is created. To add a new SSL VPN profile: **1.** Click **+**. The Add SSL VPN Profile page appears. **2.** Enter the following details: • **Name**—Enter the name for an SSL VPN profile. • **Logging**—Enable this option to log for SSL VPN. • **SSL Termination Profile**—Select an SSL termination profile from the list. To add a new SSL termination profile: **a.** Click **Add**. The Create SSL Termination Profile page appears. **b.** Enter the following details: • Name—Enter a name for the SSL termination profile. • Server Certificate—Select a server certificate from the list. To add a certificate, click **Add**. For more information on adding a device certificate, see "Add a Device Certificate" on page 235. To import a certificate, click **Import**. For more information on importing a device certificate, see "Import a Device Certificate" on page 233. • Click **OK**. **c.** Click **OK**. **3.** Click **OK**. To edit an SSL termination profile, select the profile you want to edit and click on the pencil icon.

Table 179: Fields on the Global Settings Page *(Continued)*

Field	Description
	To delete an SSL termination profile, select the profile you want to delete and click on the delete icon.
Internal SA	
Internal SA Keys	Enter the encryption key. You must ensure that the manual encryption key is in ASCII text and 24 characters long; otherwise, the configuration will result in a commit failure. **NOTE**: This option is available only for SRX5000 line of devices, SRX4100, SRX4200, SRX4600 devices, and vSRX.

RELATED DOCUMENTATION

- About the IPsec VPN Page | **610**
- Edit an IPsec VPN | **664**
- Delete an IPsec VPN | **665**

Create a Site-to-Site VPN

You are here: **Network** > **VPN** > **IPsec VPN**.

To create a site-to-site VPN:

1. Click **Create VPN** and select **Site to Site** on the upper right side of the IPsec VPN page.

   The Create Site to Site VPN page appears.
2. Complete the configuration according to the guidelines provided in Table 180 on page 617 through Table 185 on page 627.

   The VPN connectivity will change from grey to blue line in the topology to show that the configuration is complete.
3. Click **Save** to save the changes.

   If you want to discard your changes, click **Cancel**.

Table 180: Fields on the Create IPsec VPN Page

Field	Action
Name	Enter a name for the VPN.
Description	Enter a description. This description will be used for the IKE and IPsec proposals and policies. During edit, the IPsec policy description will be displayed and updated.
Routing Mode	Select the routing mode to which this VPN will be associated: • Traffic Selector (Auto Route Insertion) • Static Routing • Dynamic Routing – OSPF • Dynamic Routing – BGP For each topology, J-Web auto generates the relevant CLIs. Traffic Selector is the default mode.

Table 180: Fields on the Create IPsec VPN Page *(Continued)*

Field	Action
Authentication Method	Select an authentication method from the list that the device uses to authenticate the source of Internet Key Exchange (IKE) messages: • Certificate Based—Types of digital signatures, which are certificates that confirm the identity of the certificate holder. The following are the authentication methods for a certificate based: • rsa-signatures—Specifies that a public key algorithm, which supports encryption and digital signatures, is used. • dsa-signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ecdsa-signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ecdsa-signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used. • ecdsa-signatures-521—Specifies that the ECDSA using the 521-bit elliptic curve secp521r1 is used. **NOTE**: ecdsa-signatures-521 supports only SRX5000 line of devices with SPC3 card and junos-ike package installed. • Pre-shared Key (default method)—Specifies that a preshared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. This is the default method.

Table 180: Fields on the Create IPsec VPN Page *(Continued)*

Field	Action
Auto-create Firewall Policy	If you select **Yes**, a firewall policy is automatically between internal zone and tunnel interface zone with local protected networks as source address and remote protected networks as destination address. Another firewall policy will be created visa-versa. If you choose **No**, you don't have a firewall policy option. You need to manually create the required firewall policy to make this VPN work. **NOTE**: If you do not want to auto-create a firewall policy in the VPN workflow, then the protected network is hidden for dynamic routing in both local and remote gateway.
Remote Gateway	Displays the remote gateway icon in the topology. Click the icon to configure the remote gateway. The gateway identifies the remote peer with the IPsec VPN peers and defines the appropriate parameters for that IPsec VPN. For fields information, see Table 181 on page 620.
Local Gateway	Displays the local gateway icon in the topology. Click the icon to configure the local gateway. For fields information, see Table 183 on page 622.

Table 180: Fields on the Create IPsec VPN Page *(Continued)*

Field	Action
IKE and IPsec Settings	Configure the custom IKE or IPsec proposal and the custom IPsec proposal with recommended algorithms or values. For fields information, see Table 185 on page 627. **NOTE**: • J-Web supports only one custom IKE proposal and does not support the predefined proposal-set. Upon edit and save, J-Web deletes the predefined proposal set if configured. • On the remote gateway of the VPN tunnel, you must configure the same custom proposal and policy. • Upon edit, J-Web shows the first custom IKE and IPsec proposal when more than one custom proposal is configured.

Table 181: Fields on the Remote Gateway Page

Field	Action
Gateway is behind NAT	If enabled, the configured external IP address (IPv4 or IPv6) is referred to as the NAT device IP address.
IKE Identity	Select an option from the list to configure remote identity.
Host name	Enter a remote host name.
IPv4 Address	Enter a remote IPv4 address.
IPv6 Address	Enter a remote IPv6 address.

Table 181: Fields on the Remote Gateway Page *(Continued)*

Field	Action
Key ID	Enter a Key ID.
E-mail Address	Enter an e-mail address.
External IP Address	Enter the peer IPv4 or IPv6 address. You can create one primary peer network with up to four backups. You must enter one IPv4 or IPv6 address or you can enter up to five IP addresses separated by comma.

Protected Networks	When you select a routing mode, lists all the global address(es).
	
	Select the addresses from the Available column and then click the right arrow to move it to the Selected column.
	
	When the routing mode is:
	
	• Traffic Selector—The IP addresses will be used as remote IP in traffic selector configuration.
	
	• Static Routing:
	
	  • Static route will be configured for the selected global address(es).
	
	  • The tunnel interface (st0.x) of the local gateway will be used as the next-hop.
	
	• Dynamic Routing—Default value is **any**. You can also select specific global address(es). The selected value is configured as destination address in the firewall policy.

Add	Click **+**. The Create Global Address page appears. See Table 182 on page 622 for fields information.

Table 182: Fields on the Create Global Address Page

Field	Action
Name	Enter a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
IP Type	Select IPv4 or IPv6.
IPv4	IPv4 Address—Enter a valid IPv4 address. Subnet—Enter the subnet for IPv4 address.
IPv6	IPv6 Address—Enter a valid IPv6 address. Subnet Prefix—Enter a subnet mask for the network range. Once entered, the value is validated.

Table 183: Fields on the Local Gateway Page

Field	Action
Gateway is behind NAT	Enable this option when the local gateway is behind a NAT device.
IKE Identity	Select an option from the list to configure local identity. When **Gateway is behind NAT** is enabled, you can configure an IPv4 or IPv6 address to reference the NAT device.
Host name	Enter a host name. **NOTE**: This option is available only if **Gateway is behind NAT** is disabled.
IPv4 Address	Enter an IPv4 address.

Table 183: Fields on the Local Gateway Page *(Continued)*

Field	Action
IPv6 Address	Enter an IPv6 address.
Key ID	Enter a Key ID. **NOTE**: This option is available only if **Gateway is behind NAT** is disabled.
E-mail Address	Enter an E-mail address. **NOTE**: This option is available only if **Gateway is behind NAT** is disabled.
External Interface	Select an outgoing interface from the list for IKE negotiations. The list contains all available IP addresses if more than one IP address is configured to the specified interface. The selected IP address will be configured as the local address under the IKE gateway.
Tunnel Interface	Select an interface from the list to bind it to the tunnel interface (route-based VPN). Click **Add** to add a new interface. The Create Tunnel Interface page appears. See Table 184 on page 627.
Router ID	Enter the routing device's IP address. **NOTE**: This option is available if the routing mode is Dynamic Routing - OSPF or BGP.
Area ID	Enter an area ID within the range of 0 to 4,294,967,295, where the tunnel interfaces of this VPN need to be configured. **NOTE**: This option is available if the routing mode is Dynamic Routing - OSPF.

Table 183: Fields on the Local Gateway Page *(Continued)*

Field	Action
Tunnel Interface Passive	Enable this option to bypass traffic of the usual active IP checks. **NOTE**: This option is available if the routing mode is Dynamic Routing - OSPF.
ASN	Enter the routing device's AS number. Use a number assigned to you by the NIC. Range: 1 through 4,294,967,295 (232 – 1) in plain-number format for 4-byte AS numbers. **NOTE**: This option is available if the routing mode is Dynamic Routing - BGP.
Neighbor ID	Enter IP address of a neighboring router. **NOTE**: This option is available if the routing mode is Dynamic Routing - BGP.
BGP Group Type	Select the type of BGP peer group from the list: • external—External group, which allows inter-AS BGP routing. • internal—Internal group, which allows intra-AS BGP routing. **NOTE**: This option is available if the routing mode is Dynamic Routing - BGP.
Peer ASN	Enter the neighbor (peer) autonomous system (AS) number. **NOTE**: This option is available if you choose **external** as BGP Group Type.

Table 183: Fields on the Local Gateway Page *(Continued)*

Field	Action
Import Policies	Select one or more routing policies from the list to routes being imported into the routing table from BGP. Click **Clear All** to clear the selected polices. **NOTE**: This option is available if the routing mode is Dynamic Routing - BGP.
Export Policies	Select one or more policies from the list to routes being exported from the routing table into BGP. Click **Clear All** to clear the selected polices. **NOTE**: This option is available if the routing mode is Dynamic Routing - BGP.
Local certificate	Select a local certificate identifier when the local device has multiple loaded certificates. **NOTE**: This option is available if the authentication method is Certificate Based. Click **Add** to generate a new certificate. Click **Import** to import a device certificate. For more information see Manage Device Certificates.
Trusted CA/Group	Select the certificate authority (CA) profile from list to associate it with the local certificate. **NOTE**: This option is available if the authentication method is Certificate Based. Click **Add** to add a new CA profile. For more information see Manage Trusted Certificate Authority.

Table 183: Fields on the Local Gateway Page *(Continued)*

Field	Action
Pre-shared Key	Enter the value of the preshared key. The key can be one of the following: • ascii-text—ASCII text key. • hexadecimal—Hexadecimal key. **NOTE**: This option is available if the authentication method is Pre-shared Key.
Protected Networks	Click **+**. The Create Protected Networks page appears.
Create Protected Networks	
Zone	Select a security zone from the list that will be used as a source zone in the firewall policy.
Global Address	Select the addresses from the Available column and then click the right arrow to move it to the Selected column.
Add	Click **Add**. The Create Global Address page appears. See Table 182 on page 622.
Edit	Select the protected network you want to edit and click on the pencil icon. The Edit Global Address page appears with editable fields.
Delete	Select the protected network you want to edit and click on the delete icon. The confirmation message pops up. Click **Yes** to delete.

Table 184: Fields on the Create Tunnel Interface Page

Field	Action
Interface Unit	Enter the logical unit number.
Description	Enter a description for the logical interface.
Zone	Select a zone for the logical interface from the list to use as a source zone in the firewall policy. Click **Add** to add a new zone. Enter zone name and description and click **OK** on the Create Security Zone page.
Routing Instance	Select a routing instance from the list.
IPv4 **NOTE**: This option is available only if you select routing mode as Dynamic Routing - OSPF or BGP.	
IPv4 Address	Enter a valid IPv4 address.
Subnet Prefix	Enter a subnet mask for the IPv4 address.
IPv6 **NOTE**: This option is available only if you select routing mode as Dynamic Routing - OSPF or BGP.	
IPv6 Address	Enter a valid IPv6 address.
Subnet Prefix	Enter a subnet mask for the network range. Once entered, the value is validated.

Table 185: IKE and IPsec Settings

Field	Action
IKE Settings	

Table 185: IKE and IPsec Settings *(Continued)*

Field	Action
IKE Version	Select the required IKE version, either v1 or v2 to negotiate dynamic security associations (SAs) for IPsec. Default value is v2.
IKE Mode	Select the IKE policy mode from the list: • aggressive—Take half the number of messages of main mode, has less negotiation power, and does not provide identity protection. • main—Use six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.
Encryption Algorithm	Select the appropriate encryption mechanism from the list. Default value is aes-256-gcm.
Authentication Algorithm	Select the authentication algorithm from the list. For example, hmac-md5-96—Produces a 128-bit digest and hmac-sha1-96—Produces a 160-bit digest. **NOTE**: This option is available when the encryption algorithm is not gcm.
DH group	A Diffie-Hellman (DH) exchange allows participants to generate a shared secret value. Select the appropriate DH group from the list. Default value is group19.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). Default: 28,800 seconds. Range: 180 through 86,400 seconds.
Dead Peer Detection	Enable this option to send dead peer detection requests regardless of whether there is outgoing IPsec traffic to the peer.

Table 185: IKE and IPsec Settings *(Continued)*

Field	Action
DPD Mode	Select one of the options from the list: • optimized—Send probes only when there is outgoing traffic and no incoming data traffic - RFC3706 (default mode). • probe-idle-tunnel—Send probes same as in optimized mode and also when there is no outgoing and incoming data traffic. • always-send—Send probes periodically regardless of incoming and outgoing data traffic.
DPD Interval	Select an interval in seconds to send dead peer detection messages. The default interval is 10 seconds. Range is 2 to 60 seconds.
DPD Threshold	Select a number from 1 to 5 to set the failure DPD threshold. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times.
Advance Configuration (Optional)	
General IKE ID	Enable this option to accept peer IKE ID.
IKEv2 Re-authentication	Configure the reauthentication frequency to trigger a new IKEv2 reauthentication.
IKEv2 Re-fragmentation	This option is enabled by default.
IKEv2 Re-fragment Size	Select the maximum size, in bytes, of an IKEv2 message before it is split into fragments. The size applies to both IPv4 and IPv6 messages. Range: 570 to 1320 bytes. Default values are: • IPv4 messages—576 bytes. • IPv6 messages—1280 bytes.

Table 185: IKE and IPsec Settings *(Continued)*

Field	Action
NAT-T	Enable this option for IPsec traffic to pass through a NAT device. NAT-T is an IKE phase 1 algorithm that is used when trying to establish a VPN connection between two gateway devices, where there is a NAT device in front of one of the SRX Series devices.
NAT Keep Alive	Select appropriate keepalive interval in seconds. Range: 1 to 300. If the VPN is expected to have large periods of inactivity, you can configure keepalive values to generate artificial traffic to keep the session active on the NAT devices.
IPsec Settings	
Protocol	Select either Encapsulation Security Protocol (ESP) or Authentication Header (AH) protocol from the list to establish VPN. Default value is ESP.
Encryption Algorithm	Select the encryption method. Default value is aes-256-gcm. **NOTE**: This option is available only for the ESP protocol.
Authentication Algorithm	Select the IPsec authentication algorithm from the list. For example, hmac-md5-96—Produces a 128-bit digest and hmac-sha1-96—Produces a 160-bit digest. **NOTE**: This option is available when the encryption algorithm is not gcm.
Perfect Forward Secrecy	Select Perfect Forward Secrecy (PFS) from the list. The device uses this method to generate the encryption key. Default value is group19. PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security, but require more processing time. **NOTE**: group15, group16, and group21 support only the SRX5000 line of devices with an SPC3 card and junos-ike package installed.
Lifetime Seconds	Select the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated. Default is 3,600 seconds. Range: 180 through 86,400 seconds.

Table 185: IKE and IPsec Settings *(Continued)*

Field	Action
Lifetime Kilobytes	Select the lifetime (in kilobytes) of an IPsec SA. Default is 128kb. Range: 64 through 4294967294.
Establish Tunnel	Enable this option to establish the IPsec tunnel. IKE is activated immediately (default value) after a VPN is configured and the configuration changes are committed.
Advanced Configuration	
VPN Monitor	Enable this option to use it in a destination IP address. **NOTE**: This option is not available for Traffic Selectors routing mode.
Destination IP	Enter the destination of the Internet Control Message Protocol (ICMP) pings. The device uses the peer's gateway address by default. **NOTE**: This option is not available for Traffic Selectors routing mode.
Optimized	Enable this option for the VPN object. If enabled, the SRX Series device only sends ICMP echo requests (pings) when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series device considers the tunnel to be active and does not send pings to the peer. This option is disabled by default. **NOTE**: This option is not available for Traffic Selectors routing mode.
Source Interface	Select the source interface for ICMP requests from the list. If no source interface is specified, the device automatically uses the local tunnel endpoint interface. **NOTE**: This option is not available for Traffic Selectors routing mode.
Verify-path	Enable this option to verify the IPsec datapath before the secure tunnel (st0) interface is activated and route(s) associated with the interface are installed in the Junos OS forwarding table. This option is disabled by default. **NOTE**: This option is not available for Traffic Selectors routing mode.

Table 185: IKE and IPsec Settings *(Continued)*

Field	Action
Destination IP	Enter the destination IP address. Original, untranslated IP address of the peer tunnel endpoint that is behind a NAT device. This IP address must not be the NAT translated IP address. This option is required if the peer tunnel endpoint is behind a NAT device. The verify-path ICMP request is sent to this IP address so that the peer can generate an ICMP response. **NOTE**: This option is not available for Traffic Selectors routing mode.
Packet size	Enter the size of the packet that is used to verify an IPsec datapath before the st0 interface is brought up. Range: 64 to 1350 bytes. Default value is 64 bytes. **NOTE**: This option is not available for Traffic Selectors routing mode.
Anti Replay	IPsec protects against VPN attack by using a sequence of numbers built into the IPsec packet—the system does not accept a packet with the same sequence number. This option is enabled by default. The Anti-Replay checks the sequence numbers and enforce the check, rather than just ignoring the sequence numbers. Disable Anti-Replay if there is an error with the IPsec mechanism that results in out-of-order packets, which prevents proper functionality.
Install Interval	Select the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device. Select a value from 1 to 10.
Idle Time	Select the idle time interval. The sessions and their corresponding translations time out after a certain period of time if no traffic is received. Range is 60 to 999999 seconds.
DF Bit	Select how the device handles the Don't Fragment (DF) bit in the outer header: • clear—Clear (disable) the DF bit from the outer header. This is the default. • copy—Copy the DF bit to the outer header. • set—Set (enable) the DF bit in the outer header.

Table 185: IKE and IPsec Settings *(Continued)*

Field	Action
Copy Outer DSCP	This option enabled by default. This enables copying of Differentiated Services Code Point (DSCP) (outer DSCP+ECN) from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. Enabling this feature, after IPsec decryption, clear text packets can follow the inner CoS (DSCP+ECN) rules.

RELATED DOCUMENTATION

- About the IPsec VPN Page | **610**
- IPsec VPN Global Settings | **613**
- Edit an IPsec VPN | **664**
- Delete an IPsec VPN | **665**

Create a Remote Access VPN—Juniper Secure Connect

You are here: **Network** > **VPN** > **IPsec VPN**.

Juniper Secure Connect is Juniper's client-based SSL-VPN solution that offers secure connectivity for your network resources.

Juniper Secure Connect provides secure remote access for the users to connect to the corporate networks and resources remotely using the Internet. Juniper Secure Connect downloads the configuration from SRX Services devices and chooses the most effective transport protocols during connection establishment to deliver a great administrator and user experience.

To create a remote access VPN for Juniper secure connect:

1. Choose **Create VPN** > **Remote Access** > **Juniper Secure Connect** on the upper right-side of the IPsec VPN page.

   The Create Remote Access (Juniper Secure Connect) page appears.
2. Complete the configuration according to the guidelines provided in Table 186 on page 634 through Table 191 on page 647.

   The VPN connectivity will change from grey to blue line in the topology to show that the configuration is complete.

3. Click **Save** to complete Secure Connect VPN Configuration and associated policy if you have selected the auto policy creation option.

   If you want to discard your changes, click **Cancel**.

Table 186: Fields on the Create Remote Access (Juniper Secure Connect) Page

Field	Action
Name	Enter a name for the remote access connection. This name will be displayed as the end users realm name in the Juniper Secure Connect Client.
Description	Enter a description. This description will be used for the IKE and IPsec proposals, policies, remote access profile, client configuration, and NAT rule set. During edit the IPsec policy description will be displayed. IPsec policy and remote access profile descriptions will be updated.
Routing Mode	This option is disabled for the remote access. Default mode is Traffic Selector (Auto Route Insertion).
Authentication Method	Select an authentication method from the list that the device uses to authenticate the source of Internet Key Exchange (IKE) messages: • Pre-shared Key (default method)—Specifies that a preshared key, which is a secret key shared between the two peers, is used during authentication to identify the peers with each other. The same key must be configured for each peer. This is the default method. • Certificate Based—Specifies the type of digital signatures, which are certificates that confirm the identity of the certificate holder. The supported signature is rsa-signatures. rsa-signatures specifies that a public key algorithm, which supports encryption and digital signatures, is used.

Table 186: Fields on the Create Remote Access (Juniper Secure Connect) Page *(Continued)*

Field	Action
Auto-create Firewall Policy	If you select **Yes**, a firewall policy is automatically created between internal zone and tunnel interface zone with local protected networks as source address and remote protected networks as destination address. Another firewall policy will be created visa-versa. If you choose **No**, you don't have a firewall policy option. You need to manually create the required firewall policy to make this VPN work. **NOTE**: If you do not want to auto-create a firewall policy in the VPN workflow, then the protected network is hidden for dynamic routing in both local and remote gateway.
Remote User	Displays the remote user icon in the topology. Click the icon to configure the Juniper Secure Connect client settings. For more information on the fields, see Table 187 on page 636. **NOTE**: The J-Web UI displays the remote user's URL once local gateway is configured.
Local Gateway	Displays the local gateway icon in the topology. Click the icon to configure the local gateway. For more information on the fields, see Table 188 on page 641.

Table 186: Fields on the Create Remote Access (Juniper Secure Connect) Page *(Continued)*

Field	Action
IKE and IPsec Settings	Configure the custom IKE or IPsec proposal and the custom IPsec proposal with recommended algorithms or values. For more information on the fields, see Table 191 on page 647. **NOTE**: • J-Web supports only one custom IKE proposal and does not support the predefined proposal-set. Upon edit and save, J-Web deletes the predefined proposal set if configured. • On the remote gateway of the VPN tunnel, you must configure the same custom proposal and policy. • Upon edit, J-Web shows the first custom IKE and IPsec proposal when more than one custom proposal is configured.

Table 187: Fields on the Remote User Page

Field	Action
Default Profile	Enable this option to use the configured VPN name as remote access default profile. **NOTE**: • This option is not available if the default profile is configured. • You must enable the default profile. If not enabled, configure the default profile under **VPN** > **IPsec VPN** > **Global Settings** > **Remote Access VPN**.

Table 187: Fields on the Remote User Page *(Continued)*

Field	Action
Connection Mode	Select one of the following options from the list to establish the Juniper Secure Connect client connection: • **Manual**—You need manually connect to the VPN tunnel every time you log in. • **Always**—You are automatically connected to the VPN tunnel every time you log in. The default connection mode is Manual.
SSL VPN	Enable this option to establish SSL VPN connection from the Juniper Secure Connect Client to the SRX Series device. By default, this option is enabled. **NOTE**: This is a fallback option when IPsec ports are not reachable.
Biometric authentication	Enable this option to authenticate the client system using unique configured methods. An authentication prompt is displayed when you connect in the client system. The VPN connection will only be initiated after successful authentication through the method configured for *Windows Hello* (fingerprint recognition, face recognition, PIN entry, and so on). *Windows Hello* must be preconfigured on the client system if the Biometric authentication option is enabled.

Table 187: Fields on the Remote User Page *(Continued)*

Field	Action
Dead Peer Detection	Enable the dead peer detection (DPD) option to allow the Juniper Secure Connect client to detect if the SRX Series device is reachable. Disable this option to allow the Juniper Secure Connect client to detect till the SRX Series device connection reachability is restored. This option is enabled by default.
DPD Interval	Enter the amount of time that the peer waits for traffic from its destination peer before sending a dead-peer-detection (DPD) request packet. The Range is 2 through 60 seconds and default is 60 seconds.
DPD Threshold	Enter the maximum number of unsuccessful dead peer detection (DPD) requests to be sent before the peer is considered unavailable. The Range is 1 through 5 and default is 5.
Certificates	Enable Certificates to configure certificate options on Secure Client Connect. **NOTE**: This option is available only if you select the Certificate Based authentication method.
Expiry Warning	Enable this option to display the certificate expiry warning on the Secure Connect Client. This option is enabled by default. **NOTE**: This option is available only if you enable Certificates.

Table 187: Fields on the Remote User Page *(Continued)*

Field	Action
Warning Interval	Enter the interval (days) at which the warning to be displayed. Range is 1 through 90. Default value is 60. **NOTE**: This option is available only if you enable Certificates.
Pin Req Per Connection	Enable this option to enter the certificate pin on very connection. This option is enabled by default. **NOTE**: This option is available only if you enable Certificates.
EAP-TLS	Enable this option for the authentication process. IKEv2 requires EAP for user authentication. SRX Series device cannot act as an EAP server. An external RADIUS server must be used for IKEv2 EAP to do the EAP authentication. SRX will act as a pass-through authenticator relaying EAP messages between the Juniper Secure Connect client and the RADIUS server. This option is enabled by default. **NOTE**: This option is available only if you select the Certificate Based authentication method.
Windows Logon	Enable this option to provide users to securely log on to the Windows domain before logging on to the Windows system. The client supports domain logon using a credential service provider after establishing a VPN connection to the company network.
Domain Name	Enter the system domain name on to which the Users Machine logs.

Table 187: Fields on the Remote User Page *(Continued)*

Field	Action
Mode	Select one of the following options from the list to log on to Windows domain. • **Manual**—You must manually enter your logon data on the Windows logon screen. • **Automatic**—The client software transfers the data entered here to the Microsoft logon interface (Credential Provider) without your action.
Disconnect at Logoff	Enable this option to shut down the connection when the system switches to hibernation or standby mode. When the system resumes from hibernation or standby mode the connection has to be re-established.
Flush Credential at Logoff	Enable this option to delete username and password from the cache. You must reenter the username and password.
Lead Time Duration	Enter the lead time duration to initialize time between network logon and domain logon. After the connection is set up, the Windows logon will only be executed after the initialization time set here has elapsed.
EAP Authentication	Enable this option to execute EAP authentication prior to the destination dialog in the credential provider. Then, system will ask for the necessary PIN, regardless of whether EAP will be required for subsequent dial-in. If this option is disabled, then EAP authentication will be executed after the destination selection.

Table 187: Fields on the Remote User Page *(Continued)*

Field	Action
Auto Dialog Open	Enable this option to select whether a dialog should open automatically for connection establishment to a remote domain. If this option is disabled, then the password and PIN for the client will only be queried after the Windows logon.

Table 188: Fields on the Local Gateway Page

Field	Action
Gateway is behind NAT	Enable this option when the local gateway is behind a NAT device.
NAT IP Address	Enter the public (NAT) IP address of the SRX Series device. **NOTE**: This option is available only when **Gateway is behind NAT** is enabled. You can configure an IPv4 address to reference the NAT device.
IKE ID	This field is mandatory. Enter the IKE ID in the format user@example.com.
External Interface	Select an outgoing interface from the list for which the client will connect to. The list contains all available IP addresses if more than one IPv4 address is configured to the specified interface. The selected IP address will be configured as the local address under the IKE gateway.

Table 188: Fields on the Local Gateway Page *(Continued)*

Field	Action
Tunnel Interface	Select an interface from the list for the client to connect to. Click **Add** to add a new interface. The Create Tunnel Interface page appears. For more information on creating a new tunnel interface, see Table 189 on page 646. Click **Edit** to edit the selected tunnel interface.
Pre-shared Key	Enter one of the following values of the preshared key: • ascii-text—ASCII text key. • hexadecimal—Hexadecimal key. **NOTE**: This option is available if the authentication method is Pre-shared Key.
Local certificate	Select a local certificate from the list. Local certificate lists only the RSA certificates. To add a certificate, click **Add**. For more information on adding a device certificate, see "Add a Device Certificate" on page 235. To import a certificate, click **Import**. For more information on importing a device certificate, see "Import a Device Certificate" on page 233. **NOTE**: This option is available if the authentication method is Certificated Based.

Table 188: Fields on the Local Gateway Page *(Continued)*

Field	Action
Trusted CA/Group	Select a trusted Certificate Authority/group profile from the list. To add a CA profile, click **Add CA Profile**. For more information on adding a CA profile, see "Add a Certificate Authority Profile" on page 248. **NOTE**: This option is available if the authentication method is Certificated Based.
User Authentication	This field is mandatory. Select the authentication profile from the list that will be used to authenticate user accessing the remote access VPN. Click **Add** to create a new Profile. For more information on creating a new access profile, see "Add an Access Profile" on page 966.

Table 188: Fields on the Local Gateway Page *(Continued)*

Field	Action
SSL VPN Profile	Select the SSL VPN Profile from the list that will be used to terminate the remote access connections. To create a new SSL VPN profile: 1. Click **Add**. 2. Enter the following details: • Name—Enter the name for an SSL VPN profile. • Logging—Enable this option to log for SSL VPN. • SSL Termination Profile—Select an SSL termination profile from the list. To add a new SSL termination profile: a. Click **Add**. The Create SSL Termination Profile page appears. b. Enter the following details: • Name—Enter a name for the SSL termination profile. • Server Certificate—Select a server certificate from the list. To add a certificate, click **Add**. For more information on adding a device certificate, see "Add a Device Certificate" on page 235. To import a certificate, click **Import**. For more information on importing a device certificate, see "Import a Device Certificate" on page 233.

Table 188: Fields on the Local Gateway Page *(Continued)*

Field	Action
	• Click **OK**. c. Click **OK**. 3. Click **OK**.
Source NAT Traffic	This option is enabled by default. All traffic from the Juniper Secure Connect client is NATed to the selected interface by default. If disabled, you must ensure that you have a route from your network pointing to the SRX Series devices for handling the return traffic correctly.
Interface	Select an interface from the list through which the source NAT traffic pass through.
Protected Networks	Click **+**. The Create Protected Networks page appears.
Create Protected Networks	
Zone	Select a security zone from the list that will be used as a source zone in the firewall policy.
Global Address	Select the addresses from the Available column and then click the right arrow to move it to the Selected column. Click **Add** to select the networks the Client can connect to. The Create Global Address page appears. For more information on the fields, see Table 190 on page 647.

Table 188: Fields on the Local Gateway Page *(Continued)*

Field	Action
Edit	Select the protected network you want to edit and click on the pencil icon. The Edit Protected Networks page appears with editable fields.
Delete	Select the protected network you want to edit and click on the delete icon. The confirmation message pops up. Click **Yes** to delete the protected network.

Table 189: Fields on the Create Tunnel Interface Page

Field	Action
Interface Unit	Enter the logical unit number.
Description	Enter a description for the logical interface.
Zone	Select a zone from the list to add it to the tunnel interface. This zone is used in the auto-creation of the firewall policy. Click **Add** to add a new zone. Enter zone name and description and click **OK** on the Create Security Zone page.
Routing Instance	Select a routing instance from the list. **NOTE**: The default routing instance, primary, refers to the main inet.0 routing table in the logical system.

Table 190: Fields on the Create Global Address Page

Field	Action
Name	Enter a name for the global address. The name must be a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
IP Type	Select **IPv4**.
IPv4	
IPv4 Address	Enter a valid IPv4 address.
Subnet	Enter the subnet for IPv4 address.

Table 191: IKE and IPsec Settings

Field	Action
IKE Settings **NOTE**: The following parameters are generated automatically and are not displayed in the J-Web UI: • If the authentication method is Pre-Shared Key, the IKE version is v1, ike-user-type is shared-ike-id, and mode is Aggressive. • If the authentication method is Certificate Based, the IKE version is v2, ike-user-type is shared-ike-id, and mode is Main.	
Encryption Algorithm	Select the appropriate encryption mechanism from the list. Default value is AES-CBC 256-bit.
Authentication Algorithm	Select the authentication algorithm from the list. For example, SHA 256-bit.
DH group	A Diffie-Hellman (DH) exchange allows participants to generate a shared secret value. Select the appropriate DH group from the list. Default value is group19.

Table 191: IKE and IPsec Settings *(Continued)*

Field	Action
Lifetime Seconds	Select a lifetime duration (in seconds) of an IKE security association (SA). Default value is 28,800 seconds. Range: 180 through 86,400 seconds.
Dead Peer Detection	Enable this option to send dead peer detection requests regardless of whether there is outgoing IPsec traffic to the peer.
DPD Mode	Select one of the options from the list: • optimized—Send probes only when there is outgoing traffic and no incoming data traffic - RFC3706 (default mode). • probe-idle-tunnel—Send probes same as in optimized mode and also when there is no outgoing and incoming data traffic. • always-send—Send probes periodically regardless of incoming and outgoing data traffic.
DPD Interval	Select an interval (in seconds) to send dead peer detection messages. The default interval is 10 seconds. Range is 2 to 60 seconds.
DPD Threshold	Select a number from 1 to 5 to set the failure DPD threshold. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times.
Advance Configuration (Optional)	
NAT-T	Enable this option for IPsec traffic to pass through a NAT device. NAT-T is an IKE phase 1 algorithm that is used when trying to establish a VPN connection between two gateway devices, where there is a NAT device in front of one of the SRX Series devices.
NAT Keep Alive	Select appropriate keepalive interval in seconds. Range: 1 to 300. If the VPN is expected to have large periods of inactivity, you can configure keepalive values to generate artificial traffic to keep the session active on the NAT devices.

Table 191: IKE and IPsec Settings *(Continued)*

Field	Action
IKE Connection Limit	Enter the number of concurrent connections that the VPN profile supports. Range is 1 through 4294967295. When the maximum number of connections is reached, no more remote access user (VPN) endpoints attempting to access an IPsec VPN can begin Internet Key Exchange (IKE) negotiations.
IKEv2 Fragmentation	This option is enabled by default. IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level. Fragmentation takes place before the original message is encrypted and authenticated, so that each fragment is separately encrypted and authenticated. **NOTE**: This option is available if the authentication method is Certificated Based.
IKEv2 Fragment Size	Select the maximum size, in bytes, of an IKEv2 message before it is split into fragments. The size applies to IPv4 message. Range: 570 to 1320 bytes. Default value is 576 bytes. **NOTE**: This option is available if the authentication method is Certificated Based.
IPsec Settings **NOTE**: The authentication method is Pre-Shared Key or Certificate Based, it automatically generates protocol as ESP.	
Encryption Algorithm	Select the encryption method. Default value is AES-GCM 256-bit.
Authentication Algorithm	Select the IPsec authentication algorithm from the list. For example, HMAC-SHA-256-128. **NOTE**: This option is available when the encryption algorithm is not gcm.

Table 191: IKE and IPsec Settings *(Continued)*

Field	Action
Perfect Forward Secrecy	Select Perfect Forward Secrecy (PFS) from the list. The device uses this method to generate the encryption key. Default value is group19. PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security, but require more processing time. **NOTE**: group15, group16, and group21 support only the SRX5000 line of devices with an SPC3 card and junos-ike package installed.
Lifetime Seconds	Select the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated. Default is 3,600 seconds. Range: 180 through 86,400 seconds.
Lifetime Kilobytes	Select the lifetime (in kilobytes) of an IPsec SA. Default is 256kb. Range: 64 through 4294967294.
Advanced Configuration	
Anti Replay	IPsec protects against VPN attack by using a sequence of numbers built into the IPsec packet—the system does not accept a packet with the same sequence number. This option is enabled by default. The Anti-Replay checks the sequence numbers and enforce the check, rather than just ignoring the sequence numbers. Disable Anti-Replay if there is an error with the IPsec mechanism that results in out-of-order packets, which prevents proper functionality.
Install Interval	Select the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device. Select a value from 1 to 10 seconds.
Idle Time	Select the idle time interval. The sessions and their corresponding translations time out after a certain period of time if no traffic is received. Range is 60 to 999999 seconds.

Table 191: IKE and IPsec Settings *(Continued)*

Field	Action
DF Bit	Select how the device handles the Don't Fragment (DF) bit in the outer header: • clear—Clear (disable) the DF bit from the outer header. This is the default. • copy—Copy the DF bit to the outer header. • set—Set (enable) the DF bit in the outer header.
Copy Outer DSCP	This option enabled by default. This enables copying of Differentiated Services Code Point (DSCP) (outer DSCP+ECN) from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. Enabling this feature, after IPsec decryption, clear text packets can follow the inner CoS (DSCP+ECN) rules.

RELATED DOCUMENTATION

About the IPsec VPN Page | 610

IPsec VPN Global Settings | 613

Edit an IPsec VPN | 664

Delete an IPsec VPN | 665

Create a Remote Access VPN—NCP Exclusive Client

You are here: **Network** > **VPN** > **IPsec VPN**.

The NCP Exclusive Remote Access Client is part of the NCP Exclusive Remote Access solution for Juniper SRX Series Gateways. The VPN client is only available with NCP Exclusive Remote Access Management. Use the NCP Exclusive Client to establish secure, IPsec-based data links from any location when connected with SRX Series Gateways.

To create a remote access VPN for Juniper secure connect:

1. Choose **Create VPN** > **Remote Access** > **NCP Exclusive Client** on the upper right-side of the IPsec VPN page.

   The Create Remote Access (NCP Exclusive Client) page appears.

2. Complete the configuration according to the guidelines provided in Table 192 on page 652 through Table 196 on page 660.

   The VPN connectivity will change from grey to blue line in the topology to show that the configuration is complete.

3. Click **Save** to save the changes.

   If you want to discard your changes, click **Cancel**.

Table 192: Fields on the Create Remote Access (NCP Exclusive Client) Page

Field	Action
Name	Enter a name for the remote access connection. This name will be displayed as the end users connection name in the NCP exclusive client.
Description	Enter a description. This description will be used for the IKE and IPsec proposals, policies, remote access profile, client configuration, and NAT rule set. During edit the IPsec policy description will be displayed. IPsec policy and remote access profile descriptions will be updated.
Routing Mode	This option is disabled for the remote access. Default mode is Traffic Selector (Auto Route Insertion).

Table 192: Fields on the Create Remote Access (NCP Exclusive Client) Page *(Continued)*

Field	Action
Authentication Method	Select an authentication method from the list that the device uses to authenticate the source of Internet Key Exchange (IKE) messages: • Pre-shared Key (default method)—Specifies that a preshared key, which is a secret key shared between the two peers, is used during authentication to identify the peers with each other. The same key must be configured for each peer. This is the default method. • Certificate Based—Types of digital signatures, which are certificates that confirm the identity of the certificate holder. The supported signature is rsa-signatures. rsa-signatures specifies that a public key algorithm, which supports encryption and digital signatures, is used.
Auto-create Firewall Policy	If you select **Yes**, a firewall policy is automatically created between internal zone and tunnel interface zone with local protected networks as source address and remote protected networks as destination address. Another firewall policy will be created visa-versa. If you choose **No**, you don't have a firewall policy option. You need to manually create the required firewall policy to make this VPN work. **NOTE**: If you do not want to auto-create a firewall policy in the VPN workflow, then the protected network is hidden for dynamic routing in both local and remote gateway.
Remote User	Displays the remote user icon in the topology. This option is disabled.

Table 192: Fields on the Create Remote Access (NCP Exclusive Client) Page *(Continued)*

Field	Action
Local Gateway	Displays the local gateway icon in the topology. Click the icon to configure the local gateway. For more information on the fields, see Table 193 on page 654.
IKE and IPsec Settings	Configure the custom IKE or IPsec proposal and the custom IPsec proposal with recommended algorithms or values. For more information on the fields, see Table 196 on page 660. **NOTE**: • J-Web supports only one custom IKE proposal and does not support the predefined proposal-set. Upon edit and save, J-Web deletes the predefined proposal set if configured. • On the remote gateway of the VPN tunnel, you must configure the same custom proposal and policy. • Upon edit, J-Web shows the first custom IKE and IPsec proposal when more than one custom proposal is configured.

Table 193: Fields on the Local Gateway Page

Field	Action
Gateway is behind NAT	Enable this option when the local gateway is behind a NAT device.

Table 193: Fields on the Local Gateway Page *(Continued)*

Field	Action
NAT IP Address	Enter the public (NAT) IP address of the SRX Series device. **NOTE**: This option is available only when **Gateway is behind NAT** is enabled. You can configure an IPv4 address to reference the NAT device.
IKE ID	This field is mandatory. Enter the IKE ID in the format user@example.com.
External Interface	Select an outgoing interface from the list for which the client will connect to. The list contains all available IP addresses if more than one IPv4 address is configured to the specified interface. The selected IP address will be configured as the local address under the IKE gateway.
Tunnel Interface	Select an interface from the list for the client to connect to. Click **Add** to add a new interface. The Create Tunnel Interface page appears. For more information on creating a new tunnel interface, see Table 194 on page 659. Click **Edit** to edit the selected tunnel interface.
Pre-shared Key	Enter one of the following values of the preshared key: • ascii-text—ASCII text key. • hexadecimal—Hexadecimal key. **NOTE**: This option is available if the authentication method is Pre-shared Key.

Table 193: Fields on the Local Gateway Page *(Continued)*

Field	Action
Local certificate	Select a local certificate from the list. Local certificate lists only the RSA certificates. To add a certificate, click **Add**. For more information on adding a device certificate, see "Add a Device Certificate" on page 235. To import a certificate, click **Import**. For more information on importing a device certificate, see "Import a Device Certificate" on page 233. **NOTE**: This option is available if the authentication method is Certificated Based.
Trusted CA/Group	Select a trusted Certificate Authority/group profile from the list. To add a CA profile, click **Add CA Profile**. For more information on adding a CA profile, see "Add a Certificate Authority Profile" on page 248. **NOTE**: This option is available if the authentication method is Certificated Based.
User Authentication	This field is mandatory. Select the authentication profile from the list that will be used to authenticate user accessing the remote access VPN. Click **Add** to create a new Profile. For more information on creating a new access profile, see "Add an Access Profile" on page 966.

Table 193: Fields on the Local Gateway Page *(Continued)*

Field	Action
SSL VPN Profile	Select the SSL VPN Profile from the list that will be used to terminate the remote access connections. To create a new SSL VPN profile: 1. Click **Add**. 2. Enter the following details: • Name—Enter the name for an SSL VPN profile. • Logging—Enable this option to log for SSL VPN. • SSL Termination Profile—Select an SSL termination profile from the list. To add a new SSL termination profile: a. Click **Add**. b. Enter the following details: • Name—Enter a name for the SSL termination profile. • Server Certificate—Select a server certificate from the list. To add a certificate, click **Add**. For more information on adding a device certificate, see "Add a Device Certificate" on page 235. To import a certificate, click **Import**. For more information on importing a device certificate, see "Import a Device Certificate" on page 233. • Click **OK**. c. Click **OK**. 3. Click **OK**.

Table 193: Fields on the Local Gateway Page *(Continued)*

Field	Action
Source NAT Traffic	This option is enabled by default. All traffic from the Juniper Secure Connect client is NATed to the selected interface by default. If disabled, you must ensure that you have a route from your network pointing to the SRX Series devices for handling the return traffic correctly.
Interface	Select an interface from the list through which the source NAT traffic pass through.
Protected Networks	Click **+**. The Create Protected Networks page appears.
Create Protected Networks	
Zone	Select a security zone from the list that will be used as a source zone in the firewall policy.
Global Address	Select the addresses from the Available column and then click the right arrow to move it to the Selected column. Click **Add** to select the networks the Client can connect to. The Create Global Address page appears. For more information on the fields, see Table 195 on page 659.
Edit	Select the protected network you want to edit and click on the pencil icon. The Edit Protected Networks page appears with editable fields.

Table 193: Fields on the Local Gateway Page *(Continued)*

Field	Action
Delete	Select the protected network you want to edit and click on the delete icon. The confirmation message pops up. Click **Yes** to delete the protected network.

Table 194: Fields on the Create Tunnel Interface Page

Field	Action
Interface Unit	Enter the logical unit number.
Description	Enter a description for the logical interface.
Zone	Select a zone from the list to add it to the tunnel interface. This zone is used in the auto-creation of the firewall policy. Click **Add** to add a new zone. Enter zone name and description and click **OK** on the Create Security Zone page.
Routing Instance	Select a routing instance from the list. **NOTE**: The default routing instance, primary, refers to the main inet.0 routing table in the logical system.

Table 195: Fields on the Create Global Address Page

Field	Action
Name	Enter a name for the global address. The name must be a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.

Table 195: Fields on the Create Global Address Page *(Continued)*

Field	Action
IP Type	Select **IPv4**.
IPv4	
IPv4 Address	Enter a valid IPv4 address.
Subnet	Enter the subnet for IPv4 address.

Table 196: IKE and IPsec Settings

Field	Action
IKE Settings **NOTE**: The following parameters are generated automatically and are not displayed in the J-Web UI: • If the authentication method is Pre-Shared Key, the IKE version is 1, ike-user-type is shared-ike-id, and mode is Aggressive. • If the authentication method is Certificate Based, the IKE version is 2, ike-user-type is group-ike-id, and mode is Main.	
Encryption Algorithm	Select the appropriate encryption mechanism from the list. Default value is AES-CBC 256-bit.
Authentication Algorithm	Select the authentication algorithm from the list. For example, SHA 256-bit.
DH group	A Diffie-Hellman (DH) exchange allows participants to generate a shared secret value. Select the appropriate DH group from the list. Default value is group19.
Lifetime Seconds	Select a lifetime duration (in seconds) of an IKE security association (SA). Default value is 28,800 seconds. Range: 180 through 86,400 seconds.

Table 196: IKE and IPsec Settings *(Continued)*

Field	Action
Dead Peer Detection	Enable this option to send dead peer detection requests regardless of whether there is outgoing IPsec traffic to the peer.
DPD Mode	Select one of the options from the list: • optimized—Send probes only when there is outgoing traffic and no incoming data traffic - RFC3706 (default mode). • probe-idle-tunnel—Send probes same as in optimized mode and also when there is no outgoing and incoming data traffic. • always-send—Send probes periodically regardless of incoming and outgoing data traffic.
DPD Interval	Select an interval (in seconds) to send dead peer detection messages. The default interval is 10 seconds. Range is 2 to 60 seconds.
DPD Threshold	Select a number from 1 to 5 to set the failure DPD threshold. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times.
Advance Configuration (Optional)	
NAT-T	Enable this option for IPsec traffic to pass through a NAT device. NAT-T is an IKE phase 1 algorithm that is used when trying to establish a VPN connection between two gateway devices, where there is a NAT device in front of one of the SRX Series devices.
NAT Keep Alive	Select appropriate keepalive interval in seconds. Range: 1 to 300. If the VPN is expected to have large periods of inactivity, you can configure keepalive values to generate artificial traffic to keep the session active on the NAT devices.

Table 196: IKE and IPsec Settings *(Continued)*

Field	Action
IKE Connection Limit	Enter the number of concurrent connections that the VPN profile supports. Range is 1 through 4294967295. When the maximum number of connections is reached, no more remote access user (VPN) endpoints attempting to access an IPsec VPN can begin Internet Key Exchange (IKE) negotiations.
IKEv2 Fragmentation	This option is enabled by default. IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level. Fragmentation takes place before the original message is encrypted and authenticated, so that each fragment is separately encrypted and authenticated. **NOTE**: This option is available if the authentication method is Certificated Based.
IKEv2 Fragment Size	Select the maximum size, in bytes, of an IKEv2 message before it is split into fragments. The size applies to IPv4 message. Range: 570 to 1320 bytes. Default value is 576 bytes. **NOTE**: This option is available if the authentication method is Certificated Based.
IPsec Settings	
Encryption Algorithm	Select the encryption method. Default value is AES-GCM 256-bit.
Authentication Algorithm	Select the IPsec authentication algorithm from the list. For example, HMAC-SHA-256-128. **NOTE**: This option is available when the encryption algorithm is not gcm.

Table 196: IKE and IPsec Settings *(Continued)*

Field	Action
Perfect Forward Secrecy	Select Perfect Forward Secrecy (PFS) from the list. The device uses this method to generate the encryption key. Default value is group19. PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security, but require more processing time. **NOTE**: group15, group16, and group21 support only the SRX5000 line of devices with an SPC3 card and junos-ike package installed.
Lifetime Seconds	Select the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated. Default is 3,600 seconds. Range: 180 through 86,400 seconds.
Lifetime Kilobytes	Select the lifetime (in kilobytes) of an IPsec SA. Default is 256kb. Range: 64 through 4294967294.
Advanced Configuration	
Anti Replay	IPsec protects against VPN attack by using a sequence of numbers built into the IPsec packet—the system does not accept a packet with the same sequence number. This option is enabled by default. The Anti-Replay checks the sequence numbers and enforce the check, rather than just ignoring the sequence numbers. Disable Anti-Replay if there is an error with the IPsec mechanism that results in out-of-order packets, which prevents proper functionality.
Install Interval	Select the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device. Select a value from 1 to 10.
Idle Time	Select the idle time interval. The sessions and their corresponding translations time out after a certain period of time if no traffic is received. Range is 60 to 999999 seconds.

Table 196: IKE and IPsec Settings *(Continued)*

Field	Action
DF Bit	Select how the device handles the Don't Fragment (DF) bit in the outer header: • clear—Clear (disable) the DF bit from the outer header. This is the default. • copy—Copy the DF bit to the outer header. • set—Set (enable) the DF bit in the outer header.
Copy Outer DSCP	This option enabled by default. This enables copying of Differentiated Services Code Point (DSCP) (outer DSCP+ECN) from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. Enabling this feature, after IPsec decryption, clear text packets can follow the inner CoS (DSCP+ECN) rules.

RELATED DOCUMENTATION

About the IPsec VPN Page | **610**

IPsec VPN Global Settings | **613**

Edit an IPsec VPN | **664**

Delete an IPsec VPN | **665**

Edit an IPsec VPN

You are here: **Network** > **VPN** > **IPsec VPN**.

You can edit any of the following IPsec VPNs:

- Site-to-Site VPN
- Remote Access VPN (Juniper Secure Connect)
- Remote Access VPN (NCP Exclusive Client)

To edit IPsec VPN:

NOTE:

- When the IKE status is up and if you edit the IPsec VPN, the topology diagram is shown in green.
- All local gateway protected networks will form traffic selectors with all remote gateway protected networks and vice-versa.

1. Select an existing IPsec VPN configuration that you want to edit on the IPsec VPN page.
2. Click the pencil icon available on the upper right-side of the page.

   The edit page for the selected IPsec VPN page appears with editable fields. You can modify any previous changes done to Site-to-Site VPN, Remote Access VPN (Juniper Secure Connect), and Remote Access VPN (NCP Exclusive Client).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

NOTE:

- During edit, Auto-create Firewall Policy and Gateway behind NAT options are not supported. Gateway behind NAT is supported only for remote access VPN.
- The Source NAT Traffic option is only supported when creating remote access VPN. During edit, this option is not supported.
- For Site-to-Site VPN, when the routing mode is Traffic Selector, the traffic selector creates the complete mesh between the local and remote addresses.

RELATED DOCUMENTATION

Create a Site-to-Site VPN | 616

Create a Remote Access VPN—Juniper Secure Connect | 633

Create a Remote Access VPN—NCP Exclusive Client | 651

Delete an IPsec VPN | 665

Delete an IPsec VPN

You are here: **Network** > **VPN** > **IPsec VPN**.

You can delete any of the VPN topologies.

To delete any IPsec VPN configurations:

1. Select existing an IPsec VPN configuration(s) that you want to delete on the IPsec VPN page.
2. Click the delete icon available on the upper right-side of the page.

   The Confirm Delete window appears.

   NOTE:

   - For Site-to-Site VPN, only the associated IPsec VPN routing configuration such as static route or OSPF is deleted.
   - Remote Access VPN default profile will be deleted only if the deleting VPN is configured as default profile. You need to configure the default profile under **VPN** > **IPsec VPN** > **Global Settings** > **Remote Access VPN**.

3. Click **Yes** to delete or click **No** to retain the configuration.

RELATED DOCUMENTATION

About the IPsec VPN Page | **610**

IPsec VPN Global Settings | **613**

Create a Site-to-Site VPN | **616**

Edit an IPsec VPN | **664**

CHAPTER 60

Manual Key VPN

IN THIS CHAPTER

About the Manual Key VPN Page

IN THIS SECTION

You are here: **Network** > **VPN** > **Manual Key VPN**.

Use this page to configure manual key VPN.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a manual key VPN. See "Add a Manual Key VPN" on page 668.
- Edit a manual key VPN. See "Edit a Manual Key VPN" on page 671.
- Delete a manual key VPN. See "Delete Manual Key VPN" on page 672.

Field Descriptions

Table 197 on page 668 describes the fields on the Manual Key VPN page.

Table 197: Fields on the Manual Key VPN Page

Field	Description
Name	Displays the name of the manual tunnel.
Gateway	Displays the selected gateway.
Bind Interface	Displays the tunnel interface to which the route-based VPN is bound.
Df Bit	Displays the DF bit in the outer header.

RELATED DOCUMENTATION

- Add a Manual Key VPN | 668
- Edit a Manual Key VPN | 671
- Delete Manual Key VPN | 672

Add a Manual Key VPN

You are here: **Network** > **VPN** > **Manual Key VPN**.

To add a manual key VPN:

1. Click the add icon (**+**) on the upper right side of the Manual Key VPN page.
   The Add Manual Key VPN page appears.
2. Complete the configuration according to the guidelines provided in Table 198 on page 669.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 198: Fields on the Manual Key VPN Configuration Page

Field	Action
VPN Manual Key	
VPN Name	Enter the VPN name for the IPsec tunnel.
Remote Gateway	Enter the name for the remote gateway.
External Interface	Select an interface from the list.
Protocol	Select an option from the list to specify the types of protocols available for configuration: • ESP • AH
SPI	Enter a SPI value. Range: 256 through 16639.
Bind to tunnel interface	Select an interface from the list to which the route-based VPN is bound.
Do not fragment bit	Select an option from the list to specify how the device handles the DF bit in the outer header. • **clear**—Clear (disable) the DF bit from the outer header. This is the default. • **Set**—Set the DF bit to the outer header. • **copy**—Copy the DF bit to the outer header.
Enable VPN Monitor	Select this option to configure VPN monitoring.
Destination IP	Enter an IP address for the destination peer.

Table 198: Fields on the Manual Key VPN Configuration Page *(Continued)*

Field	Action
Optimized	Select the check box to enable optimization for the device to use traffic patterns as evidence of peer liveliness. If enabled, ICMP requests are suppressed. This feature is disabled by default.
Source Interface	Enter a source interface for ICMP requests (VPN monitoring “hellos”). If no source interface is specified, the device automatically uses the local tunnel endpoint interface.
Key Values	
Authentication	
Algorithm	Specifies the hash algorithm that authenticates packet data. Select a hash algorithm from the list: • **hmac-md5-96**—Produces a 128-bit digest. • **hmac-sha1-96**—Produces a 160-bit digest. • **hmac-sha-256-128**
ASCII Text	Select the **ASCII Text** option, and enter the key in the appropriate format.
Hexadecimal	Select the **Hexadecimal** option, and enter the key in the appropriate format.
Encryption	
Encryption	Specifies the supported Internet Key Exchange (IKE) proposals. Select an option from the list: • **3des-cbc**—3DES-CBC encryption algorithm. • **aes-128-cbc**—AES-CBC 128-bit encryption algorithm. • **aes-192-cbc**—AES-CBC 192-bit encryption algorithm. • **aes-256-cbc**—AES-CBC 256-bit encryption algorithm. • **des-cbc**—DES-CBC encryption algorithm.

Table 198: Fields on the Manual Key VPN Configuration Page *(Continued)*

Field	Action
ASCII Text	Enable this option and enter the key in the appropriate format.
Hexadecimal	Enable this option and enter the key in the appropriate format.

RELATED DOCUMENTATION

- About the Manual Key VPN Page | **667**
- Edit a Manual Key VPN | **671**
- Delete Manual Key VPN | **672**

Edit a Manual Key VPN

You are here: **Network** > **VPN** > **Manual Key VPN**.

To edit a manual key VPN:

1. Select the existing manual key VPN that you want to edit on the Manual Key VPN page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit a Manual Key VPN page appears with editable fields. For more information on the options, see "Add a Manual Key VPN" on page 668.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Manual Key VPN Page | **667**
- Add a Manual Key VPN | **668**
- Delete Manual Key VPN | **672**

Delete Manual Key VPN

You are here: **Network** > **VPN** > **Manual Key VPN**.

To delete a manual key VPN:

1. Select a manual key VPN that you want to delete on the Manual Key VPN page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Manual Key VPN Page | **667**
- Add a Manual Key VPN | **668**
- Edit a Manual Key VPN | **671**

CHAPTER 61

Dynamic VPN

IN THIS CHAPTER

About the Dynamic VPN Page

IN THIS SECTION

You are here: **Network** > **VPN** > **Dynamic VPN**.

You can view and add, edit, or delete dynamic VPN global configuration options.

NOTE: This menu is available only for SRX300 line of devices and SRX550M devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure global settings. See "Global Settings" on page 675.
- Add DVPN IPsec template. See "IPsec Template" on page 677.
- Add a dynamic VPN. See "Add a Dynamic VPN" on page 678.
- Edit a dynamic VPN. See "Edit a Dynamic VPN" on page 679.
- Delete dynamic VPN. See "Delete Dynamic VPN" on page 680.
- Launch VPN wizard. To do this, click Launch Wizard available on the upper right corner of the Dynamic VPN table. Follow the guided steps to configure the VPN wizard.

Field Descriptions

Table 199 on page 674 describes the fields on the Dynamic VPN page.

Table 199: Fields on the Dynamic VPN Page

Field	Description
Access Profile	Select a previously created access profile from the list displayed in Global Settings. Specify the access profile to use for Extended Authentication for remote users trying to download the Access Manager. **NOTE**: This Access Profile option does not control authentication for VPN sessions. For more information, see Add a Gateway and Add a VPN.
Client VPNs	Create a client configuration for the dynamic VPN feature.
Name	Enter a name for dynamic VPN.
User	Enter an username. Specifies the list of users who can use this client configuration.
IP Address	Enter an IP address and netmask for the users.
IPsec VPN	Select a previously configured IKE AutoKey configuration from the list.

Table 199: Fields on the Dynamic VPN Page *(Continued)*

Field	Description
Remote Protected Resources	Enter an IP address and netmask of a resource behind the firewall. Traffic to the specified resource will go through the VPN tunnel and therefore will be protected by the firewall's security policies.

RELATED DOCUMENTATION

- Global Settings | 675
- Edit a Dynamic VPN | 679
- Delete Dynamic VPN | 680

Global Settings

You are here: **VPN** > **Dynamic VPN**.

To add global settings:

1. Click **Global Settings** on the upper right side of the Resource Profiles page.
   The DVPN - Global Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 200 on page 675.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 200: Fields on the Global Settings page

Field	Action
Access Profile	Select an access profile from the list to use for Extended Authentication for remote users trying to download the Access Manager.
Address Profile Settings	
Address Pool	Select an address pool from the list

Table 200: Fields on the Global Settings page *(Continued)*

Field	Action
+	Click **+** to add a new address pool. The New Address Pool page appears.
New Address Pool	
Name	Enter a name for address pool.
Network Address	Enter the network prefix for the address pool for IPv4 or IPv6 addresses.
Address Ranges	
+	Click **+** to add the address range for DVPN.
Address Range Name	Enter an address range name.
Lower Limit	Enter the lower boundary for the IPv4 or IPv6 address range.
High Limit	Enter the upper boundary for the IPv4 or IPv6 address range.
X	Click **X** to delete the address ranges of DVPN.
XAUTH Attributes	
Primary DNS Sever	Enter the primary DNS IP address.
Secondary DNS Sever	Enter the secondary DNS IP address.
Primary WINS Sever	Enter the primary WINS IP address.
Secondary WINS Sever	Enter the secondary WINS IP address.

RELATED DOCUMENTATION

About the Dynamic VPN Page | 673
IPsec Template | 677
Add a Dynamic VPN | 678

IPsec Template

You are here: **VPN** > **Dynamic VPN**.

To add a dynamic VPN IPsec template:

1. Click **IPsec Template** on the upper right side of the Dynamic VPN page.
   The DVPN IPsec Template page appears.
2. Complete the configuration according to the guidelines provided in Table 201 on page 677.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 201: Fields on the DVPN IPsec Template Page

Field	Action
Clone IPsec from DVPN template	
Name	Displays the name of the cloned DVPN template.
Preshared Key	Enter the authorization key.
IKE ID	Specify the IKE IDs for the DVPN.
External Interface	Select the external interface from the list.

RELATED DOCUMENTATION

About the Dynamic VPN Page | 673
Global Settings | 675
Add a Dynamic VPN | 678

Add a Dynamic VPN

You are here: **Network** > **VPN** > **Dynamic VPN**.

To add a dynamic VPN:

1. Click the add icon (**+**) on the upper right side of the Dynamic VPN page.
   The Add DVPN page appears.
2. Complete the configuration according to the guidelines provided in Table 202 on page 678.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 202: Fields on the DVPN Page

Field	Action
Name	Enter the name of the client configuration.
IPsec VPN	Select a previously configured IKE AutoKey configuration from the list to use when establishing the VPN tunnel.
Access Users	
Local Users in Profile	Specifies the list of users who can use this client configuration. Select the users and click on the arrow button to move to copy to DVPN. **NOTE**: The server does not validate the names that you enter here, but the names must be the names that the users use to log in to the device when downloading the client.
Users in DVPN	Specifies the list of users copied from the local users in profile or the newly added users.
Username	Enter a username.
Password	Enter a password for the username.

Table 202: Fields on the DVPN Page *(Continued)*

Field	Action
IP	Enter an IP address for the user.
+	Click **+** and select **Add to DVPN** or **Add to Both** to add the user to either in Users in DVPN or to both DVPN and Local Users in Profile.
Remote Protected Resources	Enter an IP address and net mask and click **+**. Specifies the IP address and net mask of a resource behind the firewall. Traffic to the specified resource will go through the VPN tunnel and therefore will be protected by the firewall's security policies. **NOTE**: The device does not validate that the IP/net mask combination that you enter here matches up with your security policies.
Remote Exceptions	Enter an IP address and net mask and click **+**. Specifies the IP address and net mask of exceptions to the remote protected resources list.

RELATED DOCUMENTATION

- About the Dynamic VPN Page | **673**
- Edit a Dynamic VPN | **679**
- Delete Dynamic VPN | **680**

Edit a Dynamic VPN

You are here: **Network** > **VPN** > **Dynamic VPN**.

To edit a dynamic VPN setting:

1. Select the existing a dynamic VPN settings policy that you want to edit on the Dynamic VPN page.
2. Click the pencil icon available on the upper right side of the page.

The Edit DVPN page appears with editable fields. For more information on the options, see "Add a Dynamic VPN" on page 678.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Dynamic VPN Page | **673**
- Global Settings | **675**
- IPsec Template | **677**
- Add a Dynamic VPN | **678**

Delete Dynamic VPN

You are here: **Network** > **VPN** > **Dynamic VPN**.

To delete a dynamic VPN:

1. Select a dynamic VPN policy that you want to delete on the Dynamic VPN page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Dynamic VPN Page | **673**
- Global Settings | **675**
- IPsec Template | **677**
- Add a Dynamic VPN | **678**
- Edit a Dynamic VPN | **679**

7

PART

Security Policies and Objects

CHAPTER 62

Security Policies

IN THIS CHAPTER

About the Security Policies Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Security Policies**.

Use this page to get a high-level view of your firewall policy rules settings. The security policy applies the security rules to the transit traffic within a context (from-zone to to-zone). The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database in the data plane.

Using a global policy, you can regulate traffic with addresses and applications, regardless of their security zones, by referencing user-defined addresses or the predefined address “any.” These addresses can span multiple security zones.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add Global Options. See "Global Options" on page 687.
- Add a Rule. See "Add a Rule" on page 690.
- Edit a Rule. See "Edit a Rule" on page 707.
- Clone a Rule. See "Clone a Rule" on page 706.
- Delete a Rule. See "Delete Rules" on page 707.
- To save the rules configuration, click **Save**.
- To delete the rules configuration, click **Discard**.
- Drag and drop the rules within a zone context. To do this, select the rule you want to place in a different sequence number within a zone context, drag and drop it using the cursor.

  NOTE: If you drag and drop a rule outside the zone context, J-Web will display a warning message that you cannot move the rule into another zone context.

- Advanced search for policy rule. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

  3. Press Enter to display the search results in the grid.

  The supported search scenarios and its examples are as follows:

1. Logical operators:

   - AND operator for multiple parameters

     Example: Name = Rule1 AND Dynamic Application = Malware

   - OR operator for same and different parameters

     Example for same parameters: Name = Rule1 OR Name = Rule2

     Example for different parameters: Name = Rule1 OR Dynamic Application = Malware

   - Combination of AND and OR operators

     Example: Name = Rule1 AND (Dynamic Application = Malware OR Action = Reject)

   - Comma (,) separated value

     Example: Name = Rule1, Rule2

   - != operator for single parameter

     Example: Name != Rule1

2. Dynamic applications or service objects with matching characters of *Junos*

   When you search for the matching characters of Junos, such as, jun, un, nos, and os, the result displays all the matched objects but without junos prefix. For example, if the configured dynamic application is *junos:01NET*, the search for dynamic applications with *jun* characters display only *01NET*.

3. Saved policy rules

   When you add or edit a rule, click **Save** to save the configuration. To search for this saved configuration, you must wait for the device to synchronize the configuration.

- Show or hide columns in the policy rule table. To do this, click Show Hide Columns icon in the top right corner of the policy rule table and select the columns you want to display or deselect the columns you want to hide on the page.

Table 203 on page 685 describes few more options on Rules.

Table 203: More Options on the Security Policies Page

Field	Description
Create Rule Before	Adds a new rule before the selected rule. To add a new rule before the selected rule: 1. Select an existing rule before which you want to create a rule. 2. Click **More** > **Create Rule Before**. Alternatively, you can right-click on the selected rule and select **Create Rule Before**. **NOTE**: • When you create a new rule, it inherits the name, source zone, and destination zone same as parent (selected) rule. Source address and destination address will be any and the action will be Deny. • For global policy, source zone and destination zone will not be available. 3. Click tick mark to create the new rule.
Create Rule After	Adds a new rule after the selected rule. To add a new rule after the selected rule: 1. Select an existing rule after which you want to create a rule. 2. Click **More** > **Create Rule After**. Alternatively, you can right-click on the selected rule and select **Create Rule After**. **NOTE**: • When you create a new rule, it inherits the name, source zone, and destination zone same as parent (selected) rule. Source address and destination address will be any and the action will be Deny. • For global policy, source zone and destination zone will not be available. 3. Click tick mark to create the new rule.
Clone	Clones or copies the selected firewall policy configuration and enables you to update the details of the rule.
Clear All	Clears the selection of those rules that are selected.

Field Descriptions

Table 204 on page 686 describes the fields on the Security Policies page.

NOTE: On the Security Policies page:

- For logical systems and tenants, the URL Categories option will not be displayed.
- For tenants, the Dynamic Application option will not be displayed.

Table 204: Fields on the Security Policies Page

Field	Description
Seq	Displays the sequence number of rules in a zone pair.
Hits	Displays the number of hits the rule has encountered.
Rule Name	Displays the rule name. You can hover over the name column to view the rule name and its description.
Source Zone	Displays the source zone that is specified in the zone pair for the rule.
Source Address	Displays the name of the source address or address set for the rule.
Source Identity	Displays the user identity of the rule.
Destination Zone	Displays the destination zone that is specified in the zone pair for the rule.
Destination Address	Displays the name of the destination address or address set for the rule.
Dynamic Application	Displays the dynamic application names for match criteria in application firewall rule set. An application firewall configuration permits, rejects, or denies traffic based on the application of the traffic.

Table 204: Fields on the Security Policies Page *(Continued)*

Field	Description
Services	Displays the type of service for the destination of the rule.
URL Category	Displays the URL category that you want to match criteria for web filtering category.
Action	Displays the actions that need to take place on the traffic as it passes through the firewall.
Advanced Security	Displays the security option that apply for this rule.
Rule Options	Displays the rule option while permitting the traffic.
Schedule	Displays the scheduler details that allow a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active.

RELATED DOCUMENTATION

Global Options | 687

Global Options

You are here: **Security Policies & Objects** > **Security Policies**.

To add global options:

1. Click **Global Options** available on the upper right side of the Security Policies page.
   The Global Options page appears.
2. Complete the configuration according to the guidelines provided in Table 205 on page 688.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 205 on page 688 describes the fields on the Global Options page.

Table 205: Fields on the Global Options Page

Field	Action
Pre-id Default Policy	
Session Timeout	
ICMP	Enter the timeout value for ICMP sessions ranging from 4 through 86400 seconds.
ICMP6	Enter the timeout value for ICMP6 sessions ranging from 4 through 86400 seconds.
OSPF	Enter the timeout value for OSPF sessions ranging from 4 through 86400 seconds.
TCP	Enter the timeout value for TCP sessions ranging from 4 through 86400 seconds.
UDP	Enter the timeout value for UDP sessions ranging from 4 through 86400 seconds.
Others	Enter the timeout value for other sessions ranging from 4 through 86400 seconds.
Logging	
Session Initiate	Enable this option to start logging at the beginning of a session. **WARNING**: Configuring session-init logging for the pre-id-default-policy can generate a large number of logs.
Session Close	Enable this option to start logging at the closure of a session. **NOTE**: Configuring session-close logging ensures that the SRX Series Firewall generates the security logs if a flow is unable to leave the pre-id-default-policy.
Flow	
Aggressive Session Aging **NOTE**: This option is not supported for logical systems and tenants.	

Table 205: Fields on the Global Options Page *(Continued)*

Field	Action
Early Ageout	Enter a value from 1 through 65,535 seconds. The default value is 20 seconds. Specifies the amount of time before the device aggressively ages out a session from its session table.
Low watermark	Enter a value from 0 through 100 percent. The default value is 100 percent. Specifies the percentage of session table capacity at which the aggressive aging-out process ends.
High watermark	Enter a value from 0 through 100 percent. The default value is 100 percent. Specifies the percentage of session table capacity at which the aggressive aging-out process begins.
SYN Flood Protection	
SYN Flood Protection	Enable this option to defend against SYN attacks.
Mode	Select one of the following options: • **Cookie**—Uses a cryptographic hash to generate a unique Initial Sequence Number (ISN). This is enabled by default. • **Proxy**—Uses a proxy to handle the SYN attack.
TCP MSS	
All TCP Packets	Enter a maximum segment size value from 64 through 65,535 to override all TCP packets for network traffic.
Packets entering IPsec Tunnel	Enter a maximum segment size value from 64 through 65,535 bytes to override all packets entering an IPsec tunnel. The default value is 1320 bytes.
GRE Packets entering IPsec Tunnel	Enter a maximum segment size value from 64 through 65,535 bytes to override all generic routing encapsulation packets entering an IPsec tunnel. The default value is 1320 bytes.

Table 205: Fields on the Global Options Page *(Continued)*

Field	Action
GRE Packets exiting IPsec Tunnel	Enter a maximum segment size value from 64 through 65,535 bytes to override all generic routing encapsulation packets exiting an IPsec tunnel. The default value is 1320 bytes.
TCP Session	
Sequence number check	By default, this option is enabled to check sequence numbers in TCP segments during stateful inspections. The device monitors the sequence numbers in TCP segments.
SYN flag check	By default, this option is enabled to check the TCP SYN bit before creating a session. The device checks that the SYN bit is set in the first packet of a session. If it is not set, the device drops the packet.

RELATED DOCUMENTATION

Add a Rule | 690

Add a Rule

You are here: **Security Policies & Objects** > **Security Policies**.

NOTE: To reference the UTM policies and the AppQoS profiles in a security policy rules, create UTM polices and AppQoS profiles before creating or editing security policy rules if required. To create UTM policies, go to **Security Services** > **UTM** > **UTM Policies** and to create AppQoS profiles, go to **Network** > **Application QoS**.

To add a rule:

1. Click the add icon (**+**) on the upper right side of the Security Policies page.
   The inline editable fields will appear.
2. Complete the configuration according to the guidelines provided in Table 206 on page 691.
3. Click the tick icon on the right-side of the row once done with the configuration.

NOTE: Scroll back the horizontal bar if the inline tick and the cancel icons are not available when creating a new rule.

4. Click **Save** to save the changes or click **Discard** to discard the changes.

NOTE: You must perform Step 3 and Step 4 before performing any further actions in the J-Web UI.

Table 206: Fields on the Security Policies Page

Field	Action
Rule Name	Enter a name for the new rule or policy.
Rule Description	Enter a description for the security policy.
Global Policy	Enable this option to specify that the policy defined is a global policy and zones are not required.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
Source Zone	To add sources: 1. Click **+**. The Select Sources page appears. 2. Enter the following details: • **Zone**—Select the source zone from the list to which you want the rule to be associated. • **Addresses**—Select **any** or **Specific**. **NOTE**: • Starting in Juons OS Release 21.4R1, you can select the IP feeds to define the matching criteria for a policy. Also, you can view source type (Address, Address group, Wild card, Range, IP feeds) in the new Type column. • Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, `request services security-intelligence download`. To select a specific address or IP feed, select the addresses or IP feeds from the Available column and then click the right arrow to move it to the Selected column. You can select **Exclude Selected** to exclude only the selected address from the list. To create a new address, click **+**. The Create Address page appears. For more information on fields, see Table 207 on page 701. • **Source identity**—Select the user identity from the Available column and then click the right arrow to move it to the Selected column. To create a source identity, click **+**. Enter a new username or identity in the Create Source Identity page and click **OK**. • **Source identity feed**—Starting in Juons OS Release 21.4R1, you can select user identity threat feed to define the matching criteria for a policy. Select the user identity threat feed from the Available column and then click the right arrow to move it to the Selected column.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
	Maximum user identity threat feed count is 1024. That is, sum of source identity feed and destination identity feed per policy. **NOTE**: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, `request services security-intelligence download`.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
Destination Zone	To add a destination: **1.** Click **+**. The Select Destination page appears. **2.** Enter the following details: • **Zone**—Select the destination zone from the list to which you want the rule to be associated. • **Addresses**—Select **any** or **Specific**. **NOTE**: • Starting in Juons OS Release 21.4R1, you can select the IP feeds to define the matching criteria for a policy. Also, you can view source type (Address, Address group, Wild card, Range, IP feeds) in the new Type column. • Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, `request services security-intelligence download`. To select a specific address or IP feed, select the addresses or IP feeds from the Available column and then click the right arrow to move it to the Selected column. You can select **Exclude Selected** to exclude only the selected address from the list. To create a new address, click **+**. For more information on fields, see Table 207 on page 701. • **Dynamic applications**—Select **Any**, **Specific**, or **None**. **NOTE**: The Dynamic Applications option is not supported for tenants. To select a specific application, select the application from the Available column and then click the right arrow to move it to the Selected column. **NOTE**: The select all check box is only available when you search for specific dynamic applications.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
	To create a new application, click **+**. The Create Application Signature page appears. For more information on fields, see "Add Application Signatures" on page 781. **NOTE**: For logical systems, you cannot create a dynamic application inline. • **Services**—Select **Any**, **Specific**, or **None**. To select a specific service, select the service from the Available column and then click the right arrow to move it to the Selected column. To create a new service, click **+**. The Create Service page appears. For more information on fields, see Table 208 on page 702. • **URL category**—Select **any**, **Specific**, or **None** to match criteria for a web filtering category. To select a specific URL category, select the URL category from the Available column and then click the right arrow to move it to the Selected column. **NOTE**: This option is not available for logical systems and tenants. • **Destination identity feed**—Starting in Juons OS Release 21.4R1, you can select user identity threat feed to define the matching criteria for a policy. Select the user identity threat feed from the Available column and then click the right arrow to move it to the Selected column. Maximum user identity threat feed count is 1024. That is, sum of source identity feed and destination identity feed per policy. **NOTE**: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, `request services security-intelligence download`.
Action	Select an action to take when traffic matches the criteria: • Permit—Allows packet to pass through the firewall. • Deny—Block and drop the packet, but do not send notification back to the source. • Reject—Block and drop the packet and send a notice to the source host.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action

Advanced Services
Click **+**. The Select Advanced Services page appears.
NOTE:
• When the action is Reject:
  • You can configure only the SSL Proxy and Redirect Profile options.
  • You can configure only the SSL Proxy option if the dynamic application is None.
  • Advanced Security option is not supported for logical systems and tenants.
• When the action is Permit:
  • For logical systems, only IPS, IPS policy, UTM, threat prevention policy, ICAP redirect profile, and AppQOS options are supported.
  • For tenant systems, only threat prevention policy and AppQOS are supported.	

SSL proxy	Select the SSL proxy policy to associate with this rule from the list.
UTM	Select the UTM policy you want to associate with this rule from the list. The list displays all the UTM policies available. If you want to create a new UTM policy, click **Add New**. The Create UTM Policies page appears. For more information on creating a new UTM policy, see "Add a UTM Policy" on page 898.
IPS policy	Select the IPS policy from the list.
Threat prevention policy	Select the configured threat prevention policy from the list.
ICAP redirect profile	Select the configured ICAP redirect profile name from the list.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
IPsec VPN	Select the IPsec VPN tunnel from the list. **NOTE**: If you select Dynamic applications in the destination, IPsec VPN option is not supported.
Pair policy name	Enter the name of the policy with the same IPsec VPN in the opposite direction to create a pair policy. **NOTE**: If you select Dynamic applications in the destination, Pair Policy Name option is not supported.
Application QoS profile	Select the configured AppQoS profile from the list. If you want to create a new AppQoS profile, click **Add New**. The Add AppQoS Profile page appears. For more information on creating a new AppQoS profile, see "Add an Application QoS Profile" on page 603.
Threat profiling	Starting in Juons OS Release 21.4R1, you can enable this option to generate threat profiling feeds. **NOTE**: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, `request services security-intelligence download`. You can add source and destination addresses, and source and destination identities to the threat feeds. After the feeds are generated, you can configure other security policies to use the feeds to match designated traffic and perform policy actions. • Add source IP to feed—Select the threat feed from the list to add it to the source IP address. • Add source identity to feed—Select the threat feed from the list to add it to the source user identity. • Add destination IP to feed—Select the threat feed from the list to add it to the destination IP address. • Add destination identity to feed—Select the threat feed from the list to add it to the destination user identity.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
Packet capture	Enable to capture unknown application traffic specific to a security policy rule. By default, this option is disabled. Once enabled, you can view the packet capture (PCAP) file details or download the PCAP file on the **Monitor** > **Log** > **Sessions** page.
Rule Options Click on **Rule Options**. The SELECT RULE OPTIONS page appears.	
Logging	
Session initiate	Enable this option to log an event when a session is created.
Session close	Enable this option to log an event when the session closes.
Count	Enable this option to collect statistics of the number of packets, bytes, and sessions that pass through the firewall with this policy. Specifies statistical counts. An alarm is triggered whenever traffic exceeds specified packet and byte thresholds. **NOTE**: Alarm threshold fields are disabled if Enable Count is not enabled.
Authentication **NOTE**: • If you select Dynamic applications in the destination, Authentication option is not supported. • This option is not supported for logical systems and tenant systems.	
Push auth entry to JIMS	Enable this option to push authentication entries from firewall authentication, that are in auth-success state, to Juniper Identity Management Server (JIMS). This will enable the SRX Series Firewall to query JIMS to get IP/user mapping and device information. This is not a mandatory option. You can select it when at least one domain is configured on local Active Directory or configure identity management.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
Type	Select the firewall authentication type from the list. The options available are: None, Pass-through, User-firewall, and Web-authentication.
Access profile	Select an access profile from the list. **NOTE**: This option is not supported if you select the authentication type as Web-authentication.
Client name	Enter the client username or client user group name. **NOTE**: This option is not supported if you select the authentication type as User-firewall.
Domain	Select a domain name that must be in a client name from the list. **NOTE**: This option is supported only if you select the authentication type as User-firewall.
Web redirect (http)	Enable this option to redirect HTTP requests to the device's internal webserver by sending a redirect HTTP response to the client system to reconnect to the webserver for user authentication. **NOTE**: This option is not supported if you select the authentication type as Web-authentication.
Captive portal	Enable this option to redirect a client HTTP or HTTPS request to the internal HTTPS webserver of the device. The HTTPS client requests are redirected when SSL termination profile is configured. **NOTE**: This option is not supported if you select the authentication type as Web-authentication.
Interface	Select an interface for the webserver where the client HTTP or HTTPS request is redirected. **NOTE**: You cannot edit this once the policy is created. To edit the interface, go to **Network** > **Connectivity** > **Interfaces**.

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
IPv4 address	Enter IPv4 address of the webserver where the client HTTP or HTTPS request is redirected. **NOTE**: You cannot edit this once the policy is created. To edit the interface, go to **Network** > **Connectivity** > **Interfaces**.
SSL termination profile	Select an SSL termination profile from the list which contains the SSL terminated connection settings. SSL termination is a process where the SRX Series device acts as an SSL proxy server, terminates the SSL session from the client. To add a new SSL termination profile: **1.** Click **Add**. The Create SSL Termination Profile page appears. **2.** Enter the following details: • **Name**—Enter SSL termination profile name; 63-character maximum. • **Server certificate**—Select a server certificate from the list that is used to authenticate the server identity. To add a certificate, click **Add**. For more information on adding a device certificate, see "Add a Device Certificate" on page 235. To import a certificate, click **Import**. For more information on importing a device certificate, see, "Import a Device Certificate" on page 233.
Auth only browser	Enable this option to drop non-browser HTTP traffic to allow for captive portal to be presented to unauthenticated users who request access using a browser. **NOTE**: This option is not supported if you select the authentication type as Web-authentication.
User agents	Enter a user-agent value which is used to verify that the user's browser traffic is HTTP/HTTPS traffic. **NOTE**: This option is not supported if you select the authentication type as Web-authentication.
Advanced Settings	

Table 206: Fields on the Security Policies Page *(Continued)*

Field	Action
Destination address translation	Select the action to be taken on a destination address translation from the list. The options available are: None, Drop Translated, and Drop Untranslated.
Redirect options	Select a redirect action from the list. The options available are: None, Redirect Wx, and Reverse Redirect Wx. **NOTE**: This option is not supported for SRX5000 line of devices.
TCP Session Options	
Sequence number check	Enable or disable checking of sequence numbers in TCP segments during stateful inspections at policy rule level. By default, the check happens at the global level. To avoid commit failure, turn off **Sequence number check** under **Global Options** > **Flow** > **TCP Session**.
SYN flag check	Enable or disable the checking of the TCP SYN bit before creating a session at policy rule level. By default, the check happens at the global level. To avoid commit failure, turn off **SYN flag check** under **Global Options** > **Flow** > **TCP Session**.
Schedule	
Schedule	Click **Schedule** and select one of the configured schedules from the list. To add a new schedule, click **Add New Schedule**. The Add New Schedule page appears. For more information on creating a new schedule, see Table 209 on page 704.

Table 207: Fields on the Create Address Page

Field	Action
Name	Enter a name for the address. The name must be a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
IP type	Select **IPv4** or **IPv6**.

Table 207: Fields on the Create Address Page *(Continued)*

Field	Action
IPv4	
IPv4 address	Enter a valid IPv4 address.
Subnet	Enter a subnet mask for the IPv4 address.
IPv6	
IPv6 address	Enter a valid IPv6 address.
Subnet prefix	Enter a subnet prefix for the IPv6 address.

Table 208: Fields on the Create Service Page

Field	Action
Global Settings	
Name	Enter a unique name for the application.
Description	Enter description of the application.
Application protocol	Select an option from the list for application protocol.
Match IP protocol	Select an option from the list to match IP protocol.
Source port	Select an option from the list for source port.
Destination port	Select an option from the list for destination port.
ICMP type	Select an option from the list for ICMP message type.

Table 208: Fields on the Create Service Page *(Continued)*

Field	Action
ICMP code	Select an option from the list for ICMP message code.
RPC program numbers	Enter a value for RPC program numbers. The format of the value must be W or X-Y. Where, W, X, and Y are integers between 0 and 65535.
Inactivity timeout	Select an option from the list for application specific inactivity timeout.
UUID	Enter a value for DCE RPC objects. **NOTE**: The format of the value must be 12345678-1234-1234-1234-123456789012.
Custom application group	Select an application set name from the list.
Terms Click **+**. The Create Term page appears.	
Name	Enter a name for the term.
ALG	Select an option from the list for ALG.
Match IP protocol	Select an option from the list to match IP protocol.
Source port	Select an option from the list for source port.
Destination port	Select an option from the list for destination port.
ICMP type	Select an option from the list for ICMP message type.
ICMP code	Select an option from the list for ICMP message code.

Table 208: Fields on the Create Service Page *(Continued)*

Field	Action
RPC program numbers	Enter a value for RPC program numbers. **NOTE**: The format of the value must be W or X-Y. Where, W, X, and Y are integers between 0 and 65535.
Inactivity timeout	Select an option from the list for application specific inactivity timeout.
UUID	Enter a value for DCE RPC objects. **NOTE**: The format of the value must be 12345678-1234-1234-1234-123456789012.

Table 209: Fields on the Add New Schedule Page

Field	Action
Name	Enter the name for the schedule.
Description	Enter a description for the schedule.
Repeats	Select an option from the list to repeat the schedule: • Never • Daily • Weekly
All Day	Enable this option to schedule an event for an entire day. This option is available only for Never and Daily repeat type schedule.
Start date	Select the schedule start date in the YYYY-MM-DD format. This option is available only for Never repeat type schedule.

Table 209: Fields on the Add New Schedule Page *(Continued)*

Field	Action
Stop date	Select the schedule stop date in the YYYY-MM-DD format. This option is available only for Never repeat type schedule.
Start time	Enter the start time for the schedule in HH:MM:SS 24 hours format. This option is available only for Daily repeat type schedule.
Stop time	Enter the end time for the schedule in HH:MM:SS 24 hours format. This option is available only for Daily repeat type schedule.
Repeat on	Select the days and time on which you want to repeat the schedule. To set time for the selected day(s): 1. Click **Set Time** or **Set Time to Selected Days**. The Set Time to Selected Days page appears. 2. Enter the following details: • Name—Displays the day(s) you have selected. • All day—Enable this option for the event to run for the entire day. • Start time—Enter the start time in HH:MM:SS 24 hours format. • Stop time—Enter the stop time in HH:MM:SS 24 hours format. 3. Click **OK** to save changes. This option is available only for Weekly repeat type schedule.

Table 209: Fields on the Add New Schedule Page *(Continued)*

Field	Action
Schedule criteria	Select any of the following options: • **Schedule Never Stops**—Schedule can be active forever (recurrent), but only as specified by the daily or weekly schedule. • **Schedule Specify Window**—Schedule can be active during a single time slot, as specified by a start date and a stop date. Enter the following details: • **Schedule starts**—Enter the schedule start date in the YYYY-MM-DD format. • **Schedule ends**—Enter the schedule start date in the YYYY-MM-DD format. This option is available only for Daily and Weekly repeat type schedule.

RELATED DOCUMENTATION

Edit a Rule | **707**

Clone a Rule | **706**

Clone a Rule

You are here: **Security Policies & Objects** > **Security Policies**.

To clone a rule:

1. Select a rule that you want to clone on the Security Policies page.
2. Click **More** > **Clone** available on the upper right-side of the page.

   The Security Policies page appears with inline editable fields. For more information on editing the fields, see "Add a Rule" on page 690.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

   A cloned rule is created for the selected rule. By default, the name of the cloned rule is in the format: <*rule name*>_clone.

RELATED DOCUMENTATION

Delete Rules | 707

Edit a Rule

You are here: **Security Policies & Objects** > **Security Policies**.

To edit a rule:

1. Select an existing rule configuration that you want to edit on the Security Policies page.
2. Click the pencil icon available on the upper right-side of the page.

   The Security Policies page appears with inline editable fields. For more information on editing the fields, see "Add a Rule" on page 690.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Rules | 707

Delete Rules

You are here: **Security Policies & Objects** > **Security Policies**.

To delete a rule:

1. Select one or more rules that you want to delete on the Security Policies page.
2. Click the delete icon available on the upper right-side of the page.
3. Click **Yes** to delete the rules or click **No** to retain the rules.

RELATED DOCUMENTATION

About the Security Policies Page | 682

Configure Captive Portal for Web Authentication and Firewall User Authentication

SUMMARY

Learn how to configure captive portal for Web authentication and firewall user authentication using J-Web.

IN THIS SECTION

Overview

What Is Captive Portal?

Captive portal is a method of authenticating devices that need to connect to a network. On an SRX Series devices, you can enable captive portal to redirect Web browser requests to a login page that prompts you to enter your username and password. After successful authentication, you can proceed with the original page request and subsequent network access.

What Is Web Authentication?

With a Web authentication method, you point a browser to an IP address on a device that is enabled for Web authentication. This action initiates an HTTPS session on the IP address that hosts the Web authentication feature on the device. The device then prompts you to enter your username and password, and the result is cached on the device. When the traffic later encounters a Web authentication policy, your access is allowed or denied based on the previous Web authentication results.

You can use other authentication methods as well, but we will not cover those methods in this document. However, we describe each of those methods in brief:

- Pass-through authentication—Pass-through user authentication is a form of active authentication. In this method, the device prompts you to enter a username and password. If authentication validates your identity, you are allowed to pass through the firewall and access the requested resources.
- Pass-through with web-redirect—When using this authentication method for HTTPS client requests, you can use the web-redirect feature to direct your requests to the device's internal webserver. The webserver sends a redirect HTTPS response to the client system, directing it to reconnect to the webserver for user authentication. The interface that the client's request arrives at is the interface on which the redirect response is sent.

What Is Firewall User Authentication?

A firewall user is a network user who must provide a username and password for authentication when initiating a connection across the firewall. Junos OS enables administrators to restrict or to permit firewall users' access to protected resources (in different zones) behind a firewall based on their source IP address and other credentials. After defining the firewall users, you can create a policy that requires the users to authenticate using one of the three authentication methods (Web, pass-through, or pass-through with web-redirect).

Workflow

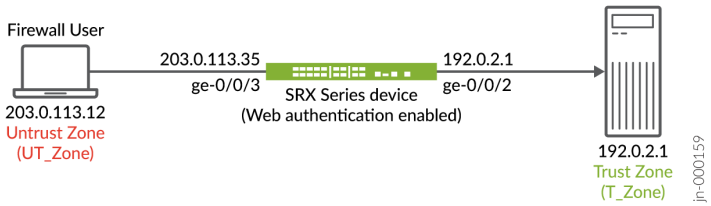
IN THIS SECTION

Scope

Here's a sample topology (see Figure 19 on page 710), which comprises:

- A firewall user's device that acts as a client.
- An SRX Series device that has access to the Internet.
- A network device that acts as an HTTPS server.

Figure 19: Sample Topology



In this sample topology, you'll use J-Web on the SRX Series device to do the following tasks:

NOTE: The values used to configure the sample topology are only examples.

Step	Action
1	Create a logical interface on ge-0/0/3, assign it the IP address 203.0.113.35, and enable Web authentication. **NOTE**: In this example, the firewall user system IP address is 203.0.113.12, which is in the same subnet as 203.0.113.0/24. Create a logical interface on ge-0/0/2 and assign it the IP address 192.0.2.1. **NOTE**: In this example, the HTTPS server IP address is 192.0.2.1.
2	Create an access profile (FWAUTH) and define local authentication services.
3	Configure Web authentication settings to display the successful login message.
4	Create an untrust (UT_ZONE) and a trust (T_ZONE) zones and assign the ge-0/0/3 and ge-0/0/2 interfaces, respectively.
5	Configure captive portal for Web authentication and firewall user authentication in the security policy rules (FWAUTH-RULE).

(Continued)

Step	Action
6	Verify that the configured values work for a firewall user: • For Web authentication, you'll successfully authenticate using https://203.0.113.35. • For firewall user authentication, you'll successfully authenticate using https://203.0.113.35 and then get redirected to https://192.0.2.1 for accessing the HTTPS server.

Before You Begin

- The values used to configure the sample topology are only examples. You can change any details necessary to match your network configuration.
- Ensure that the SRX Series device you use in this example runs Junos OS Release 21.4R1 or later.
- Ensure that your device has the required certificates installed to allow authentication. In this example, we'll use *cert1*, a self-signed certificate.

Step 1: Create a Logical Interface and Enable Web Authentication

In this step, you'll do the following tasks:

- For the ge-0/0/3 interface on the SRX Series device:
  1. Create a logical interface for an untrust zone.
  2. Assign the IPv4 address 203.0.113.35 to the interface.

     NOTE: You'll use the same IP address for enabling captive portal.

  3. Enable HTTPS on the interface for Web authentication.
- For the ge-0/0/2 interface on the SRX Series device:
  1. Create a logical interface for a trust zone.
  2. Assign the IPv4 address 192.0.2.1 to the interface.

You are here (in the J-Web UI): **Network** > **Connectivity** > **Interfaces**

To create a logical interface for an untrust zone and to enable Web authentication:

1. Select **ge-0/0/3** and then select **Create** > **Logical Interface** on the upper-right corner of the Interfaces page.

   The Add Logical Interface for ge-0/0/3.0 page appears.

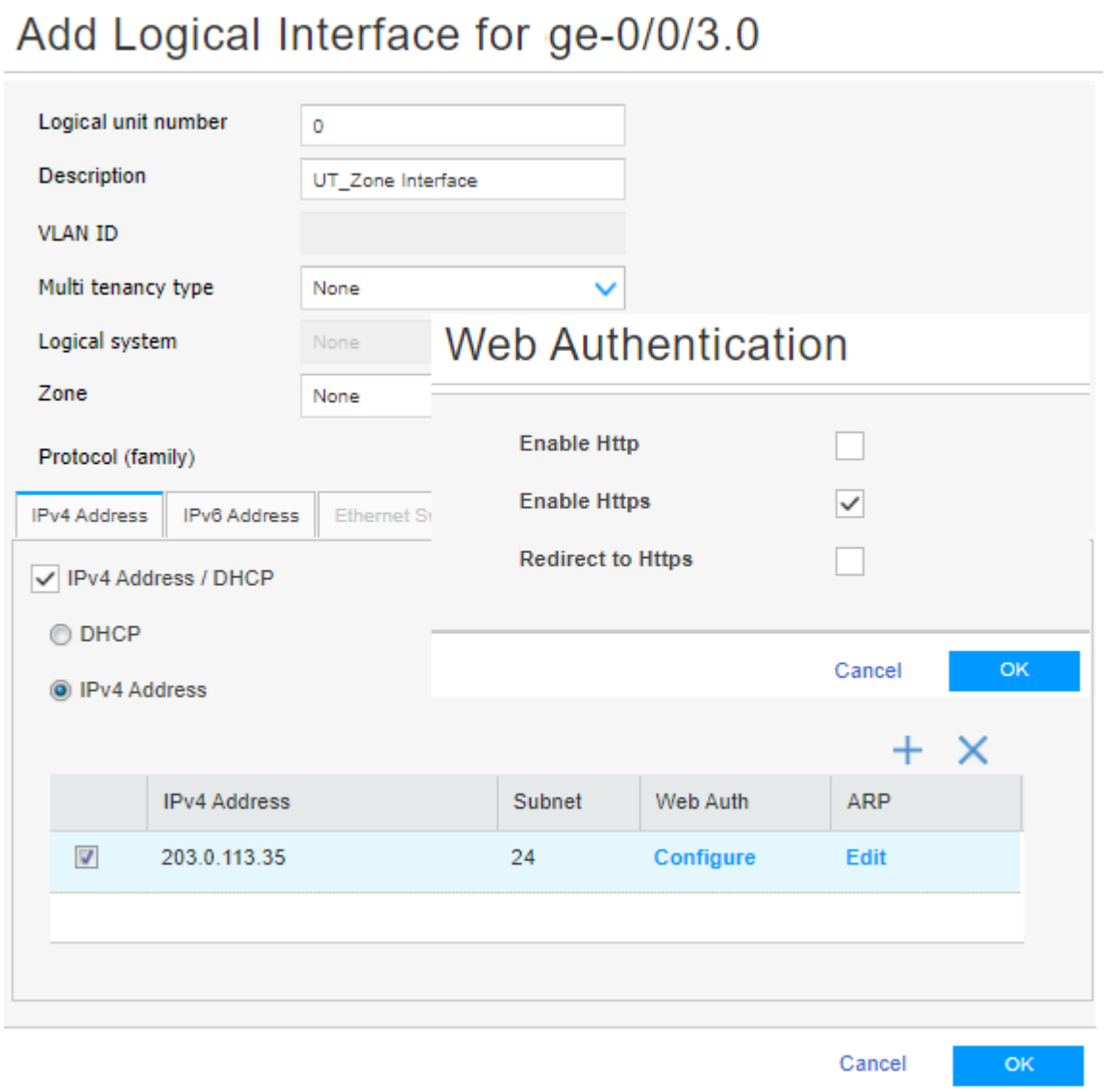
   NOTE: You cannot configure captive portal on the fxp0 interface.

2. Specify the following details:

Field	Action
Logical unit number	Type **0**.
Description	Type **UT_Zone Interface**.
VLAN ID	This field is not editable.
Multi tenancy type	Select **None** from the list.
Logical system	This field is not editable.
Zone	Select **None** from the list. In a later step, we'll create an untrust zone (UT_ZONE) and assign the ge-0/0/3 interface to it. See "Step 4: Create Security Zones and Assign Interfaces to the Zones" on page 720.
Protocol (family) - IPv4 Address	
IPv4 Address / DHCP	Select the check box to enable the IPv4 Address/ DHCP configuration.

(Continued)

Field	Action
IPv4 Address	Select **IPv4 Address**. Then, click **+** and enter the following details: • IPv4 Address—Type **203.0.113.35** for Web authentication. **NOTE**: The captive portal configuration uses the same IPv4 address. • Subnet—Select **24** using the up or down arrow. • Web Auth: **a.** Click **Configure**. The Web Authentication page appears. **b.** Select **Enable Https** dedicated to captive portal. **c.** Click **OK** to save changes.



3. Click **OK** to save the changes.

   Good job! You've created a logical interface on ge-0/0/3 with IP address 203.0.113.35 (Web authentication enabled) for your system.

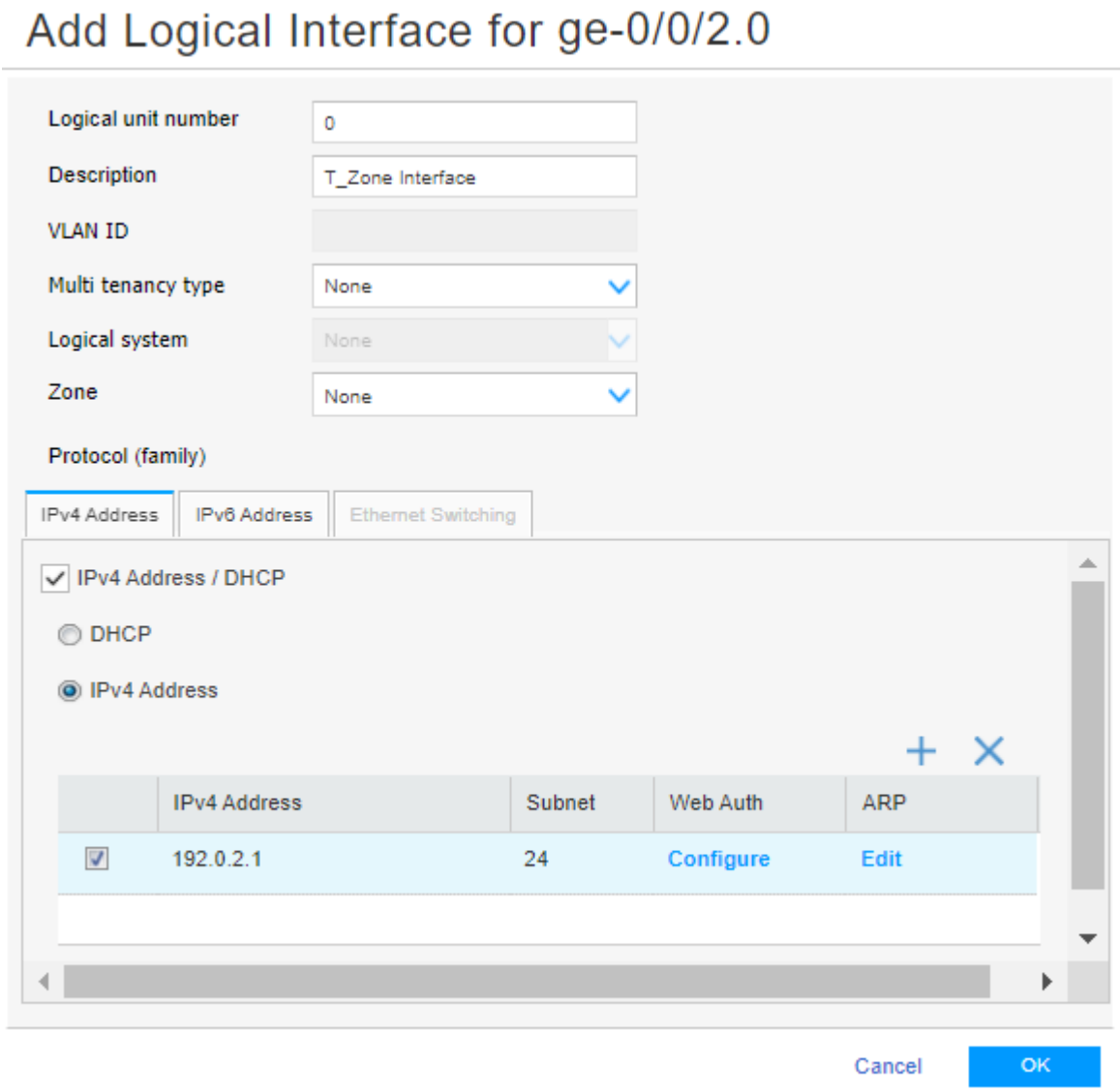
To create a logical interface for a trust zone:

1. Select **ge-0/0/2** and then select **Create** > **Logical Interface** on the upper-right corner of the Interfaces page.

   The Add Logical Interface for ge-0/0/2.0 page appears.

2. Specify the following details:

Field	Action
Logical unit number	Type **0**.
Description	Type **T_Zone Interface**.
VLAN ID	This field is not editable.
Multi tenancy type	Select **None** from the list.
Logical system	This field is not editable.
Zone	Select **None** from the list. In a later step, we'll create a trust zone (T_ZONE) and assign the ge-0/0/2 interface to it. See "Step 4: Create Security Zones and Assign Interfaces to the Zones" on page 720.
VLAN ID	This field is not editable.
Protocol (family) - IPv4 Address	
IPv4 Address / DHCP	Select the check box to enable the IPv4 Address/ DHCP configuration.
IPv4 Address	**a.** Select **IPv4 Address**. **b.** Click **+**. **c.** IPv4 Address—Type **192.0.2.1** (HTTPS server). **d.** Subnet—Select **24** using the up or down arrow. **e.** Web Auth—Leave as is. **f.** ARP—Leave as is.



3. Click **OK** to save the changes.

   Good job! You've created a logical interface on ge-0/0/2 with IP address 192.0.2.1 for the HTTPS server.

4. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

   The successful-commit message appears.

   You can also choose to commit all configuration changes at once, at the end of "Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy" on page 724.

Step 2: Create an Access Profile

Let's create an access profile to define local authentication services. You will use this access profile in Web authentication settings and security policies.

You are here (in the J-Web UI): **Security Services** > **Firewall Authentication** > **Access Profile**

To create an access profile:

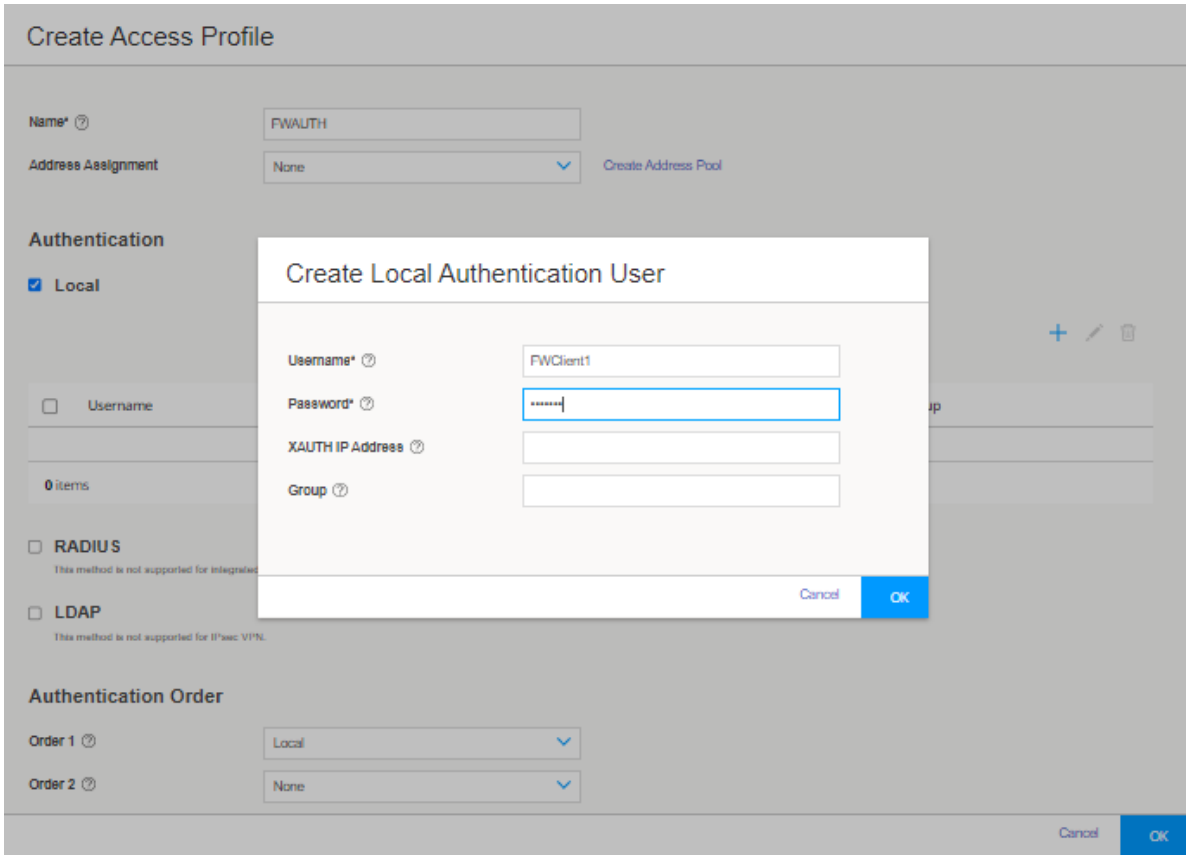
1. Click the add icon (**+**) on the upper-right corner of the Access Profile page.

   The Create Access Profile page appears.
2. Specify the following details:

Field	Action
Name	Type **FWAUTH**.
Address Assignment	(Optional) Select **None** from the list. You can select an address pool from the list. You can also add a new address pool by clicking **Create Address Pool** and providing the required values.
Authentication	
Local	**a.** Select **Local** to configure the local authentication services. **b.** Click **+** and enter the following details on the Create Local Authentication User page: **i.** Username—Type **FWClient1**. This is the username of the user requesting access. **ii.** Password—Type **$ABC123**. **iii.** XAUTH IP Address—Leave as is. **iv.** Group—Leave as is. **v.** Click **OK** to save the changes.
Authentication Order	
Order 1	Select **Local** from the list.

(Continued)

Field	Action
Order 2	By default, **None** is selected. Leave as is.



3. Click **OK** to save the changes.

   *Good job! You've created the **FWAUTH** access profile.*

4. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

   The successful-commit message appears.

   You can also choose to commit all configuration changes at once, at the end of "Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy" on page 724.

Step 3: Configure Web Authentication Settings

We'll now assign the created access profile, define a successful-login message, and upload the logo image. This image is used for both Web authentication and captive portal.

You are here (in the J-Web UI): **Security Services** > **Firewall Authentication** > **Authentication Settings**

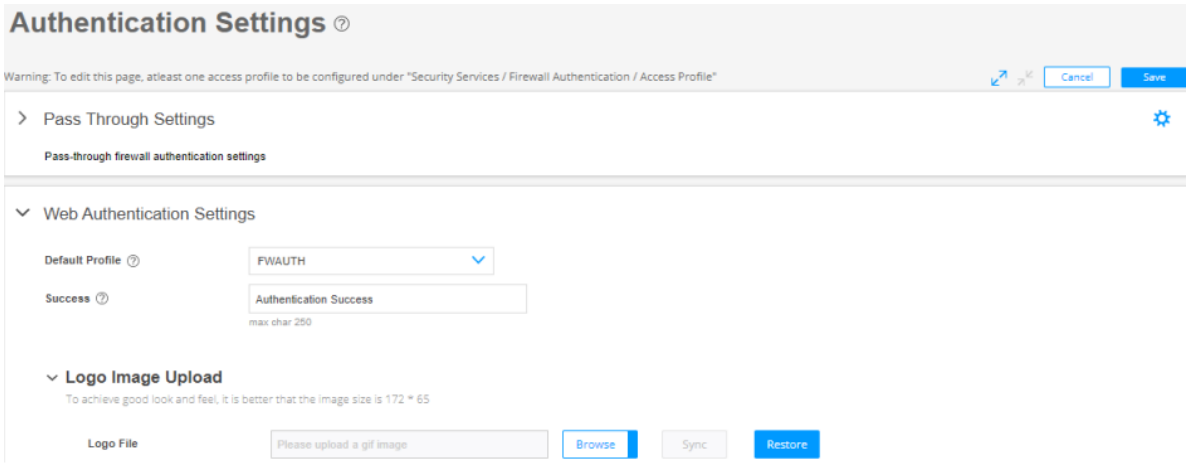
To configure Web authentication settings:

1. Click **Web Authentication Settings**.
2. Do the following:
   - **Default Profile**—Select **FWAUTH** from the list. The security policies use this profile to authenticate users.
   - **Success**—Type **Authentication Success** as the message to be displayed for users who log in successfully.
3. (Optional) To upload a customized logo:
   a. Click **Logo Image Upload**.
   b. Click **Browse** for uploading a logo file.
   c. Select a logo image and then click **OK**.

      NOTE: For a good logo, the image must be in the **.gif** format and the resolution must be 172x65.

   d. Click **Sync** to apply the logo.

      The uploaded image will now appear on the captive portal login page or the Web authentication login page.



4. Click **Save** on the upper-right corner of the Authentication Settings page to save the changes.

   Congratulations! You've successfully saved your Web authentication settings.
5. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

The successful-commit message appears.

You can also choose to commit all configuration changes at once, at the end of "Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy" on page 724.

Step 4: Create Security Zones and Assign Interfaces to the Zones

You create a security zone to define one or more network segments that regulate inbound and outbound traffic through policies.

We'll now separately create:

- An untrust zone (UT_ZONE) and assign the ge-0/0/3 interface to it.
- A trust zone (T_ZONE) and assign the ge-0/0/2 interface to it.

You are here (in the J-Web UI): **Security Policies & Objects** > **Zones/Screens**

To create UT_ZONE (untrust zone) and T_ZONE (trust zone) and to assign the defined interfaces to the zones:

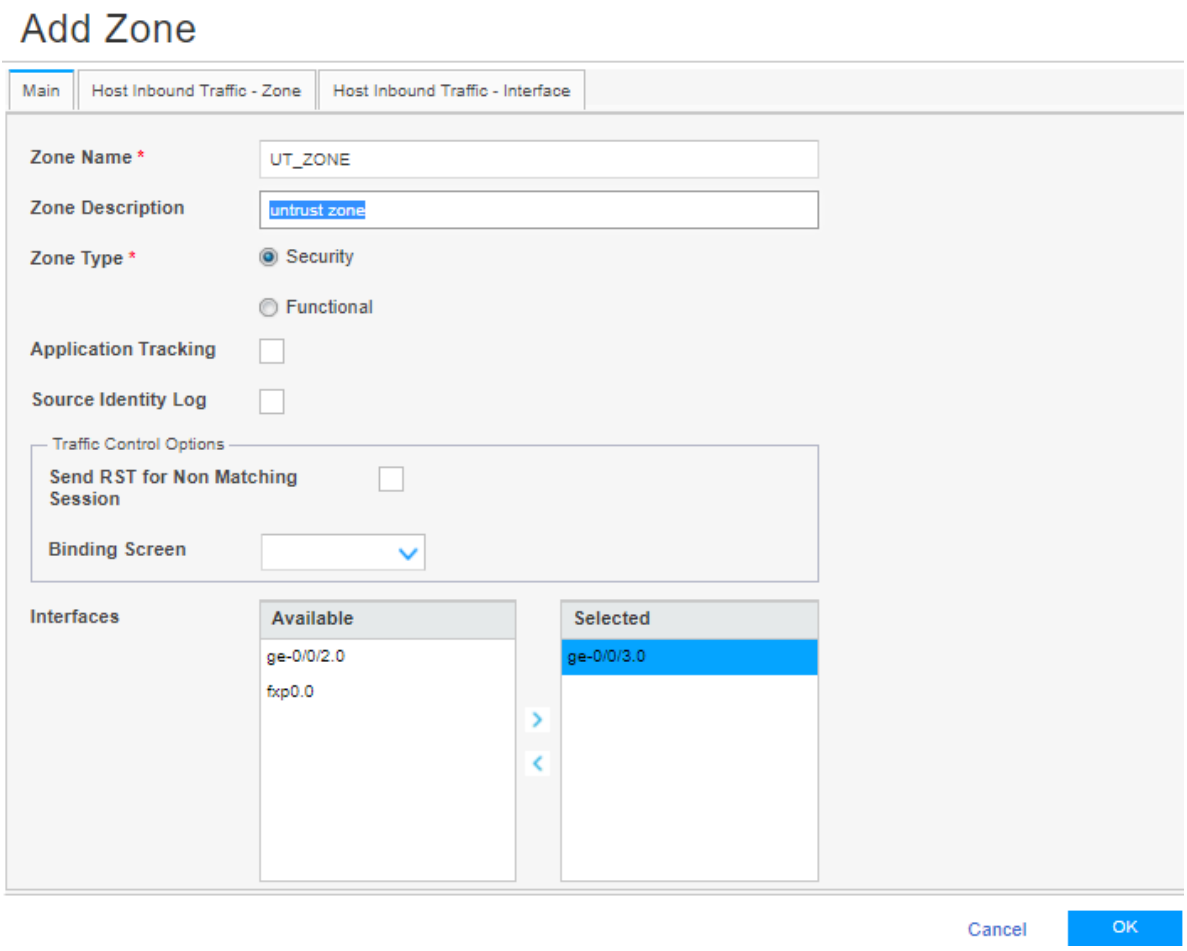
1. Click the add icon (**+**) on the upper-right corner of the Zone List page.

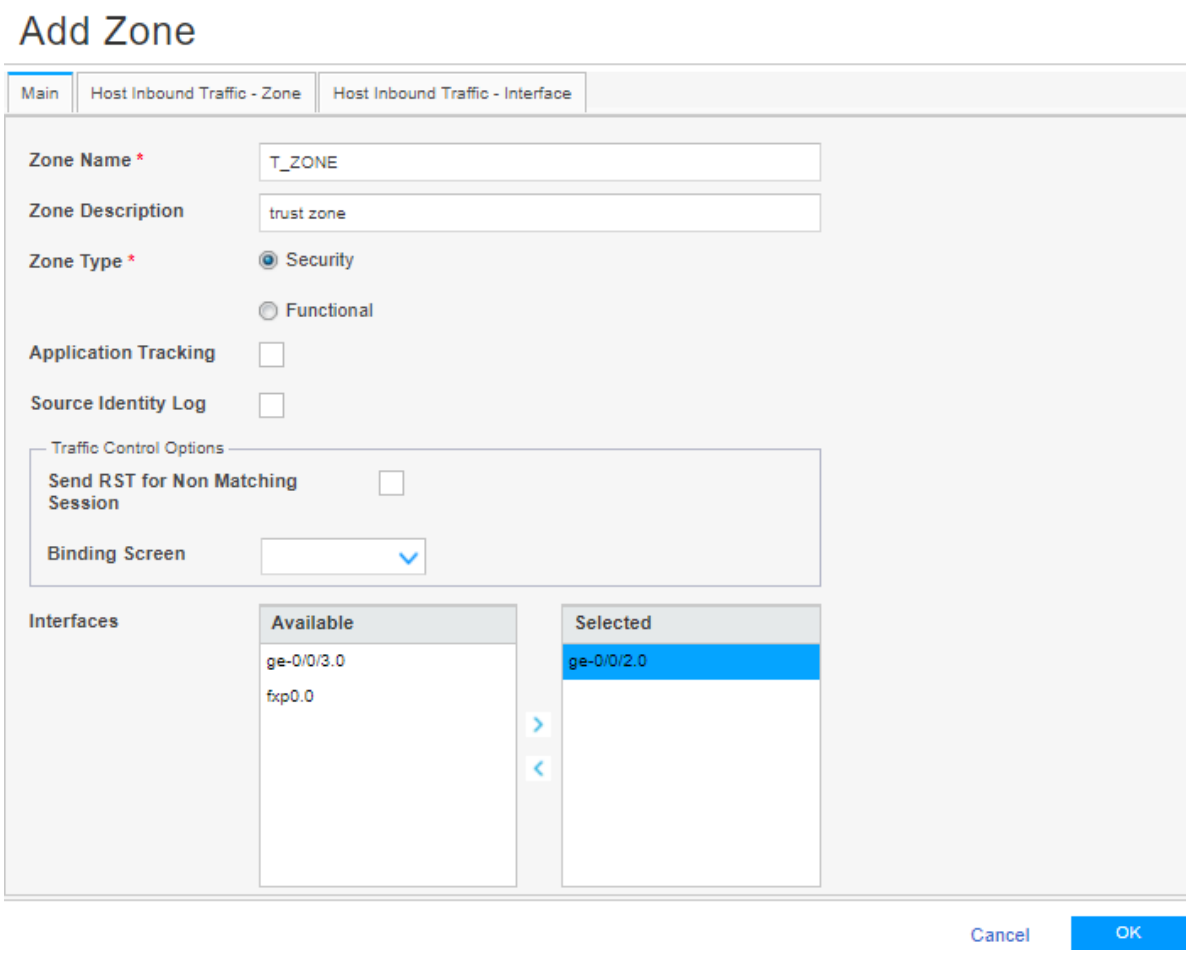
   The Add Zone page appears.
2. Specify the following details:

Field	Action
Main	
Zone name	• Type **UT_ZONE** for an untrust zone. • Type **T_ZONE** for a trust zone.
Zone description	• Type **untrust zone** for UT_ZONE. • Type **trust zone** for T_ZONE.
Zone type	Select **Security**.
Application Tracking	Leave as is.
Source Identity Log	Leave as is.

(Continued)

Field	Action
Traffic Control Options	Leave as is.
Interfaces	• For UT_ZONE, select **ge-0/0/3.0** from the Available column and click the right arrow to move it to the Selected column. • For T_ZONE, select **ge-0/0/2.0** from the Available column and click the right arrow to move it to the Selected column.

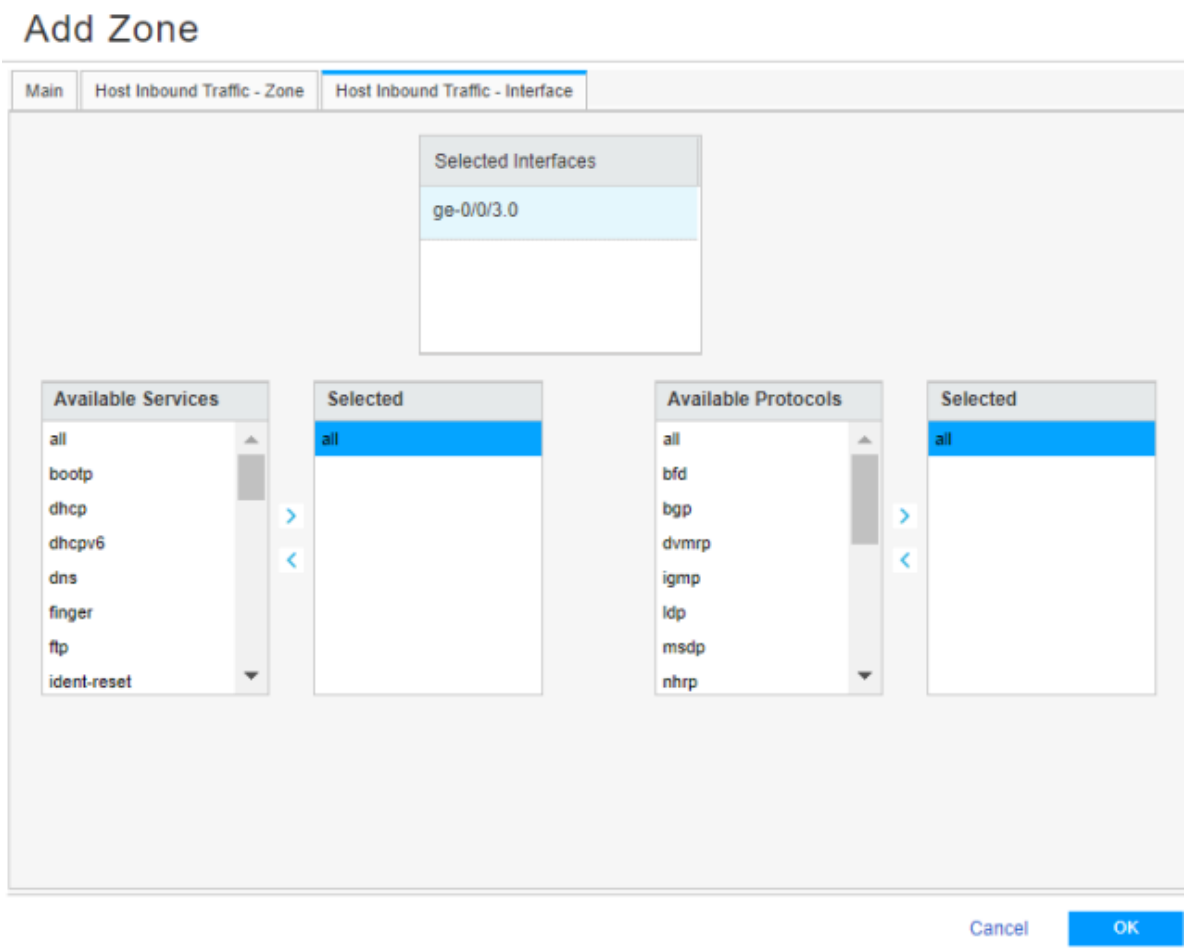


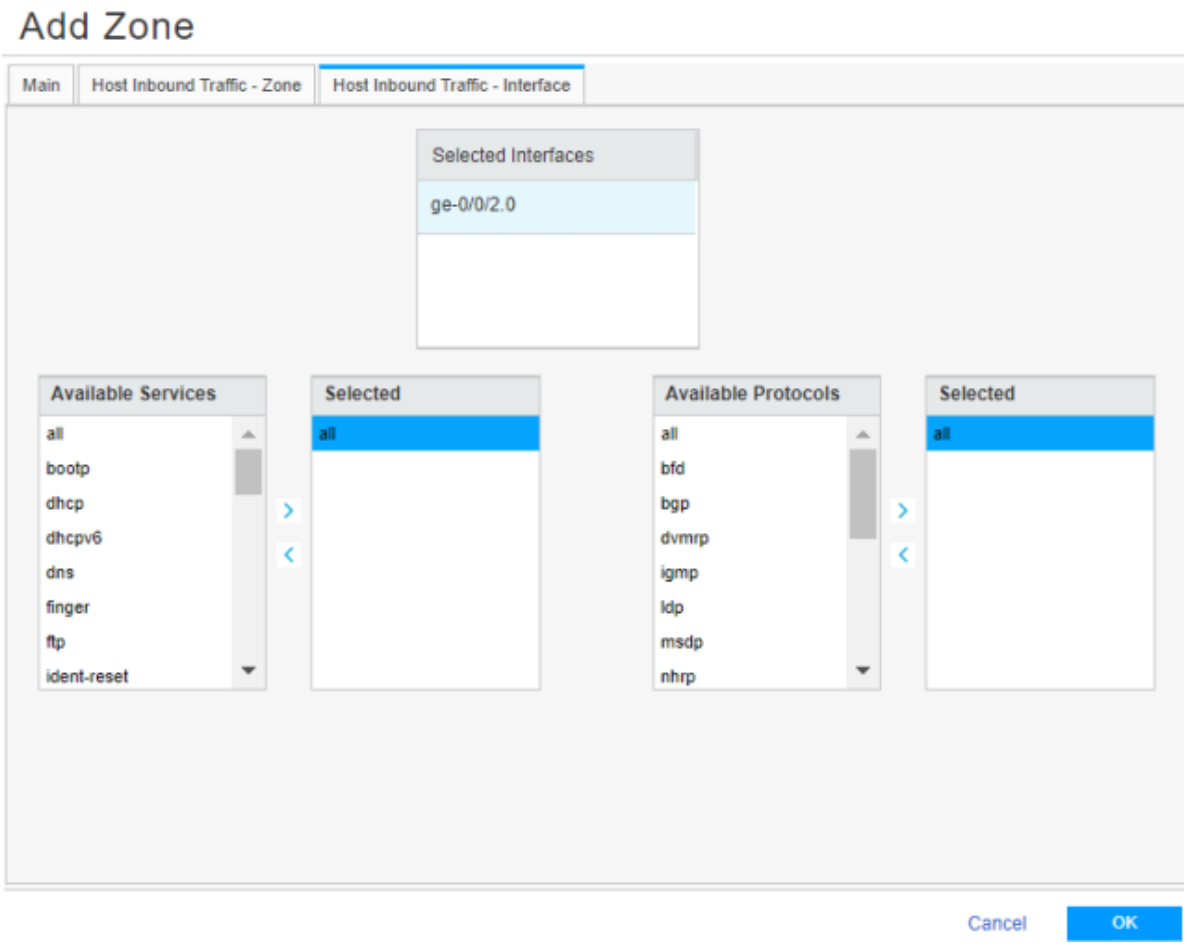


Field	Action (Sample Value)
Host Inbound Traffic - Zone	Leave as is.
Host Inbound Traffic - Interface	
Selected Interfaces	• For UT_ZONE, select **ge-0/0/3.0**. • For T_ZONE, select **ge-0/0/2.0**.
Available Services	Select **all** from the Available Services column and click the right arrow to move it to the Selected column.

(Continued)

Field	Action (Sample Value)
Available Protocols	Select **all** from the Available Protocols column and click the right arrow to move it to the Selected column.





3. Click **OK** to save the changes.

   Good job! You have assigned the ge-0/0/3 interface to UT_ZONE and ge-0/0/2 to T_ZONE.

4. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

   The successful-commit message appears.

   You can also choose to commit all configuration changes at once, at the end of "Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy" on page 724.

Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy

We'll now enable captive portal in the security policy rules to redirect a client HTTPS request to the internal HTTPS server of the device.

You are here (in the J-Web UI): **Security Policies & Objects** > **Security Policies**

To configure security policy rule for captive portal:

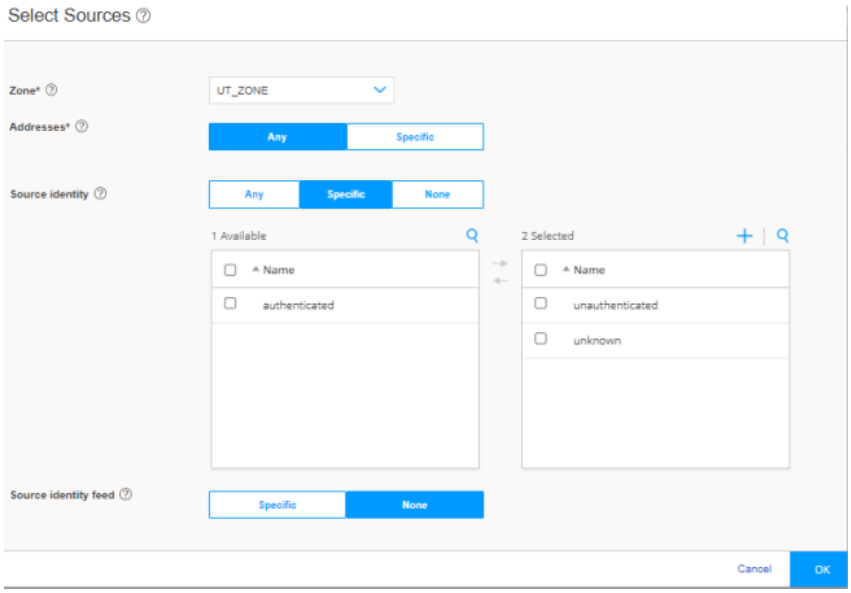
1. Click the add icon (**+**) on the upper-right corner of the Security Policies page.

The inline editable fields appear.

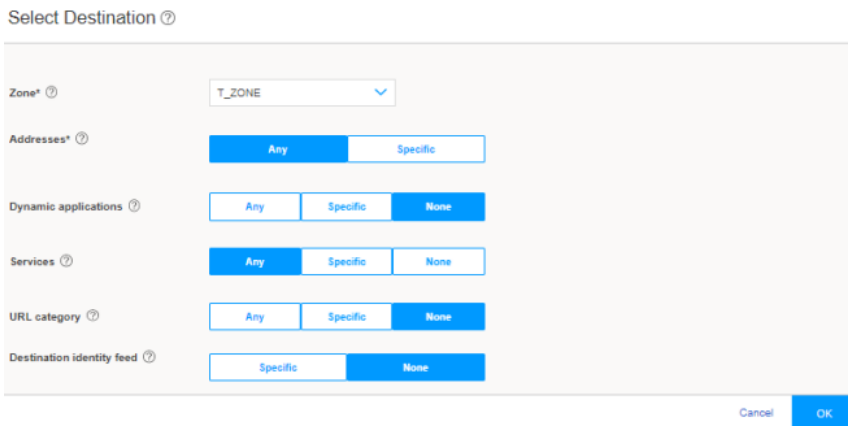
2. Specify the following details:

Field	Action
Rule Name	
Name	Type **FWAUTH-RULE**.
Description	Type **Test rule**.
Source Zone	
+	Click **+** to add a source zone. The Select Sources page appears.

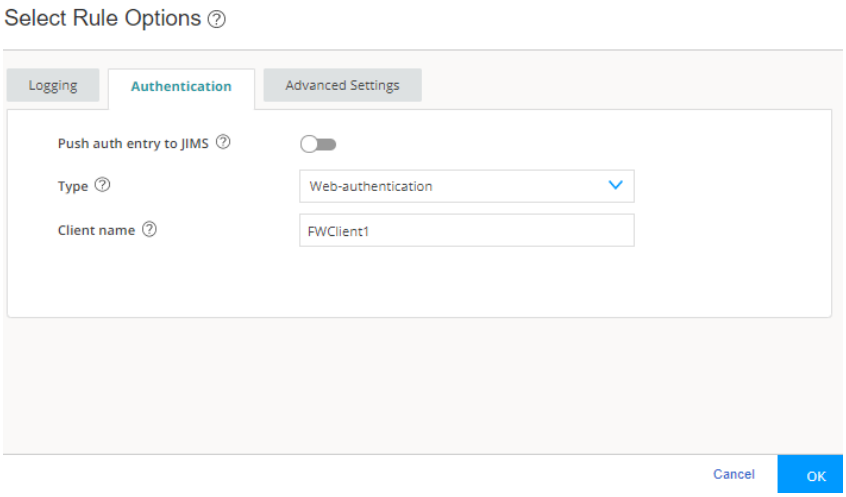
(Continued)

Field	Action
Select Sources	Specify the following details: **a.** Zone—Select **UT_ZONE** from the list to which you want the rule to be associated. **b.** Addresses—By default, **Any** is selected. Leave as is. **c.** Source identity: • For Web authentication, select **None**. • For firewall user authentication, select **Specific**. Then select **unauthenticated** and **unknown** from the Available column and click the right arrow to move these values to the Selected column. **d.** Source identity feed—Select **None**.  **e.** Click **OK** to save the changes.
Destination Zone	
+	Click **+** to add a destination zone. The Select Destination page appears.

(Continued)

Field	Action
Select Destination	Specify the following details: **a.** Zone—Select **T_ZONE** from the list to which you want the rule to be associated. **b.** Addresses—By default, **Any** is selected. Leave as is. **c.** Dynamic applications—Select **None**. **NOTE**: You cannot configure dynamic applications with Web authentication. **d.** Services—Select **Any**. **e.** URL category—Select **None**. **f.** Destination identity feed—Select **None**.  **g.** Click **OK** to save the changes.
Action	Select **Permit**.
Advanced Services	Leave as is.
Rule Options	
+	Click **+** to select rule options. The Select Rule Options page appears.

(Continued)

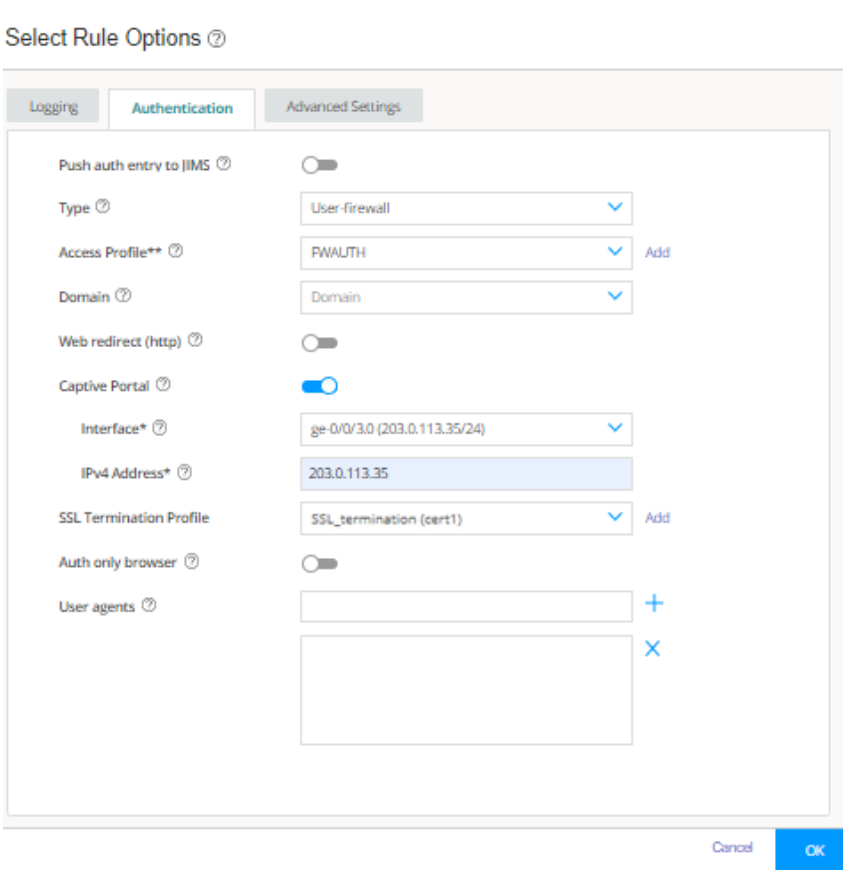
Field	Action
Logging	Leave as is.
Authentication **NOTE**: Use this configuration for *Web authentication* only.	Specify the following details: • Push auth entry to JIMS—By default, this option is disabled. Leave as is. • Type—Select **Web-authentication** from the list. • Client name—Type **FWClient1**. • Click **OK** to save the changes. 

(Continued)

Field	Action

Authentication
 	
NOTE: Use this configuration for *firewall user authentication* only.
	Specify the following details:
	
	• Push auth entry to JIMS—By default, this option is disabled. Leave as is.
	• Type—Select **User-firewall** from the list.
	• Access profile—Select **FWAUTH** from the list.
	• Domain—Leave as is.
	• Web redirect (http)—By default, this option is disabled. Leave as is.
	• Captive Portal—Enable to redirect a client HTTPS request to the webserver for user authentication.
	  • Interface—Select **ge-0/0/3.0 (203.0.113.35/24)** from the list for the webserver where the client HTTPS request is redirected. This is the same interface that you configured while enabling Web authentication.
	  • IP address—Type **203.0.113.35** for the webserver where the client HTTPS request is redirected. This is the same IPv4 address that you configured while enabling Web authentication on the ge-0/0/3 Interface.
	• SSL Termination Profile—Select **SSL_termination (cert1)** from the list for SSL termination support service. Acting as an SSL proxy server, the SRX Series device uses the SSL termination process to terminate the client's SSL session.
	• Auth only browser—By default, this option is disabled. Leave as is.
	• User agents—Leave as is.
	• Click **OK** to save the changes.

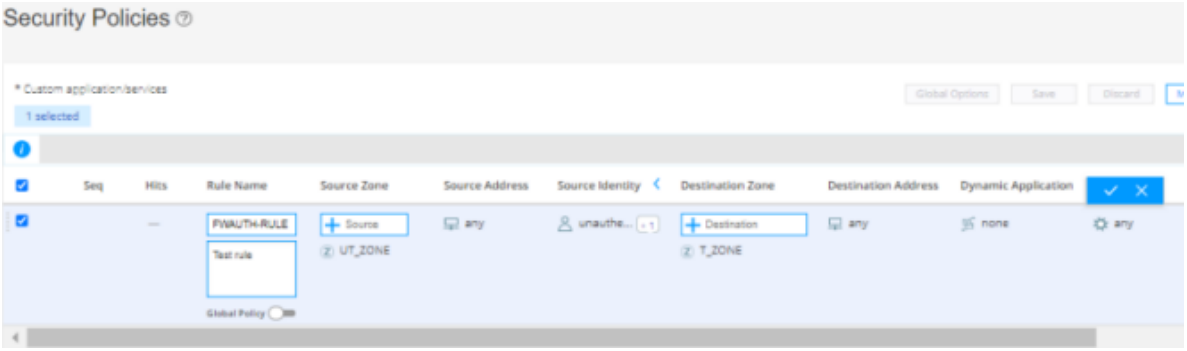
(Continued)

Field	Action
	

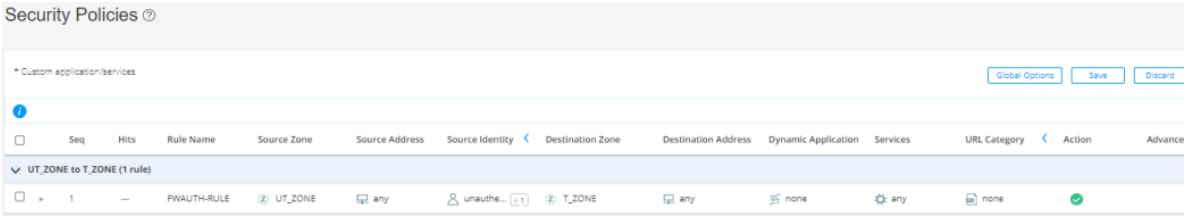
3. Click the tick icon

on the right-side of the row after you're done with the configuration.

NOTE: Slide the horizontal bar backward if the inline tick and cancel icons are not available when creating a new rule.



4. Click **Save** on the upper-right corner of the Security Policies page to save changes.



5. Click **Commit** (at the right side of the top banner) and select **Commit configuration**.

   The successful-commit message appears.

   Congratulations! You've successfully committed your configuration changes. You are all set with the Web or firewall user authentication policy.

Step 6: Verify the Web Authentication and User Authentication Configuration

IN THIS SECTION

Purpose

The final step! Let’s see wether your configurations works for a firewall user:

- For Web authentication, you’ll successfully authenticate using https://203.0.113.35. This is the same IPv4 address that you configured in "Step 1: Create a Logical Interface and Enable Web Authentication" on page 711.

- For firewall user authentication, you’ll successfully authenticate using https://203.0.113.35 and then get redirected to https://192.0.2.1 for accessing the HTTPS server. These are the same IPv4

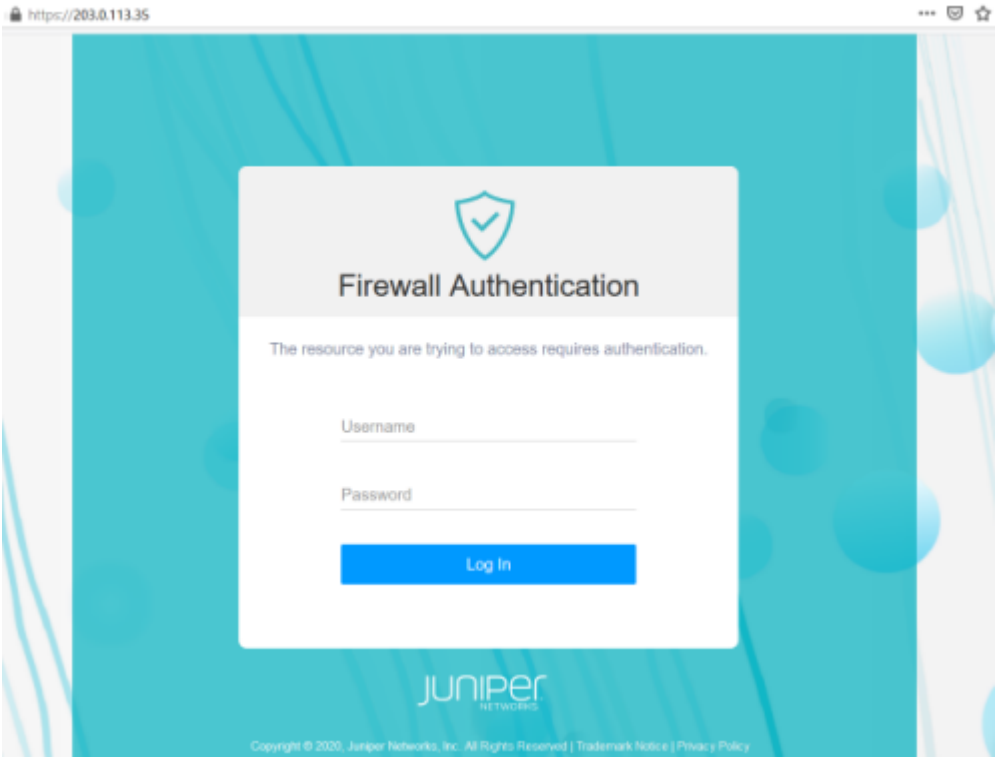
addresses that you configured in "Step 1: Create a Logical Interface and Enable Web Authentication" on page 711.

Action

To verify the Web authentication configuration:

1. Type **https://203.0.113.35** in your Web browser.

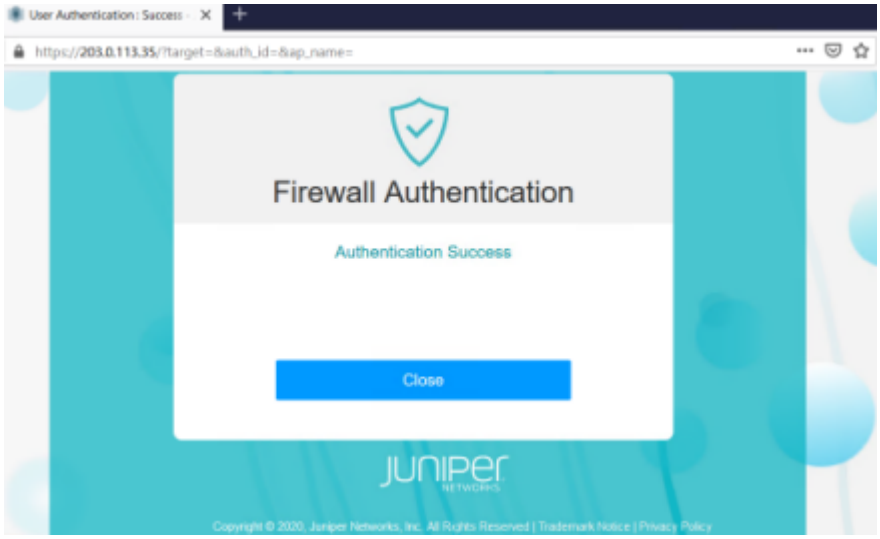
   The Firewall Authentication login page appears.



2. Type the following credentials, and then click **Log In**.

   - Username—**FWClient1**
   - Password—**$ABC123**

   Congratulations! You are successfully authenticated. You can also see the success message *Authentication Success* that you configured.

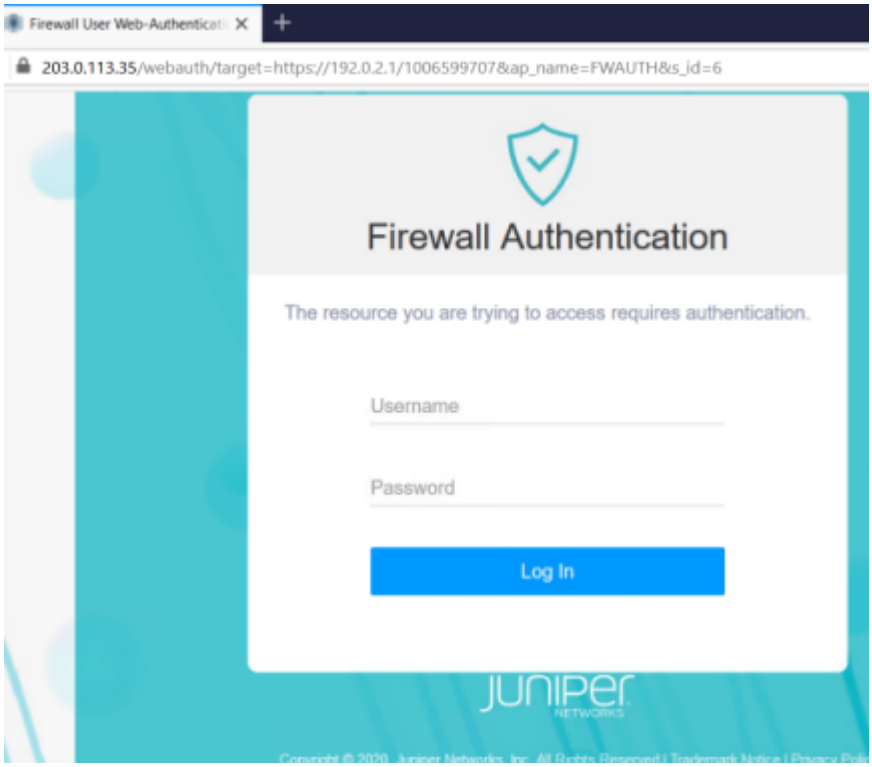


3. Click **Close**.

To verify firewall user authentication:

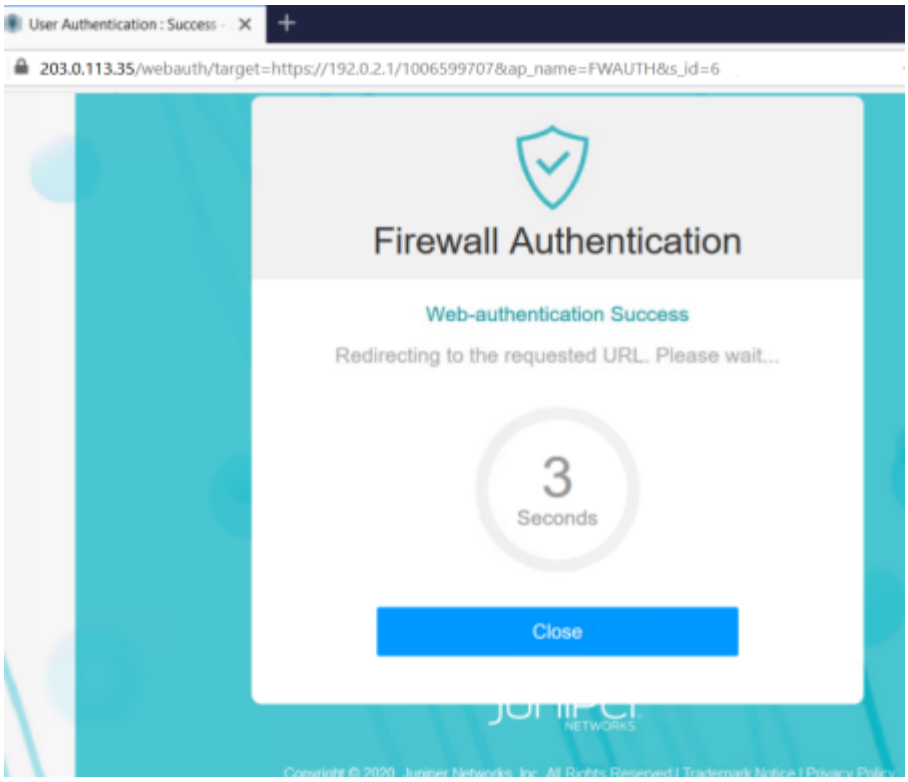
1. Type **https://192.0.2.1** in your Web browser.

   You are redirected to **https://203.0.113.35** for Web authentication.



2. Type the following credentials, and then click **Log In**.

- Username—**FWClient1**
- Password—**$ABC123**



Congratulations! You are successfully authenticated. Soon, you'll be redirected to https://192.0.2.1, and you'll be able to access the HTTPS server.

What's Next

To keep going, visit the J-Web for SRX Series Documentation page in the Juniper TechLibrary.

CHAPTER 63

Zones/Screens

IN THIS CHAPTER

About the Zones/Screens Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Zones/Screens**.

Use this page to configure zones and screens.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Zone. See "Add a Zone" on page 737.
- Edit a Zone. See "Edit a Zone" on page 740.

- Delete Zone. See "Delete Zone" on page 740.
- Add a Screen. See "Add a Screen" on page 740.
- Edit a Screen. See "Edit a Screen" on page 751.
- Delete Screen. See "Delete Screen" on page 752.

Field Descriptions

Table 210 on page 736 describes the fields on Zones/Screens page.

Table 210: Fields on Zones/Screens Page

Field	Description
Zone List	
Zone name	Displays the name of the zone.
Type	Displays the type of zone.
Host-inbound Services	Displays the services that permit inbound traffic.
Host-inbound Protocols	Displays the protocol that permit inbound traffic.
Interfaces	Displays the interfaces that are part of this zone.
Screen	Displays name of the option objects applied to the zone.
Description	Displays a description of the zone.
Screen List	
Screen name	Displays the name of the screen object.
Type	Displays the type of screen.

Table 210: Fields on Zones/Screens Page *(Continued)*

Field	Description
Description	Displays a description of the screen.

RELATED DOCUMENTATION

Add a Zone | 737

Add a Zone

You are here: **Security Policies & Objects** > **Zones/Screens**.

To add a zone:

1. Click the add icon **(+)** on the upper right side of the Zone List page.
   The Add Zone page appears.
2. Complete the configuration according to the guidelines provided in Table 211 on page 737.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 211: Fields on the Add Zone page

Field	Action
Main	
Zone name	Enter a name for the zone.
Zone description	Enter a description for the zone.
Zone type	Select a zone type: Security or Functional.
Application Tracking	Select the check box to enable application tracking support for the zone.

Table 211: Fields on the Add Zone page *(Continued)*

Field	Action
Source Identity Log	Select the check box to enable it to trigger user identity logging when that zone is used as the source zone (from-zone) in a security policy.
Traffic Control Options	Enter the following details: • Send RST for Non Matching Session—Select the check box to enable this option. Specifies that when the reset feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives. This does not match an existing session and does not have the Synchronize flag set. • Binding Screen—Select a binding screen from the list. **NOTE**: If you have already configured screens, the list shows the screen names and allows you to select or delete a screen.
Interfaces	Select interfaces from the Available column and move it to the Selected column using the arrow to include in the security zone. Starting in Junos OS Release 19.4R1, J-Web supports Wi–Fi Mini-PIM for SRX320, SRX340, SRX345, and SRX550M devices. The physical interface for the Wi-Fi Mini-PIM uses the name wl-x/0/0, where x identifies the slot on the services gateway where the Mini-PIM is installed.
Host inbound traffic - Zone	
Protocols	Specifies the protocols that permit inbound traffic of the selected type to be transmitted to hosts within the zone. Select the protocols from the Available column and move it to the Selected column using the right arrow. Select **all** to permit all protocols. **NOTE**: To deselect protocols, select the protocols in the Selected column and then use the left arrow to move them to the Available column.

Table 211: Fields on the Add Zone page *(Continued)*

Field	Action
Services	Specifies the interface services that permit inbound traffic of the selected type to be transmitted to hosts within the zone. Select the services from the Available column and move it to the Selected column using the right arrow. Select **all** to permit all services. **NOTE**: To deselect services, select the services in the Selected column and then use the left arrow to move them to the Available column.
Host inbound traffic - Interface	
Selected Interfaces	Displays the list of selected interfaces.
Interface Services	Specifies the interfaced services that permit inbound traffic from the selected interface to be transmitted to hosts within the zone. Select the interface services from the Available column and move it to the Selected column using the right arrow. Select **all** to permit all interface services. **NOTE**: If you select multiple interfaces, the existing interface services and protocols are cleared and are applied to the selected interfaces.
Interface Protocols	Specifies the interfaced protocols that permit inbound traffic from the selected interface to be transmitted to hosts within the zone. Select the interface protocols from the Available column and move it to the Selected column using the right arrow. Select **all** to permit all interface protocols.

RELATED DOCUMENTATION

Edit a Zone | 740

Edit a Zone

You are here: **Security Policies & Objects** > **Zones/Screens**.

To edit a zone:

1. Select an existing zone configuration that you want to edit on the Zones/Screens page.
2. Click the pencil icon available on the upper right side of the Zone List page.

   The Edit Zone page appears with editable fields. For more information on the options, see "Add a Zone" on page 737.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Zone | **740**

Delete Zone

You are here: **Security Policies & Objects** > **Zones/Screens**.

To delete a zone:

1. Select a zone that you want to delete on the Zones/Screens page.
2. Click the delete icon available on the upper right side of the Zone List page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Add a Screen | **740**

Add a Screen

You are here: **Security Policies & Objects** > **Zones/Screens**.

To add a screen:

1. Click the add icon **(+)** on the upper right side of the Screen List page.

   The Add Screen page appears.
2. Complete the configuration according to the guidelines provided in Table 212 on page 741.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 212 on page 741 describes the fields on the Add Screen page.

Table 212: Fields on the Add Screen Page

Field	Action
Main	
Screen name	Enter a name for the screen object.
Screen description	Enter a description for the screen object.
Generate alarms without dropping packet	Select the check box to enable this feature.
IP spoofing	Select the check box to enable this feature. Specifies that you can enable IP address spoofing. IP spoofing is when a false source address is inserted in the packet header to make the packet appear to come from a trusted source.
IP sweep	Select the check box to enable this feature. Specifies the number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.
Threshold	Enter the time interval for an IP sweep. **NOTE**: If a remote host sends ICMP traffic to 10 addresses within this interval, an IP address sweep attack is flagged and further ICMP packets from the remote host are rejected. Range: 1000 through 1000000 microseconds. The default value is 5000 microseconds.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
Port scan	Select the check box to enable this feature. Specifies the number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
Threshold	Enter the time interval for a TCP port scan. **NOTE**: If a remote host scans 10 ports within this interval, a port scan attack is flagged and further packets from the remote host are rejected. Range: 1000 through 1000000 microseconds. The default value is 5000 microseconds.
MS-Windows Defense	WinNuke attack protection—Select the check box to enable this feature. **NOTE**: WinNuke is a DoS attack targeting any computer on the Internet running Windows operating system.
IPv6 Check	Enter the following details: • Malformed IPv6—Select this check box to enable the IPv6 malformed header intrusion detection service (IDS) option. • Malformed ICMPv6—Select this check box to enable the ICMPv6 malformed IDS option.
Denial of Service	
Land attack protection	Select the check box to enable this feature. **NOTE**: Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
Teardrop attack protection	Select the check box to enable this feature. **NOTE**: Teardrop attacks exploit the reassembly of fragmented IP packets.
ICMP fragment protection	Select the check box to enable this feature. **NOTE**: ICMP packets contain very short messages. There is no legitimate reason for ICMP packets to be fragmented.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
Ping of death attack protection	Select the check box to enable this feature. **NOTE**: A ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
Large size ICMP packet protection	Select the check box to enable this feature.
Block fragment traffic	Select the check box to enable this feature.
SYN-ACK-ACK proxy protection	Select the check box to enable this feature.
Threshold	Enter the threshold value for SYN-ACK-ACK proxy protection. **NOTE**: The range is from 1 through 250000 sessions. The default value is 512 sessions.
Anomalies	

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
IP	Enter the following details: • Bad option—Select the check box to specify the number of bad options counter. • Security—Select the check box to enable the method for hosts to send security. • Unknown protocol—Select the check box to enable the IP address with security option. • Strict source route—Select the check box to enable the complete route list for a packet to take on its journey from source to destination. • Source route—Select the check box to enable this feature. Specifies the number of IP addresses of the devices set at the source that an IP transmission is allowed to take on its way to its destination. • Timestamp—Select the check box to enable the time recorded (in UTC) when each network device receives the packet during its trip from the point of origin to its destination. • Stream—Select the check box to enable a method for the 16-bit SATNET stream identifier to be carried through networks that do not support streaming. • Loose source route—Select the check box to enable a partial route list for a packet to take on its journey from source to destination. • Record route—Select the check box to enable that IP addresses of network devices along the path that the IP packet travels can be recorded.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
TCP	Enter the following details: • SYN Fragment Protection—Select the check box to enable the number of TCP SYN fragments. • SYN and FIN Flags Set Protection—Select the check box to enable the number of TCP SYN and FIN flags. **NOTE**: When you enable this option, Junos OS checks if the SYN and FIN flags are set in TCP headers. If it discovers such a header, it drops the packet. • FIN Flag Without ACK Flag Set Protection—Select the check box to enable the number of TCP FIN flags set without an ACK flag set. • TCP Packet Without Flag Set Protection—Select the check box to enable the number of TCP headers without flags set. **NOTE**: A normal TCP segment header has at least one flag control set.
Flood Defense	
Limit sessions from the same source	Enter the range within which the sessions are limited from the same source IP. Range: 1 through 50000 sessions.
Limit sessions from the same destination	Enter the range within which the sessions are limited from the same destination IP. The range is from 1 through 50000 sessions. Range: 1 through 8000000 sessions per second. The default value is 128 sessions.
ICMP flood protection	Select the check box to enable the Internet Control Message Protocol (ICMP) flood counter. **NOTE**: An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
Threshold	Enter the threshold value for ICMP flood protection. **NOTE**: Range: 1 through 4000000 ICMP pps.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
UDP flood protection	Select the check box to enable the User Datagram Protocol (UDP) flood counter. **NOTE**: UDP flooding occurs when an attacker sends IP packets containing UDP datagrams to slow system resources, such that valid connections can no longer be handled.
Threshold	Enter the threshold value for UDP flood protection. **NOTE**: Range: 1 through 100000 session. The default value is 1000 sessions.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
UDP allowlist	1. Click **Select**. The UDP Allowlist window appears. 2. Click **+** to add IP addresses that you wish to allowlist. The Add Allowlist window appears. 3. Enter the following details: • Name—Enter a Name to identify the group of IP addresses. • IPv4/IPv6 Address—Enter IPv4 or IPv6 address. • IPv4/IPv6 Address(es)—Lists the address that you have entered. **NOTE**: You can select the IP address and click **X** to delete it. 4. Click **OK** to save the changes. 5. Select the allowlist name in the UDP Allowlist page that you associated with the group of IP addresses that you entered in the Add Allowlist window from the Available column and move it to the Selected column using the right arrow. 6. Click **OK** to save the changes. **NOTE**: • The UDP Allowlist option is enabled only if you select UDP flood protection. • The allowlist that you created in the UDP Allowlist window will be available in the TCP Allowlist window also for selection. To edit an allowlist in the UDP Allowlist page, select the allowlist name and click on the pencil icon. To delete an allowlist in the UDP Allowlist page, select the allowlist name and click on the delete icon.
SYN flood protection	Select the check box to enable all the threshold and ager timeout options. Specifies that SYN flooding occurs when a host becomes so overwhelmed by SYN segments initiating incomplete connection requests that it can no longer process legitimate connection requests.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
TCP allowlist	1. Click **Select**. The TCP Allowlist window appears. 2. Click **+** to add IP addresses that you wish to allowist. The Add Allowlist window appears. 3. Enter the following details: • Name—Enter a Name to identify the group of IP addresses. • IPv4/IPv6 Address—Enter IPv4 or IPv6 address. • IPv4/IPv6 Address(es)—Lists the address that you have entered. **NOTE**: You can select the IP address and click **X** to delete it. 4. Click **OK** to save the changes. 5. Select the allowlist name in the TCP Allowlist page that you associated with the group of IP addresses that you entered in the Add Allowlist window from the Available column and move it to the Selected column using the right arrow. 6. Click **OK** to save the changes. **NOTE**: • The TCP Allowlist option is enabled only if you select SYN flood protection. • The allowlist that you created in the TCP allowlist window will be available in the UDP Allowlist window also for selection. To edit a allowlist in the TCP Allowlist page, select the allowlist name and click on the pencil icon. To delete a allowlist in the TCP Allowlist page, select the allowlist name and click on the delete icon.
Attack threshold	Enter a value to specify the number of SYN packets per second required to trigger the SYN proxy mechanism. **NOTE**: Range: 1 through 1000000 proxied requests per second. The default attack threshold value is 625 pps.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
Alarm threshold	Enter a value to specify the number of half-complete proxy connections per second at which the device makes entries in the event alarm log. **NOTE**: Range: 1 through 1000000 segments per second. The default alarm threshold value is 250 pps.
Source threshold	Enter a value to specify the number of SYN segments received per second from a single source IP address (regardless of the destination IP address and port number), before the device begins dropping connection requests from that source. **NOTE**: Range: 4 through 1000000 segments per second. The default source threshold value is 25 pps.
Destination threshold	Enter a value to specify the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based only on destination IP address, regardless of the destination port number. **NOTE**: Range: 4 through 1000000 segments per second. The default destination threshold value is 0 pps.
Ager timeout	Enter a value to specify the maximum length of time before a half-completed connection is dropped from the queue. You can decrease the timeout value until you see any connections dropped during normal traffic conditions. Range: 1 through 50 seconds. The default value is 20 seconds. **NOTE**: 20 seconds is a reasonable length of time to hold incomplete connection requests.
IPv6 EXT Header	

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
Predefined Header Type	Configure the following screen options: • Hop-by-Hop header—Select an option from the list and enter the value and click **+** to add it. To delete, select one or more headers and click **X**. • Destination header—Select an option from the list and enter the value and click **+** to add it. To delete, select one or more headers and click **X**.
Routing header	Select the check box to enable the IPv6 routing header screen option.
ESP header	Select the check box to enable the IPv6 Encapsulating Security Payload header screen option.
No-Next header	Select the check box to enable the IPv6 no next header screen option.
Mobility header	Select the check box to enable the IPv6 mobility header screen option.
Fragment header	Select the check box to enable the IPv6 fragment header screen option.
AH header	Select the check box to enable the IPv6 Authentication Header screen option.
Shim6 header	Select the check box to enable the IPv6 shim header screen option.
HIP header	Select the check box to enable the IPv6 Host Identify Protocol header screen option.
Customer Defined Header Type	Enter a value to define the type of header range and click **+** to add it. Range: 0 through 255. To delete, select one or more header types and click **X**.

Table 212: Fields on the Add Screen Page *(Continued)*

Field	Action
IPv6 ext header limit	Enter a value to set the number of IPv6 extension headers that can pass through the screen. Range: 0 through 32.
Apply to Zones	
Apply to Zones	Select zones from the Available column and move them to the Selected column using the right arrow.

RELATED DOCUMENTATION

Edit a Screen | 751

Edit a Screen

You are here: **Security Policies & Objects** > **Zones/Screens**.

To edit a screen:

1. Select an existing screen that you want to edit on the Zones/Screens page.
2. Click the pencil icon available on the upper right side of the Screen List page.

   The Edit Screen page appears with editable fields. For more information on the options, see "Add a Screen" on page 740.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Screen | 752

Delete Screen

You are here: **Security Policies & Objects** > **Zones/Screens**.

To delete a screen:

1. Select a screen that you want to delete on the Zones/Screens page.
2. Click the delete icon available on the upper right side of the Screen List page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Zones/Screens Page | **735**

CHAPTER 64

Zone Addresses

IN THIS CHAPTER

About the Zone Addresses Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Zone Addresses**.

Use this page to configure zone address or address set.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add addresses or address sets. See "Add Zone Addresses" on page 755.
- Edit addresses or address sets. See "Edit Zone Addresses" on page 758.
- Delete addresses or address sets. See "Delete Zone Addresses" on page 758.

- Clone addresses or address sets. See "Clone Zone Addresses" on page 757.
- View the details of addresses or address sets—To do this, select the address or address set for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Click the detailed view icon available to the left of the selected address or address set.
- Deselect the selected address or address set. To do this, click **More** and select **Clear All Selections**.
- Search text in the Addresses table. See "Search Text in a Zone Addresses Table" on page 758.
- Show or hide columns in the Web filtering profiles table. To do this, click the Show Hide Columns icon in the top right corner of the Web filtering profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 213 on page 754 describes the fields on the Zone Addresses page.

Table 213: Fields on the Zone Addresses Page

Field	Description
Addresses	
Zone	Displays the zone name to which the address is applied.
Name	Displays the address name.
Type	Displays the selected address type.
IP Address	Displays the IP address of the zone address.
Description	Displays the description of the address.
Address Sets	
Zone	Displays the zone name to which the address set is applied.

Table 213: Fields on the Zone Addresses Page *(Continued)*

Field	Description
Name	Displays the address sets name.
Type	Displays the selected address type.
Address List	Displays the preexisting addresses that should be included from the address set.
Address Set List	Displays the preexisting addresses that should be included from the list.
Description	Displays the description of the address set.

RELATED DOCUMENTATION

Add Zone Addresses | 755

Add Zone Addresses

You are here: **Security Policies & Objects** > **Zone Addresses**.

To create a zone address or address set:

1. Click the add icon **(+)** on the upper right side of the Zone Addresses page.
   The Create Addresses page appears.
2. Complete the configuration according to the guidelines provided in Table 214 on page 755.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 214: Fields on the Create Addresses Page

Field	Action
Object Type	Select an option from the list: Address or Address Group.

Table 214: Fields on the Create Addresses Page *(Continued)*

Field	Action
Addresses or Address Sets	
Zone	Select a zone from the list to which the address is applied.
Name	Enter the address name.
Description	Enter the description for the address.
Type	Select an option from the list: Host, Range, or DNS host.
Host IP	Enter the IPv4 or IPv6 address. **NOTE**: This option is available if you have selected Host type.
Start Address	Enter the start IPv4 or IPv6 address. **NOTE**: This option is available if you have selected Range type.
End Address	Enter the end IPv4 or IPv6 address. **NOTE**: This option is available if you have selected Range type.
DNS Name	Enter a domain hostname. The string must include alphanumeric characters, periods, dashes, no spaces are allowed and must end with an alphanumeric character. **NOTE**: This option is available if you have selected DNS Host type.
Address Sets	Displays the address set name. Select the address set.
Create Address Set	Enter the address set name and click **+** to add the address set in the Address Sets.
Address Set Name	Enter a name for address set. **NOTE**: This option is available if you have selected Address Group for Object type.

Table 214: Fields on the Create Addresses Page *(Continued)*

Field	Action
Description	Enter a description for address set. **NOTE**: This option is available if you have selected Address Group for Object type.
Address List	Specifies which of the preexisting addresses should be included or excluded from the address set. Select the addresses from the list in the Available column and then click the right arrow to move it to the Selected column. **NOTE**: This option is available if you have selected Address Group for Object type.

RELATED DOCUMENTATION

Edit Zone Addresses | **758**

Clone Zone Addresses

You are here: **Security Policies & Objects** > **Zone Addresses**.

To clone a zone address or address set:

1. Select an existing zone address or address set that you want to clone and select **Clone** from the More link.
2. Click the pencil icon available on the upper right side of the Zone Addresses page.

   The Clone Addresses page appears with editable fields. For more information on the options, see "Add Zone Addresses" on page 755.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Zone Addresses | **758**

Edit Zone Addresses

You are here: **Security Policies & Objects** > **Zone Addresses**.

To edit a zone address or address set:

1. Select an existing zone address or address set that you want to edit on the Zone Addresses page.
2. Click the pencil icon available on the upper right side of the Zone Addresses page.

   The Edit Addresses page appears with editable fields. For more information on the options, see "Add Zone Addresses" on page 755.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Zone Addresses | 758

Delete Zone Addresses

You are here: **Security Policies & Objects** > **Zone Addresses**.

To delete a zone address or address set:

1. Select a zone address or address set that you want to delete on the Zone Addresses page.
2. Click the delete icon available on the upper right side of the Zone Addresses page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Search Text in a Zone Addresses Table | 758

Search Text in a Zone Addresses Table

You are here: **Security Policies & Objects** > **Zone Addresses**.

You can use the search icon in the top right corner of the Zone Addresses page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.

   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

About the Zone Addresses Page | 753

CHAPTER 65

Global Addresses

IN THIS CHAPTER

About the Global Addresses Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Global Addresses**.

Use this page to configure global address books for security policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an Address Book. See "Add an Address Book" on page 761.
- Edit an Address Book. See "Edit an Address Book" on page 765.
- Delete an Address Book. See "Delete Address Book" on page 765.

- Upgrade the old zone-based address book to global address books. To do this, click **Upgrade** available on the right-side corner of the Global Addresses table. Click **Yes** to proceed with the upgrade to global address books and click **OK**.

Field Descriptions

Table 215 on page 761 describes the fields on the Global Addresses Page.

Table 215: Fields on the Global Addresses Page

Field	Description
Address Book Name	Displays the address book name.
Attached Zone	Displays the name of the zone that is attached to the address book.
Global	Displays information about the predefined address book. The global address book is available by default to all security zones. You do not need to attach a security zone to the global address book.
Address/Address-Set Name	Displays the addresses and address sets associated with the selected address book.
Address Value	Displays the IP address.
Address-Set Members	Displays the addresses in an address set.

RELATED DOCUMENTATION

Add an Address Book | 761

Add an Address Book

You are here: **Security Policies & Objects** > **Global Addresses**.

To add an address book:

1. Click the add icon **(+)** on the upper right side of the Global Addresses page.

   The Add Address Book page appears.
2. Complete the configuration according to the guidelines provided in Table 216 on page 762.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 216: Fields on the Global Addresses Page

Field	Action
Address Book Name	Enter a name for the address book.
Address Book Description	Enter a description for the address book.
Attach Zones	You can select more than one zone from the list for one address book. **NOTE**: Ensure that each zone has only one address book attached to it. If there is more than one address book attached to a zone, you will get the following error when you commit the configuration. `Security zone must be unique in address books.`
Addresses	

Table 216: Fields on the Global Addresses Page *(Continued)*

Field	Action
+	To add an address: 1. Click **+** available at the upper right side of the Addresses table. The Add Address page appears. 2. Enter the following details: • Address Name—Enter a name for the address. • Description—Enter a description for the address. • Address Type—Select one of the following address types from the list: ◦ IP Address ◦ Wildcard Address ◦ Domain Name ◦ Ranged Address • Value—Enter an address that matches the selected address type. 3. Click **OK** to save the changes.
Edit	To edit an address: 1. Select an existing address and click the pencil icon available at the upper right side of the Addresses table. The Add Address page appears with editable fields. 2. Click **OK** to save the changes.
Delete	Select an existing address and click the delete (**X**) icon available at the upper right side of the Addresses table to delete it.
Address Set	

Table 216: Fields on the Global Addresses Page *(Continued)*

Field	Action
+	To add an address set: 1. Click **+** available at the upper right side of the Addresses table. The Add Address Set page appears. 2. Enter the following details: • Address Set Name—Enter a name for the address set. • Description—Enter a description for the address set. • Address List—Select the address from the list in the Available column and then click the right arrow to move it to the Selected column. Specifies which of the preexisting addresses should be included or excluded from the address set. • Address Set List—Select the address sets from the list in the Available column and then click the right arrow to move it to the Selected column. Specifies which of the preexisting address sets should be included or excluded from the list. 3. Click **OK** to save the changes.
Edit	To edit an address set: 1. Select an existing address and click the pencil icon available at the upper right side of the Address Set table. The Add Address Set page appears with editable fields. 2. Click **OK** to save the changes.
Delete	Select an existing address set and click the delete (**X**) icon available at the upper right side of the Address Set table to delete it.

RELATED DOCUMENTATION

Edit an Address Book | 765

Edit an Address Book

You are here: **Security Policies & Objects** > **Global Addresses**.

To edit an address book:

1. Select an existing address book that you want to edit on the Global Addresses page.
2. Click the pencil icon available on the upper right side of the Global Addresses page.

   The Edit Address Book page appears with editable fields. For more information on the options, see "Add an Address Book" on page 761.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Address Book | 765

Delete Address Book

You are here: **Security Policies & Objects** > **Global Addresses**.

To delete an address book:

1. Select an existing address book that you want to delete on the Global Addresses page.
2. Click the delete icon available on the upper right side of the Global Addresses page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Global Addresses Page | 760

CHAPTER 66

Services

IN THIS CHAPTER

About the Services Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Services**.

Use services in policies to manage applications across devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a custom application. See "Add a Custom Application" on page 768.
- Edit a custom application. See "Edit a Custom Application" on page 771.

- Delete custom application. See "Delete Custom Application" on page 771.
- Add an application group. See "Add an Application Group" on page 772.
- Edit an application group. See "Edit an Application Group" on page 773.
- Delete an application group. See "Delete Application Group" on page 774.

Field Descriptions

Table 217 on page 767 describes the fields on the Services Page.

Table 217: Fields on the Services Page

Field	Description
Custom-Applications	
Application Name	Displays the custom application name.
Application Description	Displays a description of the custom application.
Application-Protocol	Displays the custom application protocol.
IP-Protocol	Displays the custom network protocol.
Source-Port	Displays the custom source port identifier.
Destination-Port	Displays the custom destination port identifier.
Pre-defined Applications	
Application Name	Displays the predefined application name.
Application-Protocol	Displays the predefined application protocol.
IP-Protocol	Displays the predefined network protocol.

Table 217: Fields on the Services Page *(Continued)*

Field	Description
Source-Port	Displays the predefined source port identifier.
Destination-Port	Displays the predefined destination port identifier.
Application Group	
Application Group Name	Displays the application group name.
Members	Displays members in the set.
Description	Displays a description of the application group.

RELATED DOCUMENTATION

Add a Custom Application | 768

Add a Custom Application

You are here: **Security Policies & Objects** > **Services**.

To add a custom application:

1. Click the **Custom-Applications** tab.
2. Click the add icon **(+)** on the upper right side of the Services page.
   The Add an Application page appears.
3. Complete the configuration according to the guidelines provided in Table 218 on page 769.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 218: Fields on the Add an Application Page

Field	Action
Global	
Application Name	Enter a custom application name.
Application Description	Enter a description for the custom application.
Application-protocol	Select a custom application protocol from the list.
Match IP protocol	Select a custom network protocol from the list.
Destination Port	Select a custom destination port identifier from the list.
Source Port	Select a custom source port identifier from the list.
Inactivity-timeout	Enter a value from 4 through 86400. Specifies the length of time (in seconds) that the application is inactive before it times out.
RPC-program-number	Enter a remote procedure call value from 0 through 65535.
Match ICMP message code	Select an Internet Control Message Protocol (ICMP) message code value from the list.
Match ICMP message type	Select an Internet Control Message Protocol message type value from the list.
UUID	Enter a universal unique identifier (UUID).
Application Group	Select an option from the list. Specifies the set to which this application belongs.
Terms	

Table 218: Fields on the Add an Application Page *(Continued)*

Field	Action
Add	Click **+**. The Add new term page appears.
Term Name	Enter an application term name.
ALG	Select an option from the list. Specifies the Application Layer Gateway (ALG) for the application protocol.
Match IP protocol	Select a network protocol from the list.
Destination Port	Enter the destination port identifier.
Source Port	Specifies the source port identifier.
Inactivity-timeout	Enter a value from 4 through 86400. Specifies the length of time (in seconds) that the application is inactive before it times out.
RPC-program-number	Enter a remote procedure call value from 0 through 65535.
Match ICMP message code	Select an ICMP message code value from the list.
Match ICMP message type	Select an ICMP message type value from the list.
UUID	Select an option from the list. Specifies the set to which this application belongs.
Edit	Select a term and click the pencil icon at the right corner of the table to modify the configuration.

Table 218: Fields on the Add an Application Page *(Continued)*

Field	Action
Delete	Select a term and click the delete (**X**) icon at the right corner of the table to delete the selected term.

RELATED DOCUMENTATION

Edit a Custom Application | 771

Edit a Custom Application

You are here: **Security Policies & Objects** > **Services**.

To edit a custom application:

1. Click the **Custom-Applications** tab.
2. Select an existing application that you want to edit on the Services page.
3. Click the pencil icon available on the upper right side of the Services page.

   The Edit an Application page appears with editable fields. For more information on the options, see "Add a Custom Application" on page 768.
4. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Custom Application | 771

Delete Custom Application

You are here: **Security Policies & Objects** > **Services**.

To delete a custom application:

1. Click the **Custom-Applications** tab.

2. Select an application that you want to delete on the Services page.
3. Click the delete icon available on the upper right side of the Services page.

   A confirmation message window appears.
4. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Add a Custom Application | 768

Add an Application Group | 772

Add an Application Group

You are here: **Security Policies & Objects** > **Services**.

To add an application group:

1. Click the **Application Group** tab.
2. Click the add icon **(+)** on the upper right side of the Application Group page.

   The Add New Application Set page appears.
3. Complete the configuration according to the guidelines provided in Table 219 on page 772.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 219: Fields on the Add New Application Set Page

Field	Action
Application Group Name	Enter a name for application group.
Description	Enter a description for application group.

Table 219: Fields on the Add New Application Set Page *(Continued)*

Field	Action
Application	Using the right arrow, select values from **Applications out of this set** and move them to **Applications in this set**. **NOTE**: • Enter the application name in the search box and press Enter to search for the required application. • Click **Clear** to remove the selected applications from the list of **Applications in this set** column.
Application Group	Using the right arrow, select values from **Application groups out of this group** and move them to **Application groups in this group**. **NOTE**: • Enter the application name in the search box and press Enter to search for the required application. • Click **Clear** to remove the selected applications from the list of **Application groups in this group** column.

RELATED DOCUMENTATION

Edit an Application Group | 773

Edit an Application Group

You are here: **Security Policies & Objects** > **Services**.

To edit an application group:

1. Click the **Application Group** tab.
2. Select an existing application group that you want to edit on the Services page.
3. Click the pencil icon available on the upper right side of the Services page.

   The Edit Application Set page appears with editable fields. For more information on the options, see "Add an Application Group" on page 772.

4. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Application Group | 774

Delete Application Group

You are here: **Security Policies & Objects** > **Services**.

To delete an application group:

1. Click the **Application Group** tab.
2. Select an application group name that you want to delete on the Services page.
3. Click the delete icon available on the upper right side of the Services page.

   A confirmation message window appears.
4. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Services Page | 766

CHAPTER 67

Dynamic Applications

IN THIS CHAPTER

About the Dynamic Applications Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Dynamic Applications**.

Use this page to create, modify, clone, and delete application signature groups. You can view the details of predefined application signatures that are already downloaded.

All enabled and disabled application signatures on the device are displayed in a grid format. A message `Once a new custom application signature is created or modified, the configuration is committed immediately to the device.` is displayed at the top of the page.

A status message is displayed just above the grid. It shows the version number of the installed application, the latest version available, and whether you have downloaded or installed an application package.

```
Installed application package version : 0 | Latest version 3207 available | No application package is downloaded yet
```

NOTE: If you successfully download an application package, the Install button is displayed. If you successfully install a downloaded application package, an Uninstall button is displayed.

Tasks You Can Perform

You can perform the following tasks from this page:

- Global Settings. See "Global Settings" on page 778.
- Create application signatures. See "Add Application Signatures" on page 781.
- Create application signatures group. See "Add Application Signatures Group" on page 787.
- Edit application signatures. See "Edit Application Signatures" on page 788.
- Delete application signatures. See "Delete Application Signatures" on page 788.
- Clone application signatures. See "Clone Application Signatures" on page 786.
- Search text in an application signature. See "Search Text in an Application Signatures Table" on page 789.
- View the details of application signatures—To do this, select the application signature for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected application signature profile and select **Detailed View**.
  - Mouse over to the left of the selected application signature and click **Detailed View**.
- Filter the application signatures based on select criteria. To do this, select the filter icon at the top right-hand corner of the application signatures table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.

- Show or hide columns in the application signature profiles table. To do this, click the Show Hide Columns icon in the top right corner of the application signatures table and select the options you want to view or deselect the options you want to hide on the page.
- **More**—Clone an existing application signature package, create group, or configure the page to show a detailed view.
- **Create Group**—Create a new application signature or application signatures group.

Field Descriptions

Table 220 on page 777 describes the fields on the Application Signatures page.

Table 220: Fields on the Application Signatures Page

Field	Description
Name	Displays the application signature name.
Object Type	Displays the application signature object type.
Category	Specifies the category of the application signature.
Subcategory	Specifies the subcategory of the application signature.
Risk	Displays the risk as critical, high, moderate, low, or unsafe.
Characteristic	Specifies the characteristic of the application signature.
Predefined or Custom	Displays the predefined or custom application signatures and settings that are configured on your device.
Status	Displays the status of the application signature.

RELATED DOCUMENTATION

Global Settings | 778

Global Settings

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To add global settings:

1. Click the **Global Settings** on the upper right side of the Application Signatures page.
   The Global Settings page appears.
2. Complete the configuration according to the guidelines provided in Table 221 on page 778.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 221: Fields on the Global Settings Option Page

Field	Action
General	
Custom Application Byte Limit	Select the byte limit in the range 0 through 10000. This helps in understanding when to stop the identification of custom applications.
Micro Applications	Enable micro-application detection in application identification and then use them as matching criteria in a security policy.
Application System Cache Enable or disable storing of AI result in application cache, configure ASC security services, configure miscellaneous services such as ABPR, or set the cache entry timeout.	
Application Cache	Enable this option to save the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service.

Table 221: Fields on the Global Settings Option Page *(Continued)*

Field	Action
Security Services	Enable this option for security services, such as security policies, application firewall (AppFW), Juniper ATP Cloud, IDP, and UTM
Miscellaneous Services	Enable this option for miscellaneous services, such as APBR and AppTrack.
Cache entry timeout	Enter the timeout value in seconds for the application system cache (ASC) entries. Range: 0 through 1000000 seconds. Default is 3600 seconds.
Packet Capture	
Global packet capture	Enable packet capture globally to capture all unknown application traffic. You can also enable this option specific to a security policy at the rule level. For more information, see "Add a Rule" on page 690.
Aggressive mode	Enable to capture all traffic before AppID classifies the applications. In this mode, the system captures all application traffic regardless of the application system cache (ASC) entry. Packet capture starts for the first packet of the first session.
Exclude inconclusive traffic	Disable packet capture of inconclusive traffic. This option is available when you enable the Aggressive mode option. This option disables the packet capture for the following sessions: • Sessions closed before the application identification or classification completes. • Sessions not classified even though they reach the maximum packet capture limit. If you do not configure this option, by default, the system captures packets for inconclusive sessions.
Advanced	
Maximum packets	Maximum number of UDP packets per session. Range: 1 through 1000. Default is 10 packets.

Table 221: Fields on the Global Settings Option Page *(Continued)*

Field	Action
Maximum bytes	Maximum number of TCP bytes per session. For TCP sessions, the count includes the actual payload data length and excludes IP/TCP headers for the maximum bytes limit. Range: 40 through 1,073,741,824. Default is 6000 bytes.
Maximum files	Maximum number of unique packet capture files to create before the oldest file is overwritten by a new file created. Range: 1 through 2500. Default is 100.
Maximum storage	Maximum disk space (bytes) that can be used in the Routing Engine for packet capture files. Range: 1 through 4096 MB. Default is 50 MB.
Maximum memory	Maximum memory limit for deep packet inspection (DPI). Range: 1 KB through maximum bytes (depending on the available space on the device).
Packet capture interval	Timeout value in minutes to avoid repetitive capture of same traffic. After this interval, the system continues to capture newer packet details for unknown applications until the capture limit is reached. Range: 1 through 525,600 minutes. Default is 1440 minutes (24 hours).
Repeat traffic capture	Number of repetitive captures of same traffic. Use this option to limit the number of times the same traffic can be repeatedly captured before the cache entry times out. Range: 1 through 1000. Default is 5.

RELATED DOCUMENTATION

- About the Dynamic Applications Page | **775**
- Add Application Signatures | **781**
- Add Application Signatures Group | **787**

Add Application Signatures

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To add an application signature:

1. Click **Create** > **Signature** on the upper right side of the Dynamic Applications page.
   The Create Application Signatures page appears.
2. Complete the configuration according to the guidelines provided in Table 222 on page 781.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 222: Fields on the Add Application Signatures Page

Field	Action
Name	Enter the application signature name.
Description	Enter the application signature description.
Order	Enter the order of the custom application. Lower order has higher priority. The range is 1 through 50,000.

Table 222: Fields on the Add Application Signatures Page *(Continued)*

Field	Action
Priority	Enter the priority over other signature applications. Select an option from the list: • High • Low Starting in Junos OS Release 20.2R1, by default, the priority for the custom application is set to **Low**. This allows a predefined application to take precedence. If you want to override a predefined application, you must set the priority to **High**.
Risk	Enter the risk as critical, high, moderate, low, or unsafe.
Application Identification match criteria	Select one or more options from the list: • ICMP Mapping • IP Protocol Mapping • Address Mapping • L7 Signature
ICMP Mapping	Select a value from the list. • ICMP Type—Select the numeric value of an ICMP type. The type identifies the ICMP message, such as Unassigned or Destination Unreachable. The range is from 0 through 254. • Select the numeric value of an ICMP code. The code field provides further information (such as RFCs) about the associated type field. The range is from 0 through 254.
IP Protocol Mapping	Select the numeric value of an ICMP type. The type identifies the ICMP message, such as Unassigned or Destination Unreachable. The range is from 0 through 254.

Table 222: Fields on the Add Application Signatures Page *(Continued)*

Field	Action
Address Mapping	To add a new address mapping: 1. Click **Add**. The Add Address Mapping page appears. Enter the following details: • Name—Enter the name of the address mapping. • IP Address—Enter an IPv4 or IPv6 address. • CIDR Range—Enter an IPv4 or IPV6 address prefix for classless IP addressing. • TCP Port range—Enter the TCP port range for the application. • UDP Port Range—Enter the UDP port range for the application. 2. Click the pencil icon at the top right side of the Address Mapping table. Then, edit the address mapping and click **OK**. 3. To delete an existing Address Mapping, select it and click the delete icon or right-click on it and click **Delete**.
L7 Signature	
Cacheable	Set this option to **True** only when L7 signatures are configured in a custom signature. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.
Add L7 Signature	Click **Add L7 Signature** list and select an option from the following: • Over HTTP • Over SSL • Over TCP • Over UDP The Add Signature page appears.

Table 222: Fields on the Add Application Signatures Page *(Continued)*

Field	Action
Add Signature	
Over Protocol	Displays the signature that matches the application protocol. Example: HTTP
Signature Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Port Range	Enter the port range for the application. Range is 0-65535.
Add Members Custom signatures can contain multiple members that define attributes of an application. The supported member name range is m01 through m15.	
+	Click **+** to create a member.
Context (Over HTTP)	Select the service-specific context from the following list: • http-get-url-parsed-param-parsed • http-header-content-type • http-header-cookie • http-header-host • http-header-user-agent • http-post-url-parsed-param-parsed • http-post-variable-parsed • http-url-parsed • http-url-parsed-param-parsed

Table 222: Fields on the Add Application Signatures Page *(Continued)*

Field	Action
Context (Over SSL)	Select the service-specific context as ssl-server-name.
Context (Over TCP)	Select the service-specific context as stream.
Context (Over UDP)	Select the service-specific context as stream.
Direction	Select the direction of the packet flow to match the signature: • any—The direction of the packet flow can either be from the client-side to the server-side or from the server-side to the client-side. • client-to-server—The direction of packet flow is from the client-side to the server-side. • server-to-client—The direction of packet flow is from the server-side to the client-side.
Depth	Enter the maximum number of bytes to check for context match. Use the byte limit for AppID to identify custom application pattern for applications running over TCP or UDP or Layer 7 applications. Range is 1 through 8000. The Depth is set to 1000 by default, if not explicitly configured. **NOTE**: Starting in Junos OS Release 20.2R1, Depth option is supported.
Pattern	Enter the deterministic finite automaton (DFA) pattern matched the context. The DFA pattern specifies the pattern to be matched for the signature. The maximum length is 128.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
20.2R1	Starting in Junos OS Release 20.2R1, Depth option is supported.

RELATED DOCUMENTATION

About the Dynamic Applications Page | 775

Global Settings | 778

Add Application Signatures Group | 787

Edit Application Signatures | 788

Delete Application Signatures | 788

Clone Application Signatures | 786

Search Text in an Application Signatures Table | 789

Clone Application Signatures

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To clone an application signature:

1. Select the application signature profile that you want to clone and select **Clone** from the More link.

   NOTE: Alternatively, you can right-click on the selected application signature profile and select **Clone**.

   The Clone Application Signature page appears with editable fields. For more information on the fields, see "Add Application Signatures" on page 781.

2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

About the Dynamic Applications Page | 775

Global Settings | 778

Add Application Signatures | 781

Add Application Signatures Group | 787

Edit Application Signatures | 788

Delete Application Signatures | 788

Search Text in an Application Signatures Table | 789

Add Application Signatures Group

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To add an application signature group:

1. Click **Create** > **Signature Group** on the upper right side of the Dynamic Applications page. You can also click **More** and select **Create Group**.

   The Create Application Signature Group page appears.
2. Complete the configuration according to the guidelines provided in Table 223 on page 787.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 223: Fields on the Add Application Signature Group Page

Field	Action
Name	Enter the application signature group name.
Group Members	Enter the add or remove applications associated with the application signature group. Click one of the following options: • **Add**—Click **+** to create an application signature group. • **Delete**—Select an existing application signature group that you want to delete and click the delete icon available at the upper right of the application signature group table. • **Detailed View**—Hover over the application signature group name and click the Detailed View icon to view the signature group. You can also click **More** and select **Detailed View** for the selected signature group.

RELATED DOCUMENTATION

About the Dynamic Applications Page | 775

Edit Application Signatures | 788

Delete Application Signatures | 788

Clone Application Signatures | 786

Search Text in an Application Signatures Table | 789

Edit Application Signatures

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To edit an application signature:

1. Select an existing application signature that you want to edit on the Dynamic Applications page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Application Signatures page appears with editable fields. For more information on the options, see "Add Application Signatures" on page 781.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Dynamic Applications Page | **775**
- Global Settings | **778**
- Add Application Signatures | **781**
- Add Application Signatures Group | **787**
- Add Application Signatures Group | **787**
- Delete Application Signatures | **788**
- Clone Application Signatures | **786**
- Search Text in an Application Signatures Table | **789**

Delete Application Signatures

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To delete application signatures:

1. Select an application signature that you want to delete on the Dynamic Applications page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Dynamic Applications Page | **775**

Search Text in an Application Signatures Table

You are here: **Security Policies & Objects** > **Dynamic Applications**.

You can use the search icon in the top right corner of the Dynamic Applications page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.

   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

CHAPTER 68

Application Tracking

IN THIS CHAPTER

About the Application Tracking Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Application Tracking**.

Use this page to configure application tracking.

Field Description

To configure application tracking:

1. Complete the configuration according to the guidelines provided in Table 224 on page 790.
2. Click **Save** to save the changes.

Table 224 on page 790 describes the fields on the Application Tracking page.

Table 224: Fields on the Application Tracking Page

Field	Description
Application tracking	Select this option to enable application tracking.

Table 224: Fields on the Application Tracking Page *(Continued)*

Field	Description
Logging Type	Select an option: • **Log as session(s) created**—Generates a log message when a session is created. By default, this option is disabled. • **Delay logging first session**—Enables you to specify the length of time that must pass before the first log message is created. The default is 1 minute.
First Update Interval (min)	Use the up/down arrow to set the interval time.
Session Update Interval (min)	Use the up/down arrow to set the interval time.
Application Tracking By Zone	Lists the available zones. • To enable application tracking, select the zone and click the right arrow to move it to the tracking enabled list. • To disable application tracking, select the zone and then click the left arrow to move the zone back into the available list.

RELATED DOCUMENTATION

About the Address Pools Page | 973

CHAPTER 69

Schedules

IN THIS CHAPTER

About the Schedules Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Schedules**.

Use this page to configure security policy schedules.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a schedule. See "Add a Schedule" on page 794.
- Clone a schedule. See "Clone a Schedule" on page 796.
- Edit a schedule. See "Edit a Schedule" on page 796.

- Delete a schedule. See "Delete Schedule" on page 797.
- View the details of schedules—To do this, select the schedule for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected custom object and select **Detailed View**.
  - Mouse over to the left of the selected custom object and click **Detailed View**.
- Deselect the selected schedules. To do this, click **More** and select **Clear All Selections**.
- Search text in the Schedules table. See "Search Text in Schedules Table" on page 797.
- Show or hide columns in the Schedules table. To do this, click the Show Hide Columns icon in the top right corner of the Schedules table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 225 on page 793 describes the fields on the Schedules Page.

Table 225: Fields on the Schedules Page

Field	Description
Name	Displays the name of the policy schedule.
Description	Displays a description of the policy schedule.
Start Date	Displays the start date for the first day.
End Date	Displays the stop date for the first day.
Second Start Date	Displays the start date for the second day.
Second End Date	Displays the stop date for the second day.
Schedules	On expanding, displays the days of the schedule, exclusion days if any, and the start and end time of the schedule.

RELATED DOCUMENTATION

Add a Schedule | 794

Add a Schedule

You are here: **Security Policies & Objects** > **Schedules**.

To add a schedule:

1. Click the add icon **(+)** on the upper right side of the Schedules page.
   The Create Schedule page appears.
2. Complete the configuration according to the guidelines provided in Table 226 on page 794.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 226: Fields on the Create Schedule Page

Field	Action
General	
Name	Enter the name of the scheduler.
Description	Enter a description for the scheduler.
Dates	
Start Date	Select the start date for the first day from the calendar and select the time in AM, PM, or 24 ours format.
Stop Date	Select the stop date for the first day from the calendar and select the time in AM, PM, or 24 ours format.
Second Start Date	Select the start date for the second day from the calendar and select the time in AM, PM, or 24 ours format.
Second End Date	Select the stop date for the second day from the calendar and select the time in AM, PM, or 24 ours format.

Table 226: Fields on the Create Schedule Page *(Continued)*

Field	Action
Time Ranges	
Time Ranges	Select the check box to specify the time range.
Daily Options	1. Click on the day to specify the time for a particular day. The Specify Time for <*Selected Day*> page appears. **NOTE**: Click **Specify the same time for all days** to configure the same time options to all days. 2. Select an option for time: • All Day—Specifies time options for an entire day. • Exclude Day—Excludes a specific day. • Time Ranges—Enter time ranges for the selected day: • Start Time—Enter the first day start time in HH:MM:SS and select AM, PM, or 24 hours format. • End Time—Enter the first day end time first day in HH:MM:SS and select AM, PM, or 24 hours format. • Second Start Time—Click **+** and enter the second day start time in HH:MM:SS, and then select AM, PM, or 24 hours format. • Second End Time—Enter the second day end time in HH:MM:SS and select AM, PM, or 24 hours format. **NOTE**: Click **X** to delete the second day start and end time. 3. Click **OK** to save changes.

RELATED DOCUMENTATION

Edit a Schedule | 796

Clone a Schedule

You are here: **Security Policies & Objects** > **Schedules**.

To clone a schedule:

1. Select a schedule that you want to clone and select **Clone** from the More link.

   The Clone Schedule page appears with editable fields. For more information on the fields, see "Add a Schedule" on page 794.

   > **NOTE**: Alternatively, you can right-click on the selected schedule and select **Clone**.

2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

Edit a Schedule | 796

Edit a Schedule

You are here: **Security Policies & Objects** > **Schedules**.

To edit a schedule:

1. Select an existing schedule that you want to edit on the Schedules page.
2. Click the pencil icon available on the upper right side of the Schedules page.

   The Edit Schedules page appears with editable fields. For more information on the options, see "Add a Schedule" on page 794.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

Delete Schedule | 797

Delete Schedule

You are here: **Security Policies & Objects** > **Schedules**.

To delete a schedule:

1. Select a schedule that you want to delete on the Schedules page.
2. Click the delete icon available on the upper right side of the Schedules page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Search Text in Schedules Table | 797

Search Text in Schedules Table

You are here: **Security Policies & Objects** > **Schedules**.

You can use the search icon in the top right corner of the Schedules page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.

   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

About the Schedules Page | 792

CHAPTER 70

Proxy Profiles

IN THIS CHAPTER

About the Proxy Profiles Page

IN THIS SECTION

You are here: **Security Policies & Objects** > **Proxy Profiles**.

Use this page to configure the proxy profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a proxy profile. See "Add a Proxy Profile" on page 800.
- Edit a proxy profile. See "Edit a Proxy Profile" on page 801.
- Delete a proxy profile. See "Delete Proxy Profile" on page 801.

- Filter the proxy profile based on select criteria. To do this, select the filter icon at the top right-hand corner of the Proxy Profiles table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the Proxy Profiles table. To do this, click the Show Hide Columns icon in the top right corner of the Proxy Profiles table and select the options you want to view or deselect the options you want to hide on the page.
- Advanced search for proxy profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 227 on page 799 describes the fields on the Proxy Profiles Page.

Table 227: Fields on the Proxy Profiles Page

Field	Description
Profile Name	Displays the name of the proxy profile.
Server IP / Host Name	Displays the connection type used by the proxy profile.
Port Number	Displays the port number.

RELATED DOCUMENTATION

Add a Proxy Profile | 800

Add a Proxy Profile

You are here: **Security Policies & Objects** > **Proxy Profiles**.

To add a proxy profile:

1. Click the add icon **(+)** on the upper right side of the Proxy Profiles page.
   The Create Proxy Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 228 on page 800.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 228 on page 800 describes the fields on the Create Proxy Profile Page.

Table 228: Fields on the Create Proxy Profile Page

Field	Action
Profile Name	Enter a name of the proxy profile.
Connection Type	Select the type of connection used by the proxy profile: • Server IP—Enter the server IP address. • Host Name—Enter a hostname.
Port Number	Enter the port number used by the proxy profile. Range: 0 through 65535.

RELATED DOCUMENTATION

Edit a Proxy Profile | 801

Edit a Proxy Profile

You are here: **Security Policies & Objects** > **Proxy Profiles**.

To edit a proxy profile:

1. Select an existing proxy profile that you want to edit on the Proxy Profiles page.
2. Click the pencil icon available on the upper right side of the Proxy Profiles page.

   The Edit Proxy Profile page appears with editable fields. For more information on the options, see "Add a Proxy Profile" on page 800.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete Proxy Profile | 801

Delete Proxy Profile

You are here: **Security Policies & Objects** > **Proxy Profiles**.

To delete a proxy profile:

1. Select a proxy profile that you want to delete on the Proxy Profiles page.
2. Click the delete icon available on the upper right side of the Proxy Profiles page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

Add a Proxy Profile | 800

Edit a Proxy Profile | 801

PART 8

Security Services

CHAPTER 71

UTM Default Configuration

IN THIS CHAPTER

About the Default Configuration Page

IN THIS SECTION

You are here: **Security Services** > **UTM** > **Default Configuration**.

The Default Configuration page describes the security features of Unified Treat Management .

This default configuration will be used, if there are multiple UTM policies present in the potential list. The global configuration will be used till the exact match is found in the potential list.

The following security features are parts of UTM default configuration:

- **Antivirus**—Antivirus is an in-the-cloud antivirus solution. The virus pattern and malware database are located on external servers maintained by Sophos (Sophos Extensible List) servers.
- **Web Filtering**—Web filtering lets you to manage Internet usage by preventing access to inappropriate Web content.
- **Antispam**—This feature examines transmitted messages to identify any e-mail spam.

- **Content Filtering**—This feature blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the collapsed or expanded details of the UTM default configuration options. To do this, select any one of the UTM default configurations and click **Expand All** or **Collapse All** available on the upper right side of the page.
- Edit a default configuration. See "Edit a Default Configuration" on page 806.
- Delete a default configuration. See "Delete Default Configuration" on page 806.

Field Descriptions

Table 229 on page 805 describes the fields on the Default Configuration page.

Table 229: Fields on the Default Configuration Page

Field	Function
Anti-Virus	Displays the configured antivirus. You can edit the configured antivirus.
Web Filtering	Displays the configured Web filtering. You can edit the configured web filtering.
Anti-Spam	Displays the configured antispam. You can edit the configured antispam.
Content Filtering	Displays the configured content filtering. You can edit the configured content filtering.

RELATED DOCUMENTATION

Edit a Default Configuration | 806

Delete Default Configuration | 806

Edit a Default Configuration

You are here: **Security Services** > **UTM** > **Default Configuration**.

You can edit all of the following UTM default configurations:

- Antivirus
- Web filtering
- Antispam
- Content filtering

To edit a default configuration:

1. Select any of the existing UTM default configurations that you want to edit on the Default Configuration page.
2. Click the pencil icon available on the upper right side of the page.

   The edit page for the selected default configuration appears with editable fields. You can modify any previous changes done to Antivirus, Web Filtering, Antispam, and Content Filtering.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Default Configuration Page | 804

Delete Default Configuration | 806

Delete Default Configuration

You are here: **Security Services** > **UTM** > **Default Configuration**.

You can delete all of the following UTM default configurations:

- Antivirus
- Web filtering
- Antispam
- Content filtering

To delete an individual default configuration:

1. Select any of the existing UTM default configurations that you want to delete on the Default Configuration page.
2. Click the delete icon available on the upper right side of the page.

   The Confirm Delete window appears.

   NOTE: You can only delete the configured data and not the junos-default configuration.

3. Click **Yes** to delete or click **No** to retain the profile.

To delete all the default configuration at the same time:

1. Click **Delete All Default Configurations** available on the upper right side of the page.

   The Confirm Delete window appears.

   NOTE: You can only delete the configured data and not the junos-default configuration.

2. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Default Configuration Page | 804

Edit a Default Configuration | 806

CHAPTER 72

UTM Antivirus Profiles

IN THIS CHAPTER

About the Antivirus Profiles Page

IN THIS SECTION

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

Use this page to configure antivirus.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an antivirus profile. See "Add an Antivirus Profile" on page 810.
- Clone an antivirus profile. See "Clone an Antivirus Profile" on page 816.
- Edit an antivirus profile. See "Edit an Antivirus Profile" on page 816.

- Delete antivirus profile. See "Delete Antivirus Profile" on page 817.
- View the details of an antivirus profile—To do this, select the antivirus profile for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected antivirus profile and select **Detailed View**.
  - Mouse over to the left of the selected antivirus profile and click **Detailed View**.
- Advanced search for antivirus profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.
- Filter the antivirus profiles based on select criteria. To do this, select the filter icon at the top right-hand corner of the antivirus profiles table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the antivirus profiles table. To do this, click the Show Hide Columns icon in the top right corner of the antivirus profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 230 on page 810 describes the fields on the Antivirus Profiles page.

Table 230: Fields on the Antivirus Profiles Page

Field	Function
Name	Displays the unique name of the antispam profile.
URL Allowlist	Specifies a unique customized list of all URLs or IP addresses for a given category that are to be bypassed for scanning.
Default Action	Displays the default fallback action taken when the antivirus system encounters errors.

RELATED DOCUMENTATION

- Add an Antivirus Profile | 810
- Edit an Antivirus Profile | 816
- Delete Antivirus Profile | 817

Add an Antivirus Profile

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

To add an antivirus profile:

1. Click the add icon **(+)** available on the upper right side of the Antivirus Profiles page.

   The Create Antivirus Profiles wizard appears, displaying brief instructions about creating an antivirus profile.
2. Click **Next** to navigate to the next page.
3. Complete the configuration according to the guidelines provided in Table 231 on page 811.
4. Click **Finish**.

   The Summary page is displayed with the configurations you have made.
5. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.
6. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

   A new antivirus profile is created. You can assign this antivirus profile to a UTM policy. Within the UTM policy, you can apply either the same or different antivirus profiles to the Web, file transfer and E-mail traffic.

Table 231: Fields on the Create Antivirus Profile Page

Field	Function
General	
Name	Enter a unique name for the antivirus profile. The maximum length is 29 characters.
URL Allowlist	Select the customized object from the list for a given category that are to be bypassed for scanning.
MIME Allowlist	

Table 231: Fields on the Create Antivirus Profile Page *(Continued)*

Field	Function
MIME Allowlist	Select a MIME allowlist from the list. To create a MIME list inline and add it to the MIME allowlist: **1.** Click **Create New MIME List**. The Add MIME Pattern List window appears. **2.** Enter the following details: • Name—Enter a unique name for the MIME pattern list. You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 40 characters. • Values—Click **+** and enter a value in the value list and click the tick mark. **NOTE**: Value must be two strings separated by slash(/): • The first string beginning with a letter or number and consisting of alphanumeric characters, underscores and dashes. Dashes cannot be used consecutively in the string. • The second string can be null or begin with a letter or number and consisting of alphanumeric characters, underscores, dashes, dots and pluses. Dashes, dots, and pluses cannot be used consecutively in the string. If you want to delete any MIME pattern values, select the value and click the delete icon. **3.** Click **OK**. A new MIME list is created and added to the MIME allowlist.
Exception MIME Allowlist	Select an exception MIME allowlist from the list. Click **Create New MIME list** to create and add a MIME pattern list inline.

Table 231: Fields on the Create Antivirus Profile Page *(Continued)*

Field	Function
Fallback Options	
Fallback options are used when the antivirus system experiences errors and must fall back to one of the previously configured actions to either deny (block) or permit the object.	
Content Size	Select **Block** or **Log and Permit**. If the content size exceeds a set limit, the content is either passed or blocked. The default action is Block.
Engine Error	Select **Block** or **Log and Permit** to specify whether the scan engine should be blocked (default) or logged and permitted if it is not ready during certain processes. For example, while the signature database is loading.
Trickling Timeout	Select **Block** or **Log and Permit** to specify whether the time taken to scan should be blocked (default) or logged and permitted if the scan process exceeds the timeout setting in the antivirus profile.
Out of Resources	Select **Block** or **Log and Permit** to specify whether the resource constraints should be blocked (default) or logged and permitted if the error is received during virus scanning.
Decompress Layer	Select **Block** or **Log and Permit** to specify whether the number of layers of nested compressed files that the internal antivirus scanner can decompress before the execution of the virus scan. The default action is Block.
Too many Requests	Select an option to specify whether the number of messages should be blocked (default) or logged and permitted if the messages received concurrently exceeds the device limits.
Default Action	Select a default action to take when an error occurs; **Block** or **Log and Permit**.

Table 231: Fields on the Create Antivirus Profile Page *(Continued)*

Field	Function
Notification Options	
Use the notification options to configure a method of notifying the user when a fallback occurs or a virus is detected.	
Fallback Deny	
Notify Mail Sender	Select this option to configure e-mail notifications to notify the administrator about the errors returned by either the scan engine or the scan manager when a fallback action occurs.
Notification Type	Select **None**, **Protocol**, or **Message** from the list to specify the type of notification sent when a fallback option of deny is triggered.
Custom Message Subject	Enter the subject line text for your custom message for the fallback deny notification. The maximum character length is 255.
Custom Message	Enter the customized message text for the fallback deny notification. The maximum character length is 512.
Fallback Non-Deny	
Notify Mail Recipient	Select this option to configure E-mail notifications to notify the recipient when a fallback e-mail option without a deny action is triggered.
Custom Message Subject	Enter the subject line for your custom message for the fallback non-deny notification. The maximum character length is 255.

Table 231: Fields on the Create Antivirus Profile Page *(Continued)*

Field	Function
Custom Message	Enter the customized message text for the fallback non-deny notification. The maximum character length is 512.
Virus Detection	
Notify Mail Sender	Select this option to configure E-mail notifications to notify the administrator when a virus is detected.
Notification Type	Specifies the type of notification to be sent when a virus is detected. Select **None**, **Protocol**, or **Message** from the list to specify the type of notification sent when a virus is detected.
Custom Message Subject	Enter the subject line text for your custom message for the virus detection notification. The maximum character length is 255.
Custom Message	Enter the customized message text for the virus detection notification. The maximum character length is 512.

RELATED DOCUMENTATION

- About the Antivirus Profiles Page | **808**
- Edit an Antivirus Profile | **816**
- Delete Antivirus Profile | **817**

Clone an Antivirus Profile

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

To clone an antivirus profile:

1. Select an antivirus profile that you want to clone and select **Clone** from the More link.

   NOTE: Alternatively, you can right-click on the selected antivirus profile and select **Clone**.

   The Clone Antivirus Profiles page appears with editable fields. For more information on the options, see "Add an Antivirus Profile" on page 810.

2. Click **OK** to save the changes.

   A cloned antivirus profile is created for the selected antivirus profile. By default, the name of the cloned antivirus profile is in the format: ***<Antivirus profile name>***_**clone**.

RELATED DOCUMENTATION

About the Antivirus Profiles Page | **808**

Edit an Antivirus Profile | **816**

Delete Antivirus Profile | **817**

Edit an Antivirus Profile

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

To edit an antivirus profile:

1. Select an existing antivirus profile that you want to edit on the Antivirus Profiles page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Antivirus Profiles page appears with editable fields. For more information on the options, see "Add an Antivirus Profile" on page 810.

   NOTE: Alternatively, you can right-click on the selected antivirus profile and select **Edit Antivirus Profiles**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Antivirus Profiles Page | 808
Edit an Antivirus Profile | 816
Delete Antivirus Profile | 817

Delete Antivirus Profile

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

To delete an antivirus profile:

1. Select an antivirus profile that you want to delete on the Antivirus Profiles page.
2. Click the delete icon available on the upper right side of the page.

> **NOTE**: Alternatively, you can right-click on the selected antivirus profile and select **Delete Antivirus Profiles**.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Antivirus Profiles Page | 808
Add an Antivirus Profile | 810
Edit an Antivirus Profile | 816

Prevent Virus Attacks by Using J-Web UTM Antivirus

SUMMARY

Learn about Unified Threat Management antivirus protection and how to configure UTM antivirus to prevent virus attacks on SRX Series devices by using J-Web. The UTM antivirus feature on the SRX Series

IN THIS SECTION

device scans network traffic to protect your network from virus attacks and to prevent virus spread.

UTM Antivirus Overview

In today's world, where cyber security threats are evolving and getting more sophisticated, protecting your network from virus attacks is extremely critical. The viruses, worms, and malware perform unwanted and malicious acts, such as damaging or deleting files, hacking personal data, affecting system performance, reformatting the hard disk, or using your computer to transmit viruses to other computers. The UTM antivirus software acts like a first line of defense against such security threats and prevents the spread of viruses into your network. It protects your network from virus attacks, unwanted computer malwares, spywares, rootkits, worms, phishing attacks, spam attacks, trojan horses, and so on.

NOTE: You must always ensure that the antivirus software and virus pattern database are up to date.

Juniper Networks offers the following UTM antivirus solutions:

- On-device antivirus protection

  The on-device antivirus is an on-box solution. The on-device antivirus scan engine scans the data by accessing the virus pattern database that is locally stored on the device. It provides a full file-based antivirus scanning function that is available through a separately licensed subscription service.

NOTE:

- The on-device Express or Kaspersky scan engine is not supported from Junos OS Release 15.1X49-D10 onwards; however, it is still applicable for Junos OS Release 12.3X48.
- Starting in Junos OS Release 18.4R1, SRX Series devices support the Avira on-device antivirus scanning engine.
- Avira on-device antivirus scanning engine is not supported on SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 HM devices.

- Sophos antivirus protection

  Sophos antivirus is an in-the-cloud antivirus solution. The virus pattern and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers. The Sophos antivirus scanner also uses a local internal cache to maintain query responses from the external list server. We offer the Sophos antivirus scanning as a less CPU-intensive alternative to the full file-based antivirus feature.

Benefits of UTM Antivirus

- The on-device antivirus solution:
  - Scans the application traffic locally without connecting to the server to query whether the application traffic has virus.
  - Minimizes processing delays because the pattern database is locally stored and the scan engine is on-device.
- The Sophos antivirus solution:
  - Avoids downloading and maintaining large pattern databases on the Juniper device because the virus pattern and malware database is located on external servers maintained by Sophos.
  - Improves lookup performance because the Sophos antivirus scanner uses a local internal cache to maintain query responses from the external list server.
  - Effectively prevents malicious content from reaching the endpoint client or server through the use of the Uniform Resource Identifier (URI) checking functionality.

Antivirus Workflow

IN THIS SECTION

Scope

Juniper Web (J-Web) Device Manager supports the UTM antivirus solution on SRX Series devices. In this example, you'll use Sophos antivirus protection to do the following:

1. Scan HTTP and FTP traffic from a server (10.102.70.89) to your computer for virus attacks.
2. Define a custom message **Virus Found!** to be displayed when a virus is found while scanning the traffic.
3. Create Allowlist URL (http://10.102.70.89) where AV scanning is skipped.

> **NOTE**: Assumption is that you must be able to route to the example URLs.

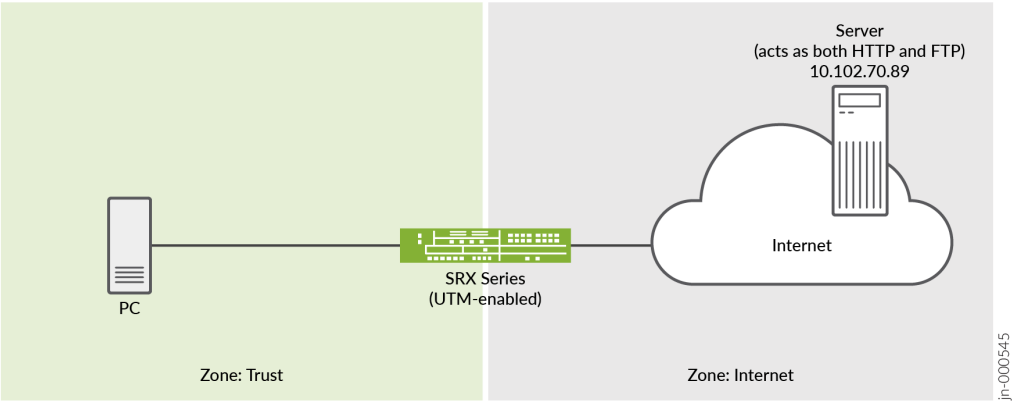
Before You Begin

- Install a valid Sophos antivirus license and application identification feature license. See Installation and Upgrade Guide, Licensing Administration Guide, and Licensing User Guide.
- Install an application signatures package for application identification. See Application Security User Guide for Security Devices.
- Ensure that the SRX Series device you use in this example runs Junos OS Release 20.4R1.

Topology

The topology used in this example comprises a PC connected to a UTM-enabled SRX Series device that has access to the Internet and a server. You'll use J-Web to scan the HTTP and FTP requests sent to the

server with this simple setup. You'll then use Sophos antivirus protection to prevent virus attacks from the server to your PC.



Video

See the following video to learn how to configure UTM antivirus using J-Web.

Video: Configure UTM Antivirus Using J-Web

Sneak Peek – J-Web UTM Antivirus Configuration Steps

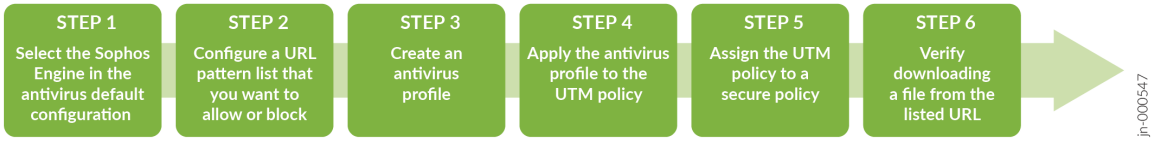


Table 232: J-Web UTM Antivirus Configuration Steps

Step	Action
Step 1	Configure the Sophos engine in Default Configuration. Here, you first define the default engine as Sophos in Default Configuration.

Table 232: J-Web UTM Antivirus Configuration Steps *(Continued)*

Step	Action
Step 2	Configure antivirus custom object. Here, you define the URL pattern list (allowlist) of URLs or addresses that will be bypassed by antivirus scanning. After you create the URL pattern list, you will create a custom URL category list and add the pattern list to it.
Step 3	Configure an antivirus feature profile using the Sophos engine. After the default configuration, you define the parameters that will be used for virus scanning in the antivirus profile. **NOTE**: You must configure DNS servers before creating the antivirus profiles. To configure DNS servers, go to **Device Administration** > **Basic Settings** > **System Identity** > **DNS servers**.
Step 4	Create a UTM policy for Sophos antivirus and apply the antivirus profile to the UTM policy. Here, you use a UTM policy to bind a set of protocols (for example, HTTP) to the Sophos UTM feature profile. You can scan other protocols as well by creating different profiles or adding other protocols to the profile, such as imap-profile, pop3-profile, and smtp-profile.
Step 5	Create a security policy for Sophos antivirus and assign the UTM policy to the security policy. Here, you use the security firewall and antivirus profile settings to scan the traffic from the trust zone (trust) to the untrust zone (Internet).
Step 6	Access a URL from the allowlist URL (http://10.102.70.89) and try to download a test virus file (eicar.txt) which is made available on the 10.102.70.89 server.

Step 1: Update Default Configuration for Antivirus

You are here: **Security Services** > **UTM** > **Default Configuration**.

In this step, you'll set up **Sophos Engine** as the default engine type.

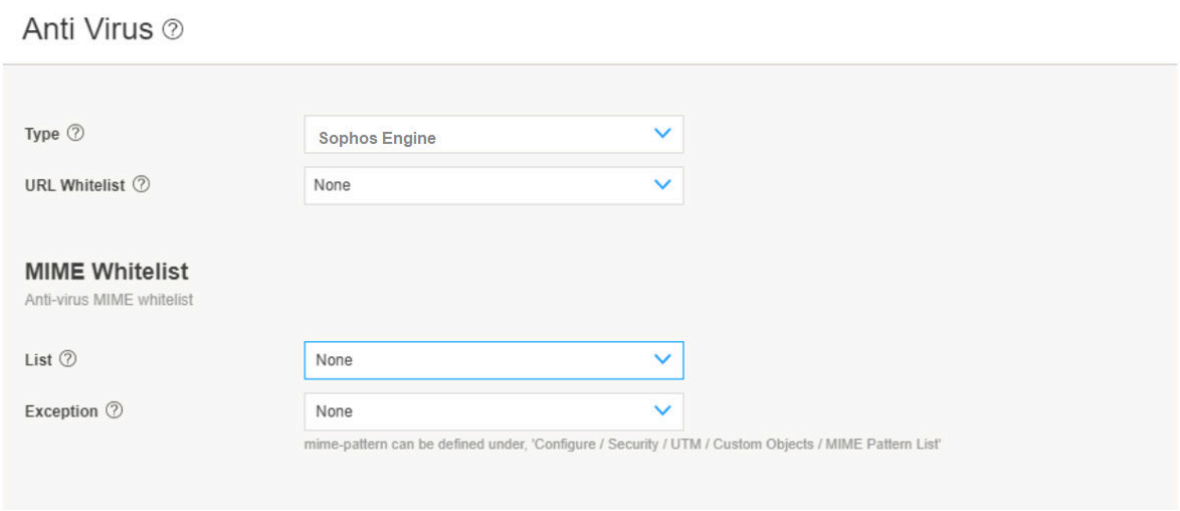
To update the default antivirus profile:

1. On the **Anti-Virus** tab, click the edit icon (pencil) to edit the default configuration.
   The Anti Virus page appears. See Figure 20 on page 823.
2. Complete the tasks listed in the Action column in Table 233 on page 823.

Table 233: Default Configuration Settings

Field	Action
Type	Select the **Sophos Engine** type for the antivirus.
URL Whitelist	Select **None**.
MIME Whitelist	
List	Select **None**.
Exception	Select **None**.

Figure 20: Default Antivirus Configuration



3. Click **OK** to save the new default configuration.

Step 2: Configure Antivirus Custom Object

IN THIS SECTION

Step 2a: Configure a URL Pattern List That You Want to Bypass

In this step, you define a URL pattern list (safelist) of URLs or addresses that will be bypassed by antivirus scanning.

You are here (in the J-Web UI): **Security Services** > **UTM** > **Custom Objects**.

To configure the safelist of URLs:

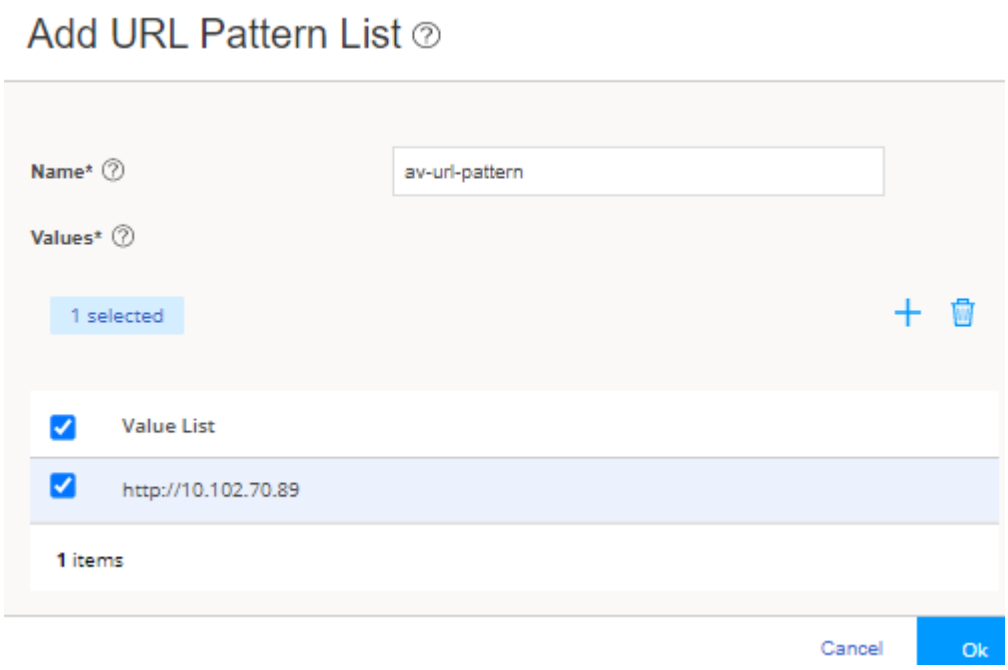
1. Click the **URL Pattern List** tab.
2. Click the add icon (**+**) to add a URL pattern list.

   The Add URL Pattern List page appears. See Figure 21 on page 825.
3. Complete the tasks listed in the Action column in Table 234 on page 824.

Table 234: URL Pattern List Settings

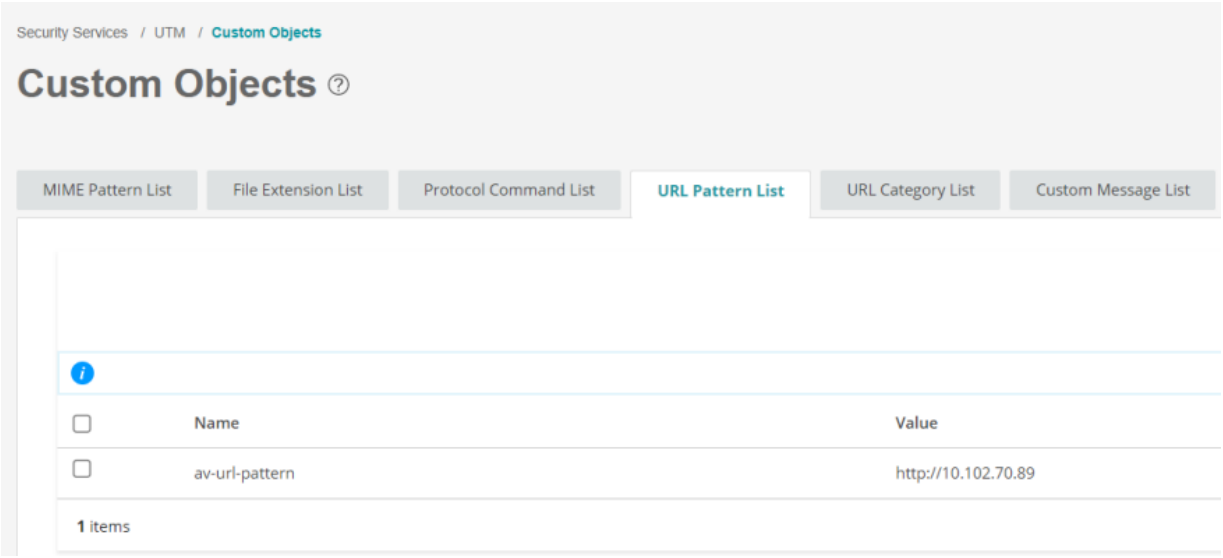
Field	Action
Name	Type **av-url-pattern**. **NOTE**: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. You can use a maximum of 29 characters.
Value	**a.** Click **+** to add a URL pattern value. **b.** Type **http://10.102.70.89**. **c.** Click the tick icon ✓ .

Figure 21: Add URL Pattern List



4. Click **OK** to save the URL pattern list configuration.

Good job! Here's the result of your configuration:



Step 2b: Categorize the URLs That You Want to Allow

You'll now assign the created URL pattern to a URL category list. The category list defines the action of mapping. For example, the *Safelist* category should be permitted.

You are here: **Security Services** > **UTM** > **Custom Objects**.

To categorize URLs:

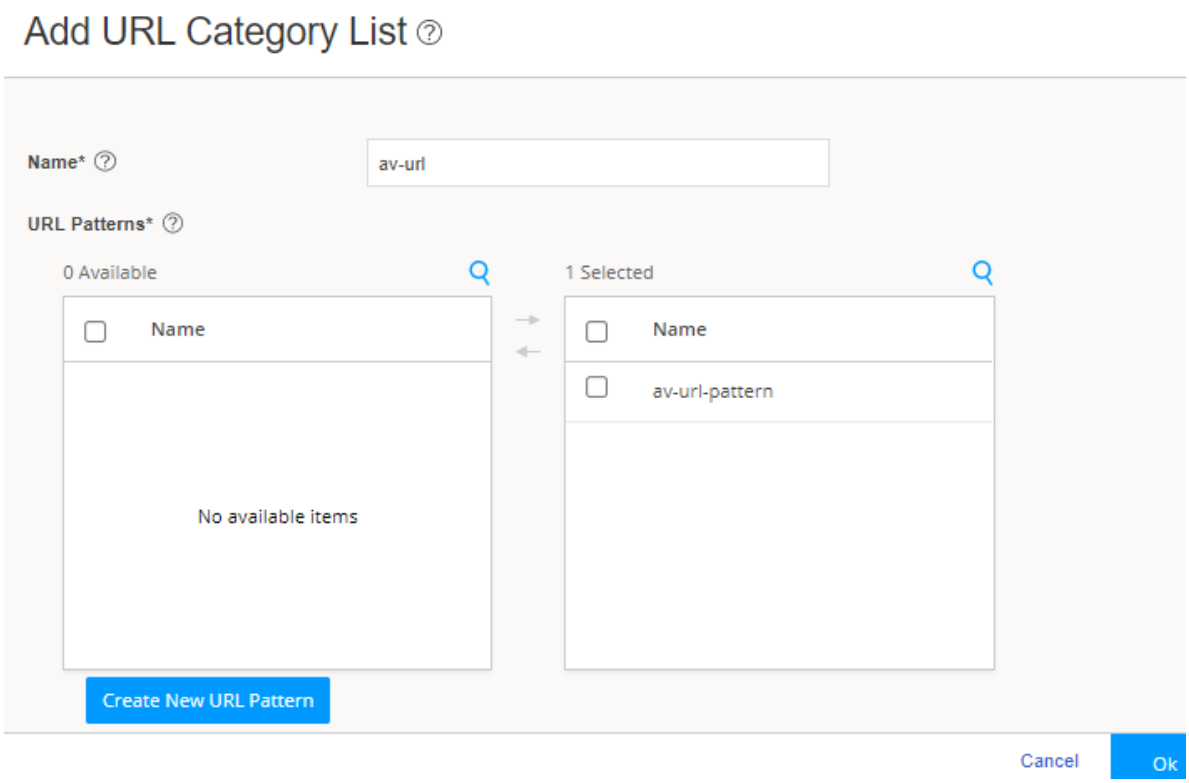
1. Click the **URL Category List** tab.
2. Click the add icon (**+**) to add a URL category list.

   The Add URL Category List page appears. See Figure 22 on page 827.
3. Complete the tasks listed in the Action column in Table 235 on page 826.

Table 235: URL Category List Settings

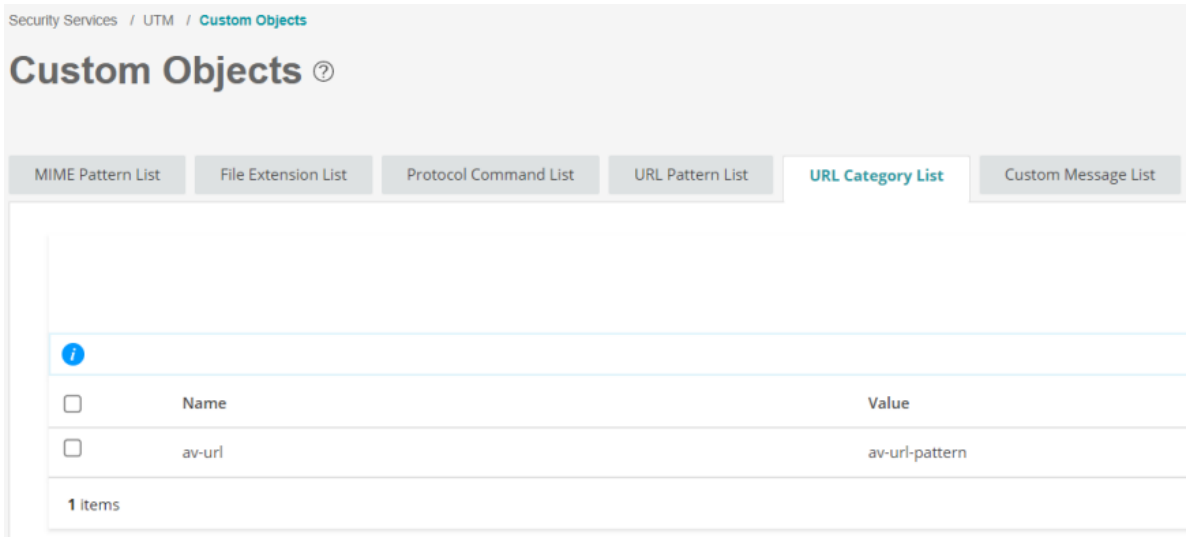
Field	Action
Name	Type **av-url** as the URL category list name for the safelisted URL pattern. **NOTE**: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. You can use a maximum of 59 characters.
URL Patterns	Select the URL pattern value **av-url-pattern** from the Available column and click the right arrow to move the URL pattern values to the Selected column. By doing this, you associate the URL pattern value **av-url-pattern** with the URL category list **av-url**.

Figure 22: Add URL Category List



4. Click **OK** to save the category list configuration.

   Good job! Here's the result of your configuration:



Step 3: Create an Antivirus Profile

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

In this step, you'll create a new UTM antivirus profile, refer the created URL objects (patterns and categories) to the profile, and specify the notification details.

To create the new antivirus profile:

1. Click the add icon (**+**) to add a new antivirus profile.

   The Create Antivirus Profiles page appears. See Figure 23 on page 829.
2. Complete the tasks listed in the Action column in Table 236 on page 828.

Table 236: Antivirus Profile Settings

Field	Action
General	
Name	Type **av-profile** for the new antivirus profile. **NOTE**: You can use a maximum of 29 characters.
URL Allowlist	Select **av-url** from the drop-down list.
Fallback Options	
Content Size	Select **Log and Permit**.
Default Action	Select **Log and Permit**.
Notification Options	
Virus Detection	Select **Notify Mail Sender**.
Notification Type	Select **Message**.
Custom Message Subject	Type ***Antivirus Alert***.
Custom Message	Type **Virus Found !**.

Figure 23: Create Antivirus Profile General Settings

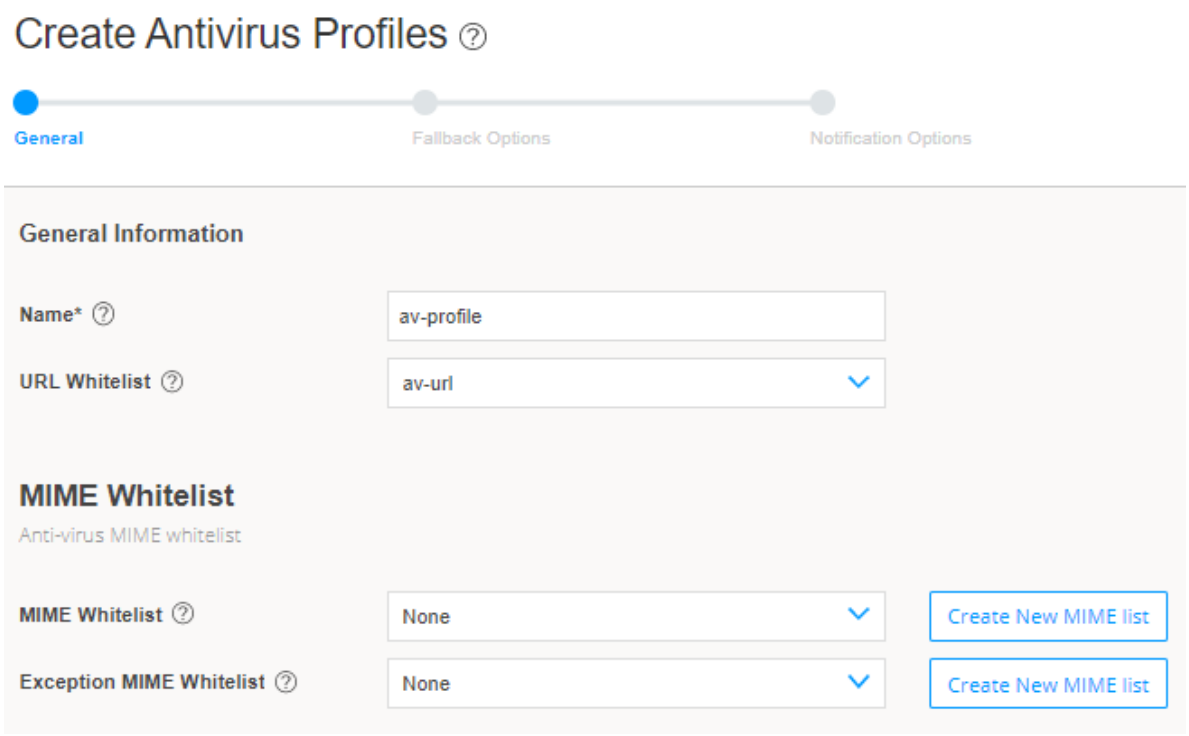
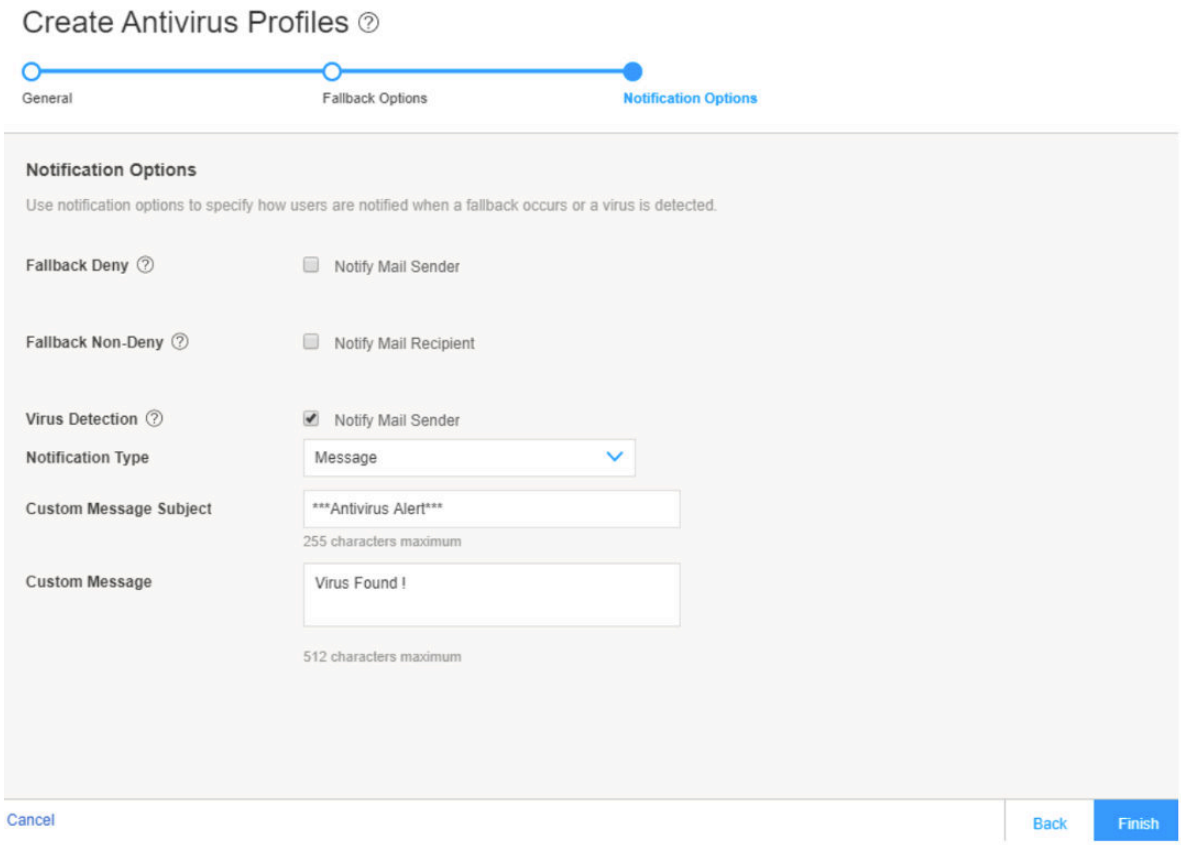


Figure 24: Create Antivirus Profile Notification Settings



3. Click **Finish**. Review the summary of the configuration and click **OK** to save your configuration.
4. Click **Close** after you see a successful-configuration message.

   Good job! Here's the result of your configuration:

Step 4: Apply the Antivirus Profile to a UTM Policy

After you've created the antivirus feature profile, you configure a UTM policy for an antivirus scanning protocol and attach this policy to the antivirus profile created in "Step 3: Create an Antivirus Profile" on page 828. In this example, you'll scan HTTP and FTP traffic for viruses.

You are here: **Security Services** > **UTM** > **UTM Policies**.

To create a UTM policy:

1. Click the add icon (**+**).

   The Create UTM Policies page appears.

2. Complete the tasks listed in the Action column in Table 237 on page 831.

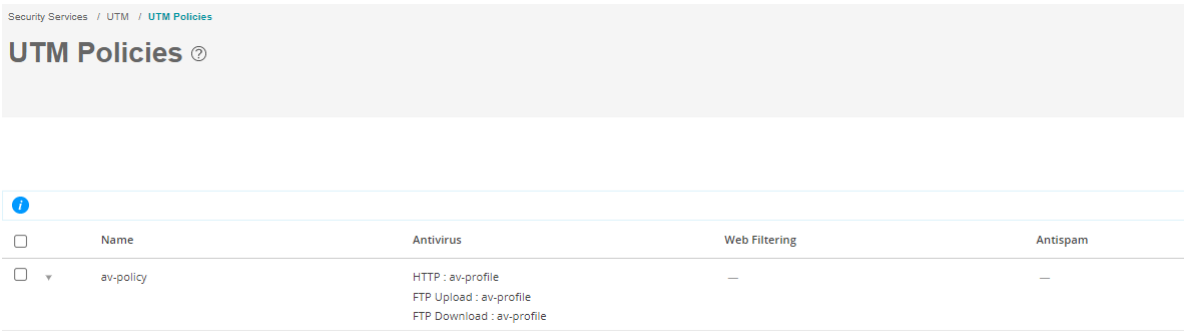
Table 237: Create UTM Policies Settings

Field	Action
General	
Name	Type **av-policy** as the name of the UTM policy and click **Next**. **NOTE**: You can use a maximum of 29 characters.
Antivirus	
HTTP	Select **av-profile** from the list.
FTP Upload	Select **av-profile** from the list.
FTP Download	Select **av-profile** from the list and click **Next** till end of the page.

3. Click **Finish**. Review the summary of the configuration and click **OK** to save the changes.
4. Click **Close** after you see a successful-configuration message.

Almost there! Here's the result of your configuration:

jn-000552



Step 5: Assign the UTM Policy to a Security Firewall Policy

In this step, you create a firewall security policy that will cause traffic passing from the trust zone (trust) to the untrust zone (internet) to be scanned by Sophos antivirus using the feature profile settings.

You haven't yet assigned the UTM configurations to the security policy from the trust zone to the internet zone. Filtering actions are taken only after you assign the UTM policy to security policy rules that act as the match criteria.

NOTE: When the security policy rules are permitted, the SRX Series device:

1. Intercepts an HTTP connection and extracts each URL (in the HTTP request) or IP address.

   NOTE: For an HTTPS connection, antivirus is supported through SSL forward proxy.

2. Searches for URLs in the user-configured safelist under Antivirus (**Security Services** > **UTM** > **Default Configuration**). Then, if the URL is in the user-configured safelist, the device permits the URL.
3. Allows or blocks the URL (if a category is not configured) based on the default action configured in the antivirus profile.

You are here: **Security Policies & Objects** > **Security Policies**.

To create security policy rules for the UTM policy:

1. Click the add icon (**+**).
2. Complete the tasks listed in the Action column in Table 238 on page 832.

Table 238: Rule Settings

Field	Action
General	
Rule Name	Type **av-security-policy** as the security policy rule name. This rule allows the URLs in the av-url category list.
Rule Description	Enter a description for the security policy rule and click **Next**.

Table 238: Rule Settings *(Continued)*

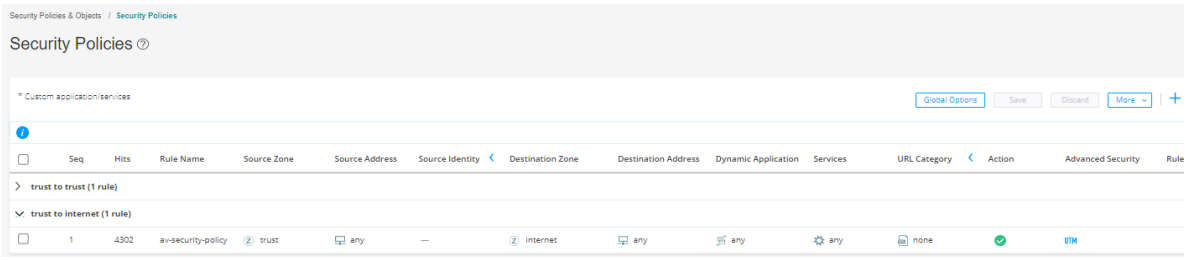
Field	Action
Source Zone	**a.** Click **+**. The Select Sources page appears. **b.** Zone—Select **trust** from the list. **c.** Addresses—Leave this field with the default value **any**. **d.** Click **OK**
Destination Zone	**a.** Click **+**. The Select Destination page appears. **b.** Zone—Select **internet** from the list. **c.** Addresses—Leave this field with the default value **any**. **d.** Services—Leave this field with the default value **any**. **e.** Click **OK**
Action	Select **Permit** from the list.
Advanced Security	**a.** Click **+**. The Select Advanced Security page appears. **b.** UTM—Select **av-policy** from the list. **c.** Click **OK**

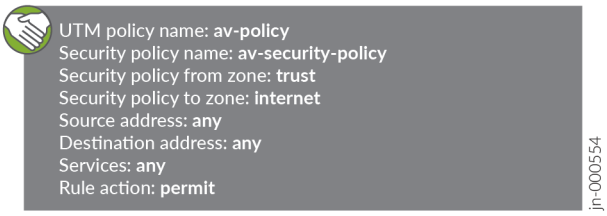
NOTE: Navigate to **Security Policies & Objects** > **Zones/Screens** to create zones. Creating zones is outside the scope of this documentation.

3. Click the tick icon

to save changes.

Good job! Here's the result of your configuration:





4. Click the commit icon (at the right side of the top banner) and select **Commit**.

   The successful-commit message appears.

   Congratulations! We're now ready to scan the traffic for virus attacks.

Step 6: Verify That UTM Antivirus Is Working

IN THIS SECTION

Purpose

Verify that your configured UTM antivirus is allowing traffic from the Allowlist server and preventing virus attacks from the server.

Action

1. Using the PC, send a HTTP request to http://10.102.70.89.

   Good job! You can access the http://10.102.70.89 server.

2. Using the PC, send a FTP request to the 10.102.70.89 server to download the eicar.txt file. The eicar.txt file is a test virus file which is made available on the 10.102.70.89 server.

   Sorry! The SRX Series device has blocked downloading the file and sent you a custom block message *****Antivirus Alert***- Virus Found!**.

   Here is an example output when you try to download the eicar.txt file and the SRX Series Firewall sends a virus alert:

```
[centos-01 ~]$ ftp 10.102.70.89
Connected to 10.102.70.89 (10.102.70.89).
220 XX FTP server (Version 6.00LS) ready.
Name (10.102.70.89:lab): root
331 Password required for root.
Password:
230 User root logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get eicar.txt
local: eicar.txt remote: eicar.txt
227 Entering Passive Mode (10,102,70,89,197,55)
150 Opening BINARY mode data connection for 'eicar.txt' (70 bytes).
netin: Connection reset by peer
426 10.102.70.89:21->10.0.1.1:36240 ***Antivirus Alert***- Virus Found!
```

   Here is an example of the anti-virus statistics output when you find a threat:

```
[edit]
root@srx> show security utm anti-virus statistics
 UTM Anti Virus statistics:

 Intelligent-prescreening passed:      0
 MIME-whitelist passed:                0
 URL-whitelist passed:                 1
 Session abort:                        0
 Scan Request:

  Total           Clean         Threat-found    Fallback
       2               0              1               0

 Fallback:
                              Log-and-Permit    Block             Permit
```

```
Engine not ready:                0                0                0
Out of resources:                0                0                0
Timeout:                         0                0                0
Maximum content size:            0                0                0
Too many requests:               0                0                0
Decompress error:                0                0                0
Others:                          0                0                0
```

What's Next?

If you want to	Then
Monitor UTM antivirus details and statistics	In J-Web, go to **Monitor** > **Security Services** > **UTM** > **Anti Virus**
Generate and view reports on URLs allowed and blocked	To generate and view reports: 1. Log in to J-Web UI and click **Monitor** > **Reports**. The Reports page appears. 2. Select any of the following predefined report name. • **Threat Assessment Report** • **Viruses Blocked** **NOTE**: You can't generate more than one report at the same time. 3. Click **Generate Report**. The Report Title page appears. 4. Enter the required information and click **Save**. A reported is generated.
Learn more about UTM features	See Unified Threat Management User Guide

Sample Configuration Output

In this section, we present samples of configurations that block virus attacks from the websites defined in this example.

You configure the following UTM configurations at the `[edit security utm]` hierarchy level.

Creating custom objects at the [edit security utm] hierarchy level:

```
custom-objects {
    url-pattern {
        av-url-pattern {
            value http://10.102.70.89 ;
        }
    }
    custom-url-category {
        av-url {
            value av-url-pattern;
        }
    }
}
```

Creating the antivirus profile at the [edit security utm] hierarchy level:

```
    default-configuration {
        anti-virus {
            type sophos-engine;
        }
    }
```

```
    feature-profile {
        anti-virus {
            profile av-profile {
                notification-options {
                    virus-detection {
                    type message;
                    notify-mail-sender;
                    custom-message “Virus-Found!”;
                    custom-message-subject “***Antivirus Alert***”;
                    }
                }
            }
        }
    }
```

Creating the UTM policy:

```
utm-policy av-policy {
            anti-virus {
                http-profile av-profile;
                ftp {
                    upload-profile av-profile;
                    download-profile av-profile;
                }
            }
        }
```

Creating rules for a security policy at the `[edit security policies]` hierarchy level:

```
from-zone trust to-zone internet {
    policy av-security-policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy av-policy;
                }
            }
        }
    }
}
```

CHAPTER 73

UTM Web Filtering Profiles

IN THIS CHAPTER

About the Web Filtering Profiles Page

IN THIS SECTION

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

Use this page to manage Internet usage by preventing access to inappropriate Web content.

A Web filtering profile defines a set of permissions and actions to take based on Web connections predefined by website categories. In addition, you can create custom URL categories and URL pattern lists during this process.

For an example use case, see Allow or Block Websites by Using J-Web Integrated UTM Web Filtering.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Web filtering profile. See "Add a Web Filtering Profile" on page 841.
- Edit a Web filtering profile. See "Edit a Web Filtering Profile" on page 848.
- Clone a Web filtering profile. See "Clone a Web Filtering Profile" on page 847.
- Delete a Web filtering profile. See "Delete Web Filtering Profile" on page 849.
- Filter the Web filtering profiles based on select criteria. To do this, select the filter icon at the top right-hand corner of the Web filtering profiles table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the Web filtering profiles table. To do this, click the Show Hide Columns icon in the top right corner of the Web filtering profiles table and select the columns you want to view or deselect the columns you want to hide on the page.
- View the details of a Web filtering profile—To do this, select the Web filtering profile for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected Web filtering profile and select **Detailed View**.
  - Mouse over to the left of the selected Web filtering profile and click **Detailed View**.
- Advanced search for Web filtering profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 239 on page 841 describes the fields on the Web filtering page.

Table 239: Fields on the Web Filtering Page

Field	Action
Name	Displays the name for the Web filtering profile.
Profile type	Displays the type of profile based on the filtering type selected.
Default action	Displays the default action to be taken for the web filtering profile.
Timeout	Displays the time interval to wait before the connection to the server is closed.

RELATED DOCUMENTATION

- Add a Web Filtering Profile | 841
- Edit a Web Filtering Profile | 848
- Delete Web Filtering Profile | 849

Add a Web Filtering Profile

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

To create a new web filtering profile:

1. Click the add icon **(+)** available on the upper right side of the Web Filtering Profiles page.

   The Create Web Filtering Profiles page appears.
2. Complete the configuration according to the guidelines provided in Table 240 on page 842 through Table 242 on page 846.
3. Click **Finish** to save the changes or click **Back** to go to the previous tab. If you want to discard your changes, click **Cancel**.

   If you click **Finish**, a new web filtering profile is created.

Table 240: Fields on the General tab

Field	Action
Name	Enter a name for the Web filtering profile. The maximum length is 29 characters.
Timeout	Enter a timeout value to wait for a response from the Websense server. The maximum value is 1800 seconds. Default value is 15 seconds.
Engine type	Select an engine type for Web filtering: The available options are • Juniper Enhanced—Specifies that the Juniper Enhanced Web filtering intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). • Websense Redirect—Specifies that the Web filtering module intercepts an HTTP request. The URL in the request is then sent to the external Websense server which makes a permit or a deny decision. • Local—Specifies that the Web filtering module intercepts URLs and makes a permit or deny decision locally. **NOTE**: The default value is Juniper Enhanced.
Safe search	Enable a safe search solution to ensure that the embedded objects such as images on the URLs received from the search engines are safe and that no undesirable content is returned to the client. **NOTE**: This option is available only for the Juniper Enhanced engine type. By default, this option is enabled.
Account	Enter the user account associated with the Websense Web filtering profile. **NOTE**: This option is available only for the Websense Redirect engine type.
Server	Enter the hostname or IP address for the Websense server. **NOTE**: This option is available only for the Websense Redirect engine type.

Table 240: Fields on the General tab *(Continued)*

Field	Action
Port	Enter the port number for communicating with the Websense server. The default port is 15868. **NOTE**: This option is available only for the Websense Redirect engine type.
Sockets	Enter the number of sockets used for communication between the client and the server. The default value is 8. **NOTE**: This option is available only for the Websense Redirect engine type.
Custom Block Message/URL	Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. Maximum length is 512 characters.
Custom Quarantine Message	Define a custom message to allow or deny access to a blocked site based on a user response to the message. Maximum length is 512 characters. **NOTE**: This option is available only for the Juniper Enhanced and the Local engine types.
Base Filter	Select a predefined base filter, which has default actions for all categories, for Web filtering. Click **Clear All** to discard the changes. **NOTE**: This option is available only for the Juniper Enhanced engine type.

Table 241: Fields on the URL Categories Tab

Field	Action
Apply actions	To apply actions that the device must take for the selected category: 1. Click **Apply Actions**. The Apply Actions page appears. 2. Enter the following details: • Action—Select an action for the URL category from the list. The options are Permit, Log and Permit, Block or Quarantine. • Custom Message—Select a custom message for the URL category. **NOTE**: • This option is applicable only when the action is Block or Quarantine. • Click **Clear all** to clear the custom message. To add a custom message list inline: a. Click **Create New**. b. Enter the following details: • Name—Enter a unique name for the custom message list. Special characters such as hyphen, underscore, !, @, $, *, + are allowed. The maximum length is 29 characters. • Type—Select an option from the list. The options are Redirect URL or User Message. • Content—Enter a content for the custom message list. The maximum length is 512 characters. c. Click **OK** to add a new custom message list. Else, click **Cancel**. 3. Click **OK** to apply actions for the category. Else, click **Cancel**.

Table 241: Fields on the URL Categories Tab *(Continued)*

Field	Action
Create	To add a new URL category: 1. Click **+**. The Select URL Categories page appears. 2. Select one or more predefined and custom URL categories to apply to the list. The Name column displays the list of URL categories to choose from. Click the search icon in the top right corner of the table to search for any particular URL category in the list. 3. Enter the following details: • Action—Select an action for the URL category from the list. The options available are Permit, Log and Permit, Block, and Quarantine. **NOTE**: The default action is Log and Permit. • Custom Message—Select a custom message for the URL category. **NOTE**: • This option is applicable only when the action is Block or Quarantine. • Click **Clear all** to clear the custom message. • Click **Create New** to add a custom message list inline. 4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
Delete	Select a URL category that you want to delete and click the delete icon in the top right corner of the table
Search	Click the search icon in the top right corner of the table and the URL category you want to search.
Category name	Displays the URL category names. Select one or more categories from the list.

Table 241: Fields on the URL Categories Tab *(Continued)*

Field	Action
Action	Displays the action taken for the URL category.
Custom message	Displays the respective custom messages for the URL categories.

Table 242: Fields on the Fallback Options Tab

Field	Action
Global Reputation Actions	Select to choose the action you want to take for each reputation level. URLs can be processed using their reputation score if there is no category available.
Very Safe	Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you. **NOTE**: If you have not defined the percentage, the default score is 90 through 100. The options are Permit, Log and Permit, Block, and Quarantine.
Moderately Safe	Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you. **NOTE**: If you have not defined the percentage, the default score is 80 through 89. The options are Permit, Log and Permit, Block, and Quarantine.
Fairly Safe	Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you. **NOTE**: If you have not defined the percentage, the default score is 70 through 79. The options are Permit, Log and Permit, Block, and Quarantine.

Table 242: Fields on the Fallback Options Tab *(Continued)*

Field	Action
Suspicious	Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you. **NOTE**: If you have not defined the percentage, the default score is 60 through 69. The options are Permit, Log and Permit, Block, and Quarantine.
Harmful	Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you. **NOTE**: If you have not defined the percentage, the default score is 50 through 59. The options are Permit, Log and Permit, Block, and Quarantine.
Default Action	Select an option from the list for the actions to be taken for URL categories with no assigned action and for uncategorized URLs. The options are Permit, Log and Permit, Block, and Quarantine.
Fallback Action	Select an option from the list. The options are Log and Permit and Block. Use this option when the ThreatSeeker Websense Cloud servers are unreachable. A timeout occurs for requests to ThreatSeeker Cloud.

RELATED DOCUMENTATION

- About the Web Filtering Profiles Page | 839
- Clone a Web Filtering Profile | 847
- Edit a Web Filtering Profile | 848
- Delete Web Filtering Profile | 849

Clone a Web Filtering Profile

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

To clone a Web filtering profile:

1. Select a Web filtering profile that you want to clone and select **Clone** from the More link.

   NOTE: Alternatively, you can right-click on the selected Web filtering profile and select **Clone**.

   The Clone Web Filtering Profiles page appears with editable fields. For more information on the options, see "Add a Web Filtering Profile" on page 841.

2. Click **OK** to save the changes.

   A cloned Web filtering profile is created for the selected Web filtering profile. By default, the name of the cloned Web filtering profile is in the format: ***<Web filtering profile name>***_**clone**.

RELATED DOCUMENTATION

About the Web Filtering Profiles Page | 839
Add a Web Filtering Profile | 841
Edit a Web Filtering Profile | 848
Delete Web Filtering Profile | 849

Edit a Web Filtering Profile

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

To edit a Web filtering profile:

1. Select a Web filtering profile that you want to edit on the Web Filtering page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Web Filtering Profiles page appears with editable fields. For more information on the options, see "Add a Web Filtering Profile" on page 841.

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

About the Web Filtering Profiles Page | 839
Add a Web Filtering Profile | 841
Clone a Web Filtering Profile | 847
Delete Web Filtering Profile | 849

Delete Web Filtering Profile

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

To delete Web filtering profiles:

1. Select one or more Web filtering profiles that you want to delete from the Web Filtering page.
2. Click the delete icon available on the upper right side of the page.

   A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Web Filtering Profiles Page | **839**
- Add a Web Filtering Profile | **841**
- Clone a Web Filtering Profile | **847**
- Edit a Web Filtering Profile | **848**

Allow or Block Websites by Using J-Web Integrated UTM Web Filtering

SUMMARY

Learn about Web filtering and how to filter URLs on UTM-enabled SRX Series devices by using J-Web. Web filtering helps you to allow or block access to the Web and to monitor your network traffic.

IN THIS SECTION

UTM URL Filtering Overview

Today, most of us spend an amount of time on the Web. We surf our favorite sites, follow interesting links sent to us through E-mail, and use a variety of Web-based applications for our office network. This increased use of the network helps us both personally and professionally. However, it also exposes the organization to a variety of security and business risks, such as potential data loss, lack of compliance, and threats such as malware, viruses, and so on. In this environment of increased risk, it's wise for businesses to implement Web or URL filters to control network threats. You can use a Web or URL filter to categorize websites on the Internet and to either allow or block user access.

Here's an example of a typical situation where a user of office network has access to a website blocked:

On the Web browser, the user types **www.game.co.uk**, a popular gaming site. The user receives a message such as `Access Denied` or `The Website is blocked`. Display of such a message means that your organization has inserted a filter for the gaming websites, and you can't access the site from your workplace.

Juniper Web (J-Web) Device Manager supports UTM Web filtering on SRX Series devices.

In J-Web, a Web filtering profile defines a set of permissions and actions based on Web connections predefined by website categories. You can also create custom URL categories and URL pattern lists for a Web filtering profile.

NOTE: You cannot inspect URLs within e-mails using J-Web UTM Web filtering.

Benefits of UTM Web Filtering

- Local Web filtering:
  - Doesn't require a license.
  - Enables you to define your own lists of allowed sites (allowlist) or blocked sites (blocklist) for which you want to enforce a policy.

- Enhanced Web filtering:
  - Is the most powerful integrated filtering method and includes a granular list of URL categories, support for Google Safe Search, and a reputation engine.
  - Doesn’t require additional server components.
  - Provides real-time threat score for each URL.
  - Enables you to redirect users from a blocked URL to a user-defined URL rather than simply preventing user access to the blocked URL.
- Redirect Web filtering:
  - Tracks all queries locally, so you don't need an Internet connection.
  - Uses the logging and reporting features of a standalone Websense solution.

Web Filtering Workflow

IN THIS SECTION

Scope

In this example, you’ll:

1. Create your own custom URL pattern lists and URL categories.
2. Create a Web filtering profile using the Local engine type. Here, you define your own URL categories, which can be allowed sites (allowlist) or blocked sites (blocklist) that are evaluated on the SRX Series device. All URLs added for blocked sites are denied, while all URLs added for allowed sites are permitted.
3. Block inappropriate gaming websites and allow suitable websites (for example, www.juniper.net).
4. Define a custom message to display when users attempt to access gaming websites.
5. Apply the Web filtering profile to a UTM policy.

6. Assign the UTM policy to a security policy rule.

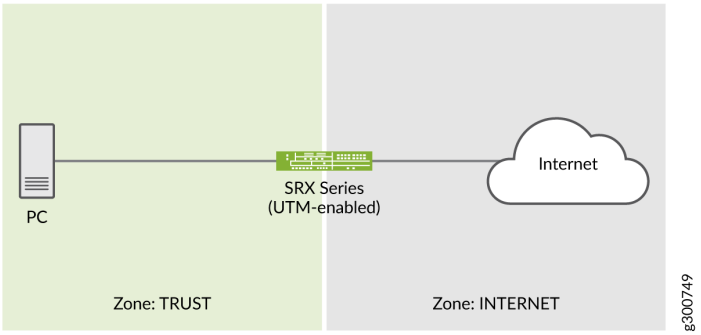
> **NOTE**: Web filtering and URL filtering have the same meaning. We'll use the term *Web filtering* throughout our example.

Before You Begin

- We assume that your device is set with the basic configuration. If not, see Configure Setup Wizard.
- You do not need a license to configure the Web filtering profile if you use the Local engine type. This is because you will be responsible for defining your own URL pattern lists and URL categories.
- You need a valid license (**wf_key_websense_ewf**) if you want to try the Juniper Enhanced engine type for the Web filtering profile. Redirect Web filtering does not need a license.
- Ensure that the SRX Series device you use in this example runs Junos OS Release 20.4R1 and later.

Topology

In this topology, we have a PC connected to a UTM-enabled SRX Series device that has access to the Internet. Let's use J-Web to filter the HTTP/HTTPS requests sent to the Internet using this simple setup.



Sneak Peek – J-Web UTM Web Filtering Steps

Step 1: List URLs That You Want to Allow or Block

In this step, we define custom objects (URLs and patterns) to handle the URLs that you want to allow or block.

You are here (in the J-Web UI): **Security Services** > **UTM** > **Custom Objects**.

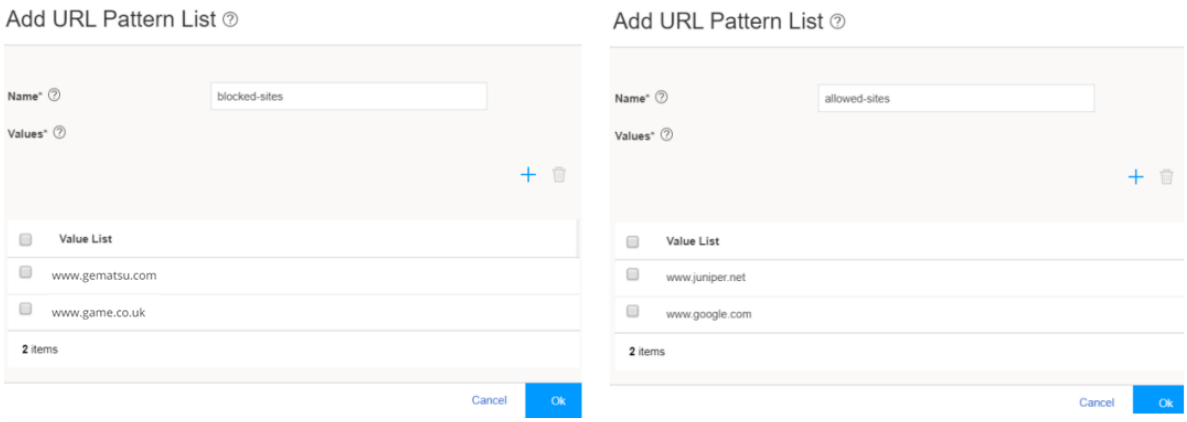
To list URLs:

1. Click the URL Pattern List tab.
2. Click the add icon (**+**) to add a URL pattern list.

   The Add URL Pattern List page appears. See Figure 25 on page 854.
3. Complete the tasks listed in the Action column in the following table:

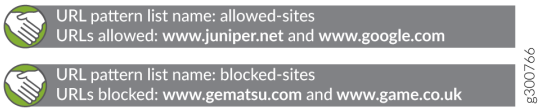
Field	Action
Name	Type **allowed-sites** or **blocked-sites**. **NOTE**: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 29 characters.
Value	**a.** Click **+** to add a URL pattern value. **b.** Type the following: • For allowed-sites—**www.juniper.net** and **www.google.com** • For blocked-sites—**www.gematsu.com** and **www.game.co.uk** **c.** Click the tick icon ✓ .

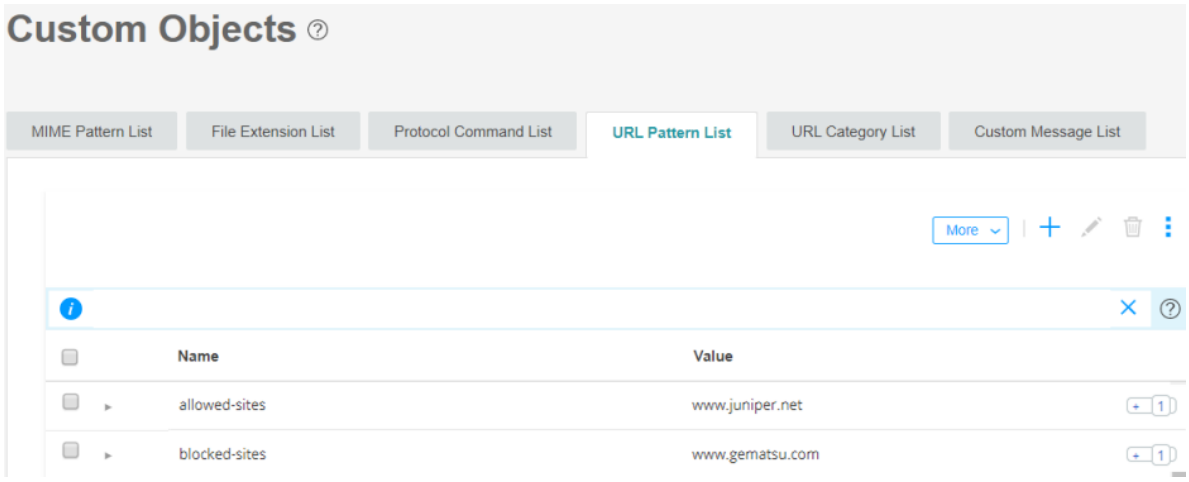
Figure 25: Add URL Pattern List



4. Click **OK** to save the changes.

   Good job! Here's the result of your configuration:





Step 2: Categorize the URLs That You Want to Allow or Block

We'll now assign the created URL patterns to URL category lists. The category list defines the action associated with the associated URLs. For example, the *Gambling* category should be blocked.

You are here: **Security Services** > **UTM** > **Custom Objects**.

To categorize URLs:

1. Click the URL Category List tab.

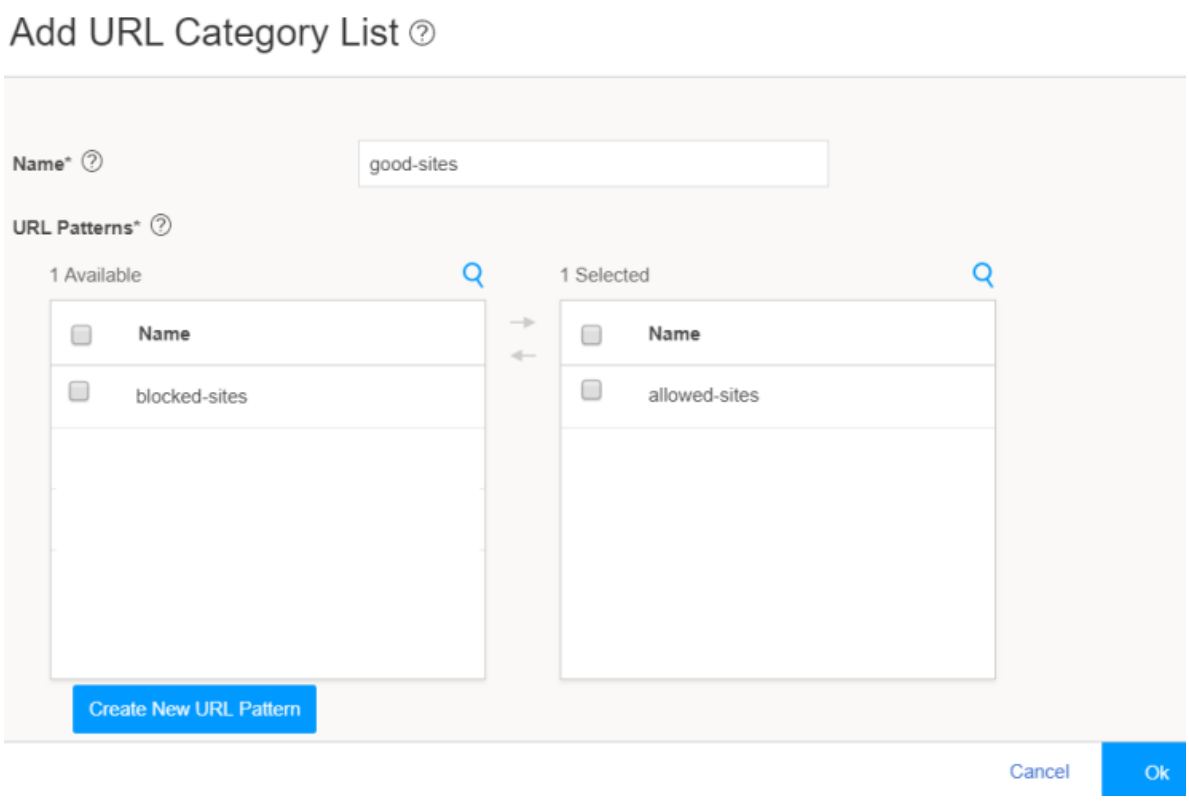
2. Click the add icon (**+**) to add a URL category list.

   The Add URL Category List page appears. See Figure 26 on page 856.

3. Complete the tasks listed in the Action column in the following table:

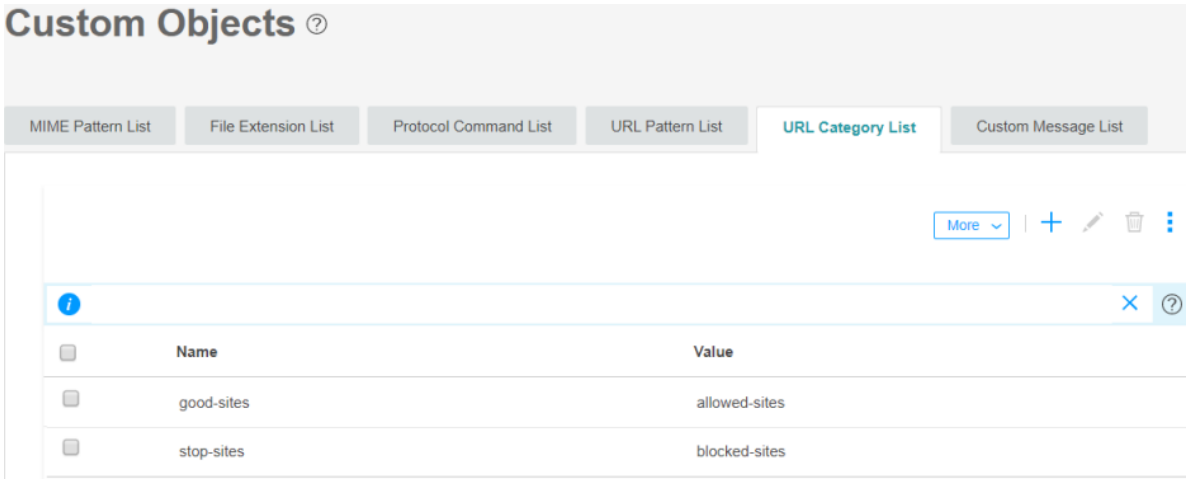
Field	Action
Name	Type the URL category list name as **good-sites** for the allowed-sites URL pattern or **stop-sites** for the blocked-sites URL pattern. **NOTE**: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 59 characters.
URL Patterns	**a.** Select the URL pattern values **allowed-sites** or **blocked-sites** from the Available column to associate the URL pattern values with the URL categories good-sites or stop-sites, respectively. **b.** Click the right arrow to move the URL pattern values to the Selected column.

Figure 26: Add URL Category List



4. Click **OK** to save the changes.

   Good job! Here's the result of your configuration:



Step 3: Add a Web Filtering Profile

Now, let's link the created URL objects (patterns and categories) to a UTM Web filtering profile. This mapping allows you to set different values for your filtering behavior.

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

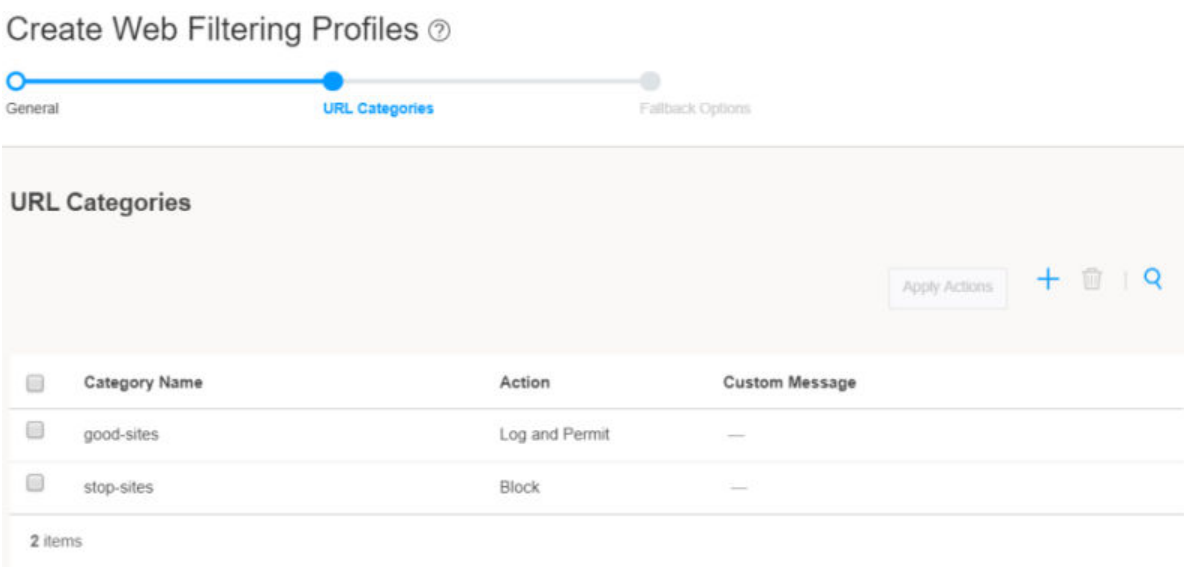
To create a Web filtering profile:

1. Click the add icon (**+**) to add a Web filtering profile.

   The Create Web Filtering Profiles page appears. See Figure 27 on page 858.
2. Complete the tasks listed in the Action column in the following table:

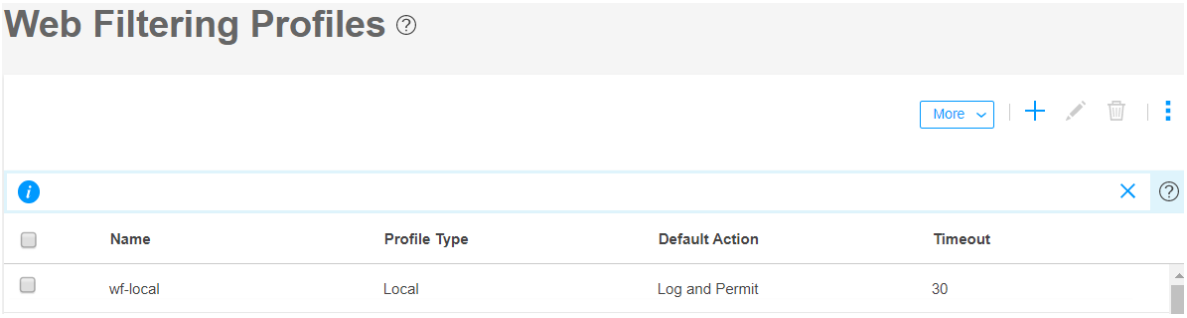
Field	Action
General	
Name	Type **wf-local** for the Web filtering profile. **NOTE**: The maximum length is 29 characters.
Timeout	Type **30** (in seconds) to wait for a response from the Local engine. The maximum value is 1800 seconds. The default value is 15 seconds.
Engine type	Select the **Local** engine type for Web filtering. Click **Next**. **NOTE**: The default value is Juniper Enhanced.
URL Categories	
+	Click the add icon to open the Select URL Categories window.
Select URL categories to apply to the list	Select **good-sites** or **stop-sites**.
Action	Select **Log and Permit** for the good-sites category from the list. Select **Block** for the stop-sites category from the list. Click **Next** and then click **Next** to skip the Fallback Options configuration.

Figure 27: Create Web Filtering Profile



3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.

   Good job! Here's the result of your configuration:



4. Click **Close** after you see a successful-configuration message.

Step 4: Reference a Web Filtering Profile in a UTM Policy

We now need to assign the Web filtering profile (wf-local) to a UTM policy that can be applied to a security policy.

You are here: **Security Services** > **UTM** > **UTM Policies**.

To create a UTM policy:

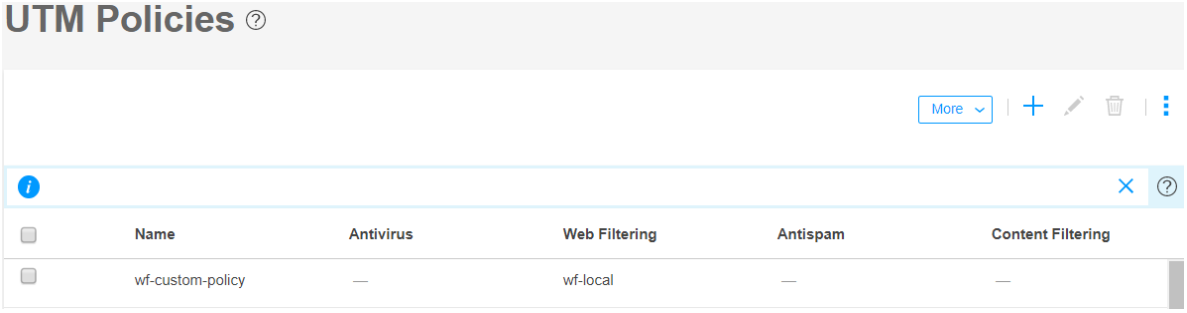
1. Click the add icon (**+**) to add a UTM policy.

   The Create UTM Policies page appears.
2. Complete the tasks listed in the Action column in the following table:

Field	Action
General – General Information	
Name	Type **wf-custom-policy** for the UTM policy. **NOTE**: The maximum length is 29 characters. Click **Next** and then click **Next** to skip the Antivirus configuration.
Web Filtering - Web Filtering Profiles by Traffic Protocol	
HTTP	Select **wf-local** from the list and click **Next** till the end of the workflow.

3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.

   Almost there! Here's the result of your configuration:



4. Click **Close** after you see a successful message.

   Almost done! Now, you create a default UTM web filtering policy that references your list of good and stop sites.

   You are here: **Security Services** > **UTM** > **Default Configuration Web Filtering**.

5. Click the edit (pencil) icon to modify the default web filtering policy.

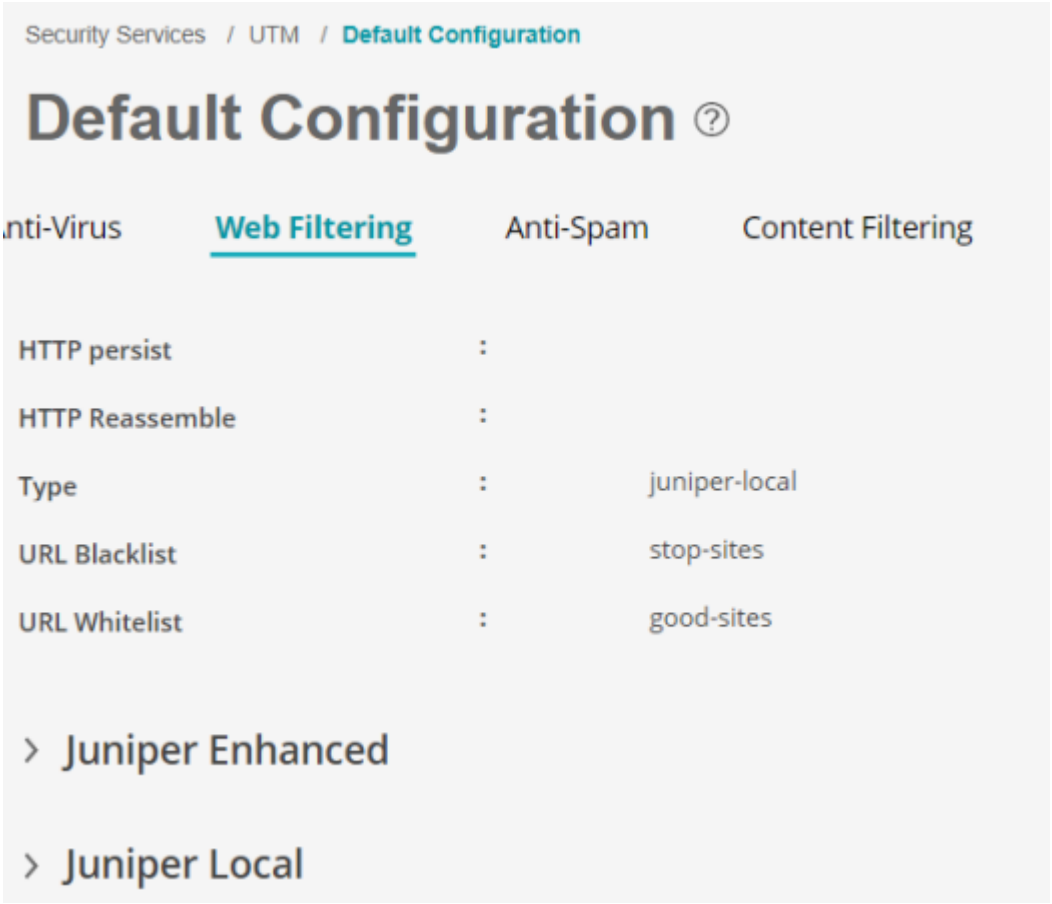
   The Web Filtering page appears.

6. Complete the tasks listed in the Action column in the following table:

Field	Action
Type	Use the menu pull-down to select **Juniper Local** to configure the use of the local UTM filtering database.
URL Blocklist	Use the menu pull-down to select **stop-sites** to link to the list of URLs that are not allowed (blocked).
URL Allowlist	Use the menu pull-down to select **good-sites** to link to the list of URLs that are allowed.
Juniper Local > Global	
Custom Block Message	Enter **Juniper Web Filtering has been set to block this site**.
Default Action	Select **Block** from the list. Skip other fields and click **OK**.

7. Click **OK** to save changes.

   Almost there! Here's the result of your UTM default web filtering configuration:



Good news! You're done with UTM Web filtering configuration.

Step 5: Assign a UTM Policy to a Security Policy

You haven't yet assigned the UTM configuration to the security policy from the TRUST zone to the INTERNET zone. Filtering actions are taken only after you assign the UTM policy to security policy rules that act as the match criteria.

NOTE: When the security policy rules are permitted, the SRX Series device:

1. Intercepts an HTTP/HTTPS connection and extracts each URL (in the HTTP/HTTPS request) or IP address.

   NOTE: For an HTTPS connection, Web filtering is supported through SSL forward proxy.

2. Searches for URLs in the user-configured blocklist or allowlist under Web Filtering (Security Services > UTM > Default Configuration). Then, if the URL is in the:
   a. User-configured blocklist, the device blocks the URL.
   b. User-configured allowlist, the device permits the URL.
3. Checks the user-defined categories and blocks or allows the URL based on the user-specified action for the category.
4. Allows or blocks the URL (if a category is not configured) based on the default action configured in the Web filtering profile.

You are here: **Security Policies & Objects** > **Security Policies**.

To create security policy rules for the UTM policy:

1. Click the add icon (**+**).
2. Complete the tasks listed in the Action column in Table 243 on page 862.

Table 243: Rule Settings

Field	Action
General – General Information	
Rule Name	Type **wf-local-policy** for the security policy allowing the good-sites category and denying the stop-sites category.
Rule Description	Enter a description for the security policy rule.
Source Zone	a. Click **+**. The Select Sources page appears. b. Zone—Select **TRUST** from the list. c. Addresses—Leave this field with the default value **Any**. d. Click **OK**

Table 243: Rule Settings *(Continued)*

Field	Action
Destination Zone	**a.** Click **+**. The Select Destination page appears. **b.** Zone—Select **INTERNET** from the list. **c.** Addresses—Leave this field with the default value **Any**. **d.** Services—Leave this field with the default value **Any**. **e.** URL Category—Leave this field blank. **f.** Click **OK**
Action	By default, **Permit** is selected. Leave as is.
Advanced Security	**a.** Click **+**. The Select Advanced Security page appears. **b.** UTM—Select **wf-custom-policy** from the list. **c.** Click **OK**

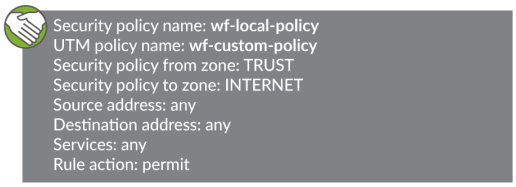
NOTE: Navigate to **Security Policies & Objects** > **Zones/Screens** to create zones. Creating zones is outside the scope of this documentation.

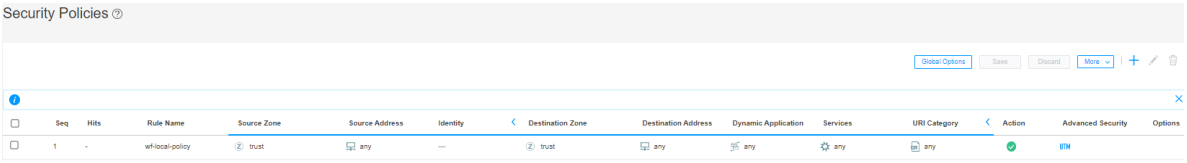
3. Click the tick icon

and then click **Save** to save changes.

NOTE: Scroll back the horizontal bar if the inline tick and cancel icons are not available when creating a new rule.

Good job! Here's the result of your configuration:





4. Click the commit icon (at the right side of the top banner) and select **Commit**.

   The successful-commit message appears.

   Congratulations! We're ready to filter the URL requests.

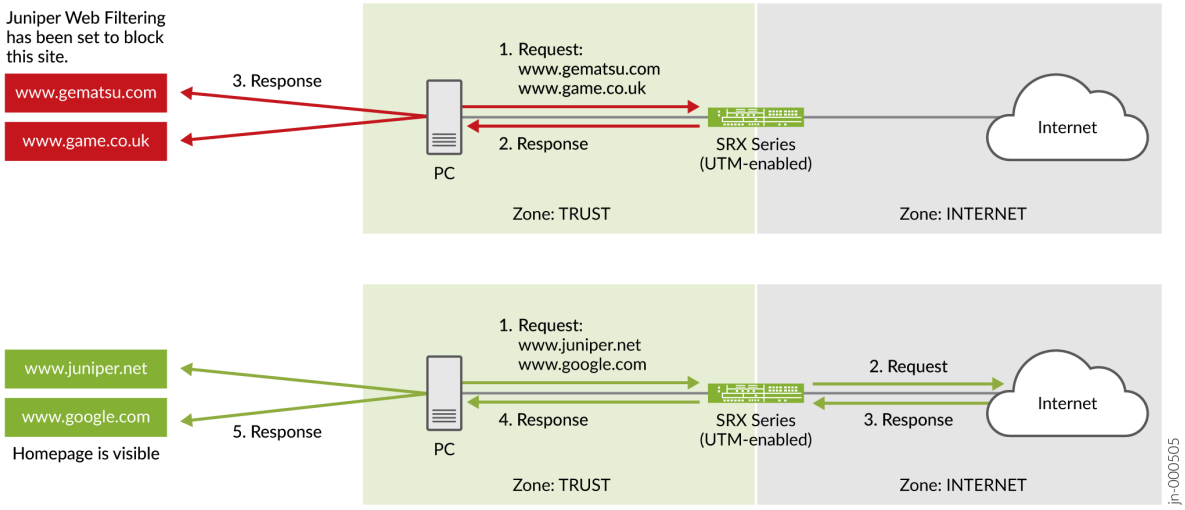
Step 6: Verify That the URLs Are Allowed or Blocked from the Server

Let's verify that our configurations and security policy work fine with the defined URLs in the topology:

- If you enter www.gematsu.com and www.game.co.uk, the SRX Series device should block the URLs and display the configured blocked site message.

  NOTE: Most sites use HTTPS. The blocked site messge is only seen for HTTP sites. For HTTPS you can expect a Secure Connection Failed error message such as "`An error occurred during a connection to <blocked-site-url> PR_CONNECT_RESET_ERROR`".

- If you enter www.juniper.net and www.google.com, the SRX Series device should allow the URLs with their homepage displayed.



What's Next

What to do?	Where?
Monitor UTM Web filtering information and statistics.	In J-Web, go to **Monitor** > **Security Services** > **UTM Web Filtering**.
Generate and view reports on URLs allowed and blocked.	In J-Web, go to **Reports**. Generate reports for Threat Assessment Reports and Top Blocked Applications via Webfilter logs.
Learn more about UTM features.	Unified Threat Management User Guide

Sample Configuration Output

In this section, we present samples of configurations that allow and block the websites defined in this example.

You configure the following UTM configurations at the `[edit security utm]` hierarchy level.

Creating custom objects:

```
custom-objects {
    url-pattern {
        blocked-sites {
            value [ http://*.gematsu..com http://*.game.co.uk];
```

```
        }
        allowed-sites {
            value [ http://*.juniper.net http://*.google.com];
        }
    }
    custom-url-category {
        good-sites {
                    value allowed-sites;
                }
                stop-sites {
                    value blocked-sites;
                }
    }
 }
```

Creating the Web filtering profile:

```
default-configuration {
        web-filtering {
                url-whitelist good-sites;
                url-blacklist stop-sites;
                type juniper-local;
                juniper-local {
                    default block;
                    custom-block-message "Juniper Web Filtering has been set to block this
site.";
                    fallback-settings {
                        default log-and-permit;
                        server-connectivity log-and-permit;
                        timeout log-and-permit;
                        too-many-requests log-and-permit;
                    }
                }
           }
        }
```

```
    feature-profile {
        web-filtering {
            juniper-local {
                profile wf-local {
                    category {
```

```
                    stop-sites {
                        action  block;
                    }
                    good-sites {
                        action log-and-permit;
                    }
                    }
                    timeout 30;
                }
            }
        }
    }
```

Creating the UTM policy:

```
utm-policy wf-custom-policy {
    web-filtering {
        http-profile wf-local;
    }
}
```

You configure the security policy rules at the `[edit security policies]` hierarchy level.

Creating rules for a security policy:

```
from-zone trust to-zone internet {
    policy wf-local-policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy wf-custom-policy;
                }
            }
        }
    }
}
```

CHAPTER 74

UTM Antispam Profiles

IN THIS CHAPTER

About the Antispam Profiles Page

IN THIS SECTION

You are here: **Security Services** > **UTM** > **Antispam Profiles**.

Use the Antispam Profiles page to view and manage antispam profiles. An antispam profile is used to examine transmitted e-mail messages to identify e-mail spam by using a constantly updated spam block list.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an antispam profile. See "Add an Antispam Profile" on page 870.
- Edit an antispam profile. See "Edit an Antispam Profile" on page 872.

- Delete an antispam profile. See "Delete Antispam Profile" on page 873.
- Clone an antispam profile. See "Clone an Antispam Profile" on page 871
- View the details of an antispam profile—To do this, select the antispam profile for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected antispam profile and select **Detailed View**.
  - Mouse over to the left of the selected antispam profile and click **Detailed View**.
- Advanced search for antispam profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.
- Filter the antispam profiles based on select criteria. To do this, select the filter icon at the top right-hand corner of the antispam profiles table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the antispam profiles table. To do this, click the Show Hide Columns icon in the top right corner of the antispam profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 244 on page 870 describes the fields on the Antispam Profiles page.

Table 244: Fields on the Antispam Profiles Page

Field	Description
Name	Name of the antispam profile.
Sophos Blocklist	Indicates whether Sophos Blocklist is enabled (server-based filtering) or disabled (local filtering).
Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.

RELATED DOCUMENTATION

Add an Antispam Profile

You are here: **Security Services** > **UTM** > **Antispam Profiles**.

To add an antispam profile:

1. Click the add icon (**+**) on the upper right side of the Antispam Profiles page.
   The Create Antispam Profiles page appears.
2. Complete the configuration according to the guidelines provided in Table 245 on page 871.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 245: Fields on the Create Antispam Profiles Page

Field	Action
General Information	
Name	Enter a unique name for your antispam profile.
Sophos Blocklist	Enable this option to use server-based spam filtering. By default, this option is enabled. **NOTE**: If you disable this option, then local spam filtering is used.
Action	
Default Action	Select an option to be taken when a spam message is detected. The options available are: • Tag E-Mail Subject Line—Adds a custom string at the beginning of the subject of the e-mail. • Tag SMTP Header—Adds a custom string to the e-mail header. • Block E-Mail—Blocks the spam e-mail. • None—No action taken.
Custom Tag	Enter a custom string for identifying a message as spam. By default, the device uses ***SPAM***.

RELATED DOCUMENTATION

About the Antispam Profiles Page | 868

Clone an Antispam Profile | 871

Edit an Antispam Profile | 872

Delete Antispam Profile | 873

Clone an Antispam Profile

You are here: **Security Services** > **UTM** > **Antispam Profiles**.

To clone an antispam profile:

1. Select an antispam profile that you want to clone and select **Clone** from the More link.

   NOTE: Alternatively, you can right-click on the selected antispam profile and select **Clone**.

   The Clone Antispam Profiles page appears with editable fields. For more information on the fields, see "Add an Antispam Profile" on page 870.

2. Click **OK** to save the changes.

   A cloned antispam profile is created for the selected antispam profile. By default, the name of the cloned antispam profile is in the format: ***<Antispam profile name>***_**clone**.

RELATED DOCUMENTATION

About the Antispam Profiles Page | 868
Add an Antispam Profile | 870
Edit an Antispam Profile | 872
Delete Antispam Profile | 873

Edit an Antispam Profile

You are here: **Security Services** > **UTM** > **Antispam Profiles**.

To edit an antispam profile:

1. Select an existing antispam profile that you want to edit on the Antispam Profiles page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Antispam Profiles page appears. You can modify any previous changes done to Sophos Blocklist, Default Action, and Custom Tag for the selected antispam profile. For more information on the options, see "Add an Antispam Profile" on page 870.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Antispam Profiles Page | 868
Add an Antispam Profile | 870

Clone an Antispam Profile | 871

Delete Antispam Profile | 873

Delete Antispam Profile

You are here: **Security Services** > **UTM** > **Antispam Profiles**.

To delete antispam profiles:

1. Select one or more antispam profiles that you want to delete on the Antispam Profiles page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Antispam Profiles Page | 868

Add an Antispam Profile | 870

Clone an Antispam Profile | 871

Edit an Antispam Profile | 872

CHAPTER 75

UTM Content Filtering Profiles

IN THIS CHAPTER

About the Content Filtering Profiles Page

IN THIS SECTION

You are here: **Security Services** > **UTM** > **Content Filtering Profiles**.

Use this page to configure content filtering.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a content filtering profile. See "Add a Content Filtering Profile" on page 876.
- Clone a content filtering profile. See "Clone a Content Filtering Profile" on page 880
- Edit a content filtering profile. See "Edit a Content Filtering Profile" on page 881.

- Delete a content filtering profile. See "Delete Content Filtering Profile" on page 882.
- View the details of a content filtering profile—To do this, select the content filtering profile for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected content filtering profile and select **Detailed View**.
  - Mouse over to the left of the selected content filtering profile and click **Detailed View**.
- Advanced search for content filtering profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.
- Filter the content filtering profiles based on select criteria. To do this, select the filter icon at the top right-hand corner of the content filtering profiles table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the content filtering profiles table. To do this, click the Show Hide Columns icon in the top right corner of the content filtering profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 246 on page 876 describes the fields on the Content Filtering Profiles page.

Table 246: Fields on the Content Filtering Profiles Page

Field	Description
Name	Displays the unique name of the content filtering profile.
Permit Command List	Displays the permitted protocol command name.
Block Command List	Displays the blocked protocol command.
Notification Type	Displays the notification type opted.

RELATED DOCUMENTATION

- Add a Content Filtering Profile | 876
- Edit a Content Filtering Profile | 881
- Delete Content Filtering Profile | 882

Add a Content Filtering Profile

You are here: **Security Services** > **UTM** > **Content Filtering Profiles**.

To add a content filtering profile:

1. Click the add icon (**+**) on the upper right side of the Content Filtering Profiles page.
   The Create Content Filtering page appears.
2. Complete the configuration according to the guidelines provided in Table 247 on page 877.
3. Click **Finish**.
   The Summary page is displayed with the configurations you have made.
4. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
   A new content filter profile is created.

Table 247: Fields on the Create Content Filtering Profiles Page

Field	Action
General - General Information	
Name	Enter a unique name for the content filtering profile.
Notification Options	
Notification Mail Sender	Select the **Notify Mail Sender** check box to send an e-mail when a virus is detected and a content block is triggered.
Notification Type	Select the **None**, **Protocol Only**, or **Message** options from the list to specify the type of notification sent when a content block is triggered.
Custom Notification Message	Specifies the customized message text for the content-block notification. Enter the text for this custom notification message (if you are using one).
Protocol Commands	

Table 247: Fields on the Create Content Filtering Profiles Page *(Continued)*

Field	Action
Command Block List	Select the protocol command name to be blocked from the list. By blocking certain commands, traffic can be controlled on the protocol command level. To create a protocol command inline and add it to the command block list: 1. Click **Create Protocol Command**. The Add Protocol Command List window appears. 2. Enter the following details: • Name—Enter a unique name for the protocol command list. You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters. • Values—Click **+** and enter a value in the value list and click the tick mark. To delete any value list, select the value and click on the delete icon. 3. Click **OK**. A new protocol command is created and added to the command block list.
Command Permit List	Select the protocol command name to be permitted from the list. Click **Create Protocol Command** to create a protocol command inline and add it to the permitted list.
Content Types	

Table 247: Fields on the Create Content Filtering Profiles Page *(Continued)*

Field	Action
Block Content Type	Select the content type you want to block. The available options are: • ActiveX • Windows executables (.exe) • HTTP Cookie • Java Applet • ZIP files
File Extensions	
Extension Block List	Select an extension from the list that you want to block. To create a file extension inline and add it to the extension block list: 1. Click **Create File Extensions**. The Add File Extension List window appears. 2. Enter the following details: • Name—Enter a unique name for the file extension list. You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters. • Values—Select one or more values in the Available Column and move it to the Selected Column using the right arrow. 3. Click **OK**. A new file extension is created and added to the extension block list.
MIME Types	

Table 247: Fields on the Create Content Filtering Profiles Page *(Continued)*

Field	Action
MIME Block List	Select the MIME type from the list. To create a MIME list inline and add it to the MIME block list: 1. Click **Create MIME List**. The Add MIME Pattern List window appears. 2. Enter the following details: • Name—Enter an unique name for the MIME pattern list. You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 40 characters. • Values—Click **+** and enter a value in the value list and click the tick mark. To delete any value list, select the value and click on the delete icon. 3. Click **OK**. A new MIME list is created and added to the MIME block list.
MIME Permit List	Select the MIME type from the list. Click **Create MIME List** to create a MIME list inline and add it to the MIME permit list.

RELATED DOCUMENTATION

About the Content Filtering Profiles Page | 874
Edit a Content Filtering Profile | 881
Delete Content Filtering Profile | 882

Clone a Content Filtering Profile

You are here: **Security Services** > **UTM** > **Content Filtering Profiles**.

To clone a content filtering profile:

1. Select a content filtering profile that you want to clone and select **Clone** from the More link.

   NOTE: Alternatively, you can right-click on the selected content filtering profile and select **Clone**.

   The Clone Content Filtering Profiles page appears with editable fields. For more information on the fields, see "Add a Content Filtering Profile" on page 876.

2. Click **OK** to save the changes.

   A cloned content filtering profile is created for the selected content filtering profile. By default, the name of the cloned content filtering profile is in the format: ***<Content filtering profile name>***_**clone**.

RELATED DOCUMENTATION

About the Content Filtering Profiles Page | 874

Edit a Content Filtering Profile | 881

Delete Content Filtering Profile | 882

Edit a Content Filtering Profile

You are here: **Security Services** > **UTM** > **Content Filtering Profiles**.

To edit a content filtering profile:

1. Select an existing content filtering profile that you want to edit on the Content Filtering profiles page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Content Filtering Profiles page appears with editable fields. For more information on the options, see "Add a Content Filtering Profile" on page 876.

   NOTE: Alternatively, you can right-click on the selected content filtering profile and select **Edit Profile**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Content Filtering Profiles Page | 874

Delete Content Filtering Profile

You are here: **Security Services** > **UTM** > **Content Filtering Profiles**.

To delete a content filtering profile:

1. Select a content filtering profile that you want to delete on the Content Filtering Profiles page.
2. Click the delete icon available on the upper right side of the page.

> **NOTE**: Alternatively, you can right-click on the selected content filtering profile and select **Delete Profile**.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

CHAPTER 76

UTM Custom Objects

IN THIS CHAPTER

About the Custom Objects Page

IN THIS SECTION

You are here: **Security Services** > **UTM** > **Custom Objects**.

Use the Custom Objects page to define your own objects for URL filtering, antivirus filtering, and content filtering.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a MIME pattern list. See "Add a MIME Pattern List" on page 886.
- Add a file extension list. See "Add a File Extension List" on page 888.
- Add a protocol command list. See "Add a Protocol Command List" on page 888.
- Add an URL pattern list. See "Add a URL Pattern List" on page 889.
- Add an URL category list. See "Add a URL Category List" on page 890.
- Add a custom message list. See "Add a Custom Message List" on page 892.
- Edit custom objects. See "Edit Custom Objects" on page 893.
- Delete custom objects. See "Delete Custom Objects" on page 894.
- Clone custom objects. See "Clone Custom Objects" on page 893
- View the details of custom objects—To do this, select the custom object for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected custom object and select **Detailed View**.
  - Mouse over to the left of the selected custom object and click **Detailed View**.
- Filter the custom objects based on select criteria. To do this, select the filter icon at the top right-hand corner of the custom objects table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the custom objects table. To do this, click the Show Hide Columns icon in the top right corner of the custom objects table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for custom objects. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

   NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 248 on page 885 describes the fields on the Custom Objects page.

Table 248: Fields on the Custom Objects Page

Field	Description
MIME Pattern List	
Name	Displays the user-defined name or a predefined MIME pattern name.
Value	Displays the user-defined value or a predefined MIME pattern value.
Filename Extension List	
Name	Displays the user-defined name or a predefined file extension name.
Value	Displays the user-defined value or a predefined file extension value.
Protocol Command List	
Name	Displays only the user-defined protocol command names.
Value	Displays only the user-defined protocol command values.
URL Pattern List	

Table 248: Fields on the Custom Objects Page *(Continued)*

Field	Description
Name	Displays only the user-defined URL pattern names.
Value	Displays only the user-defined URL pattern values.
URL Category List	
Name	Displays only the predefined URL categories.
Value	Displays only the predefined URL categories from the SurfControl server. You can also configure URLs. The URLs configured in the URL pattern list are displayed here.
Custom Message List The Custom Message List displays the custom messages that you have created. It also displays the type of action taken when you create block message or URL, or quarantine message or URL for each category.	
Name	Displays the name of the custom message that you have created.
Type	Displays the type of custom message. The options are Redirect-URL or User Message.
Content	Displays the content of the custom message. It is either a user message or a URL to which you will be redirected.

RELATED DOCUMENTATION

Add a MIME Pattern List | 886

Add a MIME Pattern List

You are here: **Security Services** > **UTM** > **Custom Objects**.

To add a MIME pattern list:

1. Click the **MIME Pattern List** tab.
2. Click the add icon (**+**) on the upper right side of the MIME Pattern List tab.

   The Add MIME Pattern List page appears.
3. Complete the configuration according to the guidelines provided in Table 249 on page 887.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 249: Fields on the Add MIME Pattern List Page

Field	Action
Name	Enter a name for the MIME pattern list. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 40 characters.
Value	To add a MIME pattern value: 1. Click **+**. 2. Enter the MIME pattern value in the Value List. **NOTE**: Value must be two strings separated by slash(/): • The first string beginning with a letter or number and consisting of alphanumeric characters, underscores and dashes. Dashes cannot be shown continuously in the string. • The second string can be null or begin with a letter or number and consisting of alphanumeric characters, underscores, dashes, dots and pluses. Dashes, dots, and pluses cannot be shown continuously in the string. 3. Click the tick mark. If you want to delete any MIME pattern values, select the value and click the delete icon.

RELATED DOCUMENTATION

Clone Custom Objects | **893**

Edit Custom Objects | **893**

Delete Custom Objects | **894**

Add a File Extension List

You are here: **Security Services** > **UTM** > **Custom Objects**.

To add a file extension list:

1. Click the **File Extension List** tab.
2. Click the add icon (**+**) on the upper right side of the File Extension List tab.

   The Add File Extension List page appears.
3. Complete the configuration according to the guidelines provided in Table 250 on page 888.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 250: Fields on the Add File Extension List Page

Field	Action
Name	Enter a name for the file extension list. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters.
Value	Select values from the list in the Available column to associate it with the file extension name and then click the right arrow to move it to the Selected column.

RELATED DOCUMENTATION

Clone Custom Objects | 893

Edit Custom Objects | 893

Delete Custom Objects | 894

Add a Protocol Command List

You are here: **Security Services** > **UTM** > **Custom Objects**.

To add a protocol command list:

1. Click the **Protocol Command List** tab.
2. Click the add icon (**+**) on the upper right side of the Protocol Command List tab.

The Add Protocol Command List page appears.

3. Complete the configuration according to the guidelines provided in Table 251 on page 889.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 251: Fields on the Add Protocol Command List Page

Field	Action
Name	Enter a name for the protocol command list. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters.
Value	To add a protocol command value: 1. Click **+**. 2. Enter the protocol command value in the Value List. 3. Click the tick mark. If you want to delete any protocol command values, select the value and click the delete icon.

RELATED DOCUMENTATION

Clone Custom Objects | 893
Edit Custom Objects | 893
Delete Custom Objects | 894

Add a URL Pattern List

You are here: **Security Services** > **UTM** > **Custom Objects**.

To add a URL pattern list:

1. Click the **URL Pattern List** tab.
2. Click the add icon (**+**) on the upper right side of the URL Pattern List tab.
   The Add URL Pattern List page appears.
3. Complete the configuration according to the guidelines provided in Table 252 on page 890.

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 252: Fields on the Add URL Pattern List Page

Field	Action
Name	Enter a name for the URL pattern list. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters. **NOTE**: Multiple URLs are supported in a pattern.
Value	To add a URL pattern value: 1. Click **+**. 2. Enter the URL pattern value in the Value List. 3. Click the tick mark. If you want to delete any URL pattern values, select the value and click the delete icon.

RELATED DOCUMENTATION

Clone Custom Objects | 893

Edit Custom Objects | 893

Delete Custom Objects | 894

Add a URL Category List

You are here: **Security Services** > **UTM** > **Custom Objects**.

To add a URL category list:

1. Click the **URL Category List** tab.
2. Click the add icon (**+**) on the upper right side of the URL Category List tab.
   The Add URL Category List page appears.
3. Complete the configuration according to the guidelines provided in Table 253 on page 891.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 253 on page 891 provides guidelines on using the fields on the Add URL Category List page.

Table 253: Fields on the Add URL Category List Page

Field	Action
Name	Enter a name for the URL category list. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 59 characters.
Value	Select values from the list in the Available column to associate it with the URL category list name and then click the right arrow to move it to the Selected column. To add a new URL pattern inline: 1. Click **Create New URL Pattern**. The Add URL Pattern List page appears. 2. Enter a URL pattern name. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters. 3. Click **+** to add a URL pattern value. 4. Enter the URL pattern value in the Value List. 5. Click the tick mark. 6. Optional. If you want to delete any URL pattern values, select the value and click the delete icon. 7. Click **OK** to save the changes.

RELATED DOCUMENTATION

Clone Custom Objects | 893

Edit Custom Objects | 893

Delete Custom Objects | 894

Add a Custom Message List

You are here: **Security Services** > **UTM** > **Custom Objects**.

To add a custom message list:

1. Click the **Custom Message List** tab.
2. Click the add icon (**+**) on the upper right side of the Custom Message List tab.

   The Add Custom Message List page appears.
3. Complete the configuration according to the guidelines provided in Table 254 on page 892.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 254: Fields on the Add Custom Message List Page

Field	Action
Name	Enter a name for the custom message list. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 59 characters.
Type	Select an option: • Redirect URL—Specifies custom redirect URL server. • User Message—Specifies that website access has been blocked by an organization's access policy.
Content	Enter content of the custom message; maximum length is 1024 characters. It is either a user message or a URL to which you will be redirected.

RELATED DOCUMENTATION

Clone Custom Objects | **893**

Edit Custom Objects | **893**

Delete Custom Objects | **894**

Clone Custom Objects

You are here: **Security Services** > **UTM** > **Custom Objects**.

You can clone all of the following custom objects:

- MIME pattern list
- File extension list
- Protocol command list
- URL pattern list
- URL category list
- Custom message list

To clone a custom object:

1. Right-click any of the custom objects and select **Clone**. You can also select **Clone** from the More link.
   The clone page for the selected custom object appears with editable fields.
2. Make the required changes in the editable fields.
3. Click **OK** to save the changes.
   A cloned custom object is created for the selected custom objects. By default, the name of the cloned custom objects is in the format: ***<custom objects name>***_**clone**.

RELATED DOCUMENTATION

Add a MIME Pattern List | 886

Add a File Extension List | 888

Add a Protocol Command List | 888

Add a URL Pattern List | 889

Add a URL Category List | 890

Add a Custom Message List | 892

Edit Custom Objects

You are here: **Security Services** > **UTM** > **Custom Objects**.

You can edit all of the following custom objects:

- MIME pattern list
- File extension list
- Protocol command list
- URL pattern list
- URL category list
- Custom message list

To edit a custom objects:

1. Select any of the existing custom objects that you want to edit on the Custom Objects page.
2. Click the pencil icon available on the upper right side of the page.

   The edit page for the selected custom object appears with editable fields. You can modify the parameters of the custom object as required.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

Add a MIME Pattern List | 886

Add a File Extension List | 888

Add a Protocol Command List | 888

Add a URL Pattern List | 889

Add a URL Category List | 890

Add a Custom Message List | 892

Delete Custom Objects

You are here: **Security Services** > **UTM** > **Custom Objects**.

You can delete all of the following custom objects:

- MIME pattern list
- File extension list
- Protocol command list

- URL pattern list
- URL category list
- Custom message list

To delete a custom object:

1. Select any of the existing custom objects that you want to delete from the Custom Objects page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the selected custom object.

RELATED DOCUMENTATION

About the Custom Objects Page | **883**

Clone Custom Objects | **893**

Edit Custom Objects | **893**

CHAPTER 77

UTM Policies

IN THIS CHAPTER

About the UTM Policies Page

IN THIS SECTION

You are here: **Security Services** > **UTM** > **UTM Policies**.

Use this page to configure UTM Policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a UTM policy. See "Add a UTM Policy" on page 898.
- Clone a UTM policy. See "Clone a UTM Policy" on page 901.
- Edit a UTM policy. See "Edit a UTM Policy" on page 902.

- Delete a UTM policy. See "Delete UTM Policy" on page 902.
- View the details of a UTM policy—To do this, select the UTM policy for which you want to view the details and select any of the following options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected UTM policy and select **Detailed View**.
  - Mouse over to the left of the selected UTM policy and click **Detailed View**.
- Advanced search for UTM policy. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.
- Show or hide columns in the UTM policy table. To do this, click the Show Hide Columns icon in the top right corner of the UTM policies table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 255 on page 898 describes the fields on the UTM policy page.

Table 255: Fields on the UTM Policy Page

Field	Description
Name	Displays the UTM policy name.
Antivirus	Displays the antivirus profile.
Web Filtering	Displays the Web filtering profile.
Antispam	Displays the antispam profile.
Content Filtering	Displays the content filtering profiles.

RELATED DOCUMENTATION

Add a UTM Policy | 898

Add a UTM Policy

You are here: **Security Services** > **UTM** > **UTM Policies**.

To add a UTM policy:

1. Click the add icon (**+**) on the upper right side of the UTM Policy page.
   The Create UTM Policies page appears.
2. Complete the configuration according to the guidelines provided in Table 256 on page 899.
3. Click **Finish**.
   The Summary page is displayed with the configurations you have made.
4. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
   A UTM policy is created.

Table 256: Fields on the Create UTM Policies Page

Field	Action
General—General Information	
Name	Enter a UTM policy name.
Antivirus—Antivirus Profiles by Traffic Protocol	
Apply to all protocols	Select the check box to apply the default profile to all protocols such as HTTP, FTP, IMAP, SMTP, and POP3. If you do not select the check box, you can apply different profiles to different protocols.
HTTP	Select an option from the list to specify the UTM policy for the HTTP protocol to be scanned.
FTP Upload	Select an option from the list to specify the UTM policy for the FTP protocol to be scanned.
FTP Download	Select an option from the list to specify the UTM policy for the FTP protocol to be scanned.
IMAP	Select an option from the list to specify the UTM policy for the IMAP protocol to be scanned.
SMTP	Select an option from the list to specify the UTM policy for the SMTP protocol to be scanned.
POP3	Select an option from the list to specify the UTM policy for the POP3 protocol to be scanned.
Create Another Profile	Click **Create Another Profile** to create an antivirus profile inline. For more information on the fields, see "Add an Antivirus Profile" on page 810.
Web Filterings—Web Filtering Profiles by Traffic Protocol	

Table 256: Fields on the Create UTM Policies Page *(Continued)*

Field	Action
HTTP	Select an option from the list to specify the UTM policy for the HTTP protocol to be scanned.
Create Another Profile	Click **Create Another Profile** to create Web filtering profile inline. For more information on the fields, see "Add a Web Filtering Profile" on page 841.
Antispam—Antispam Profiles by Traffic Protocol	
SMTP profile	Select an option from the list to specify the UTM policy for the SMTP protocol to be scanned.
Create Another Profile	Click **Create Another Profile** to create antispam profile inline. For more information on the fields, see "Add an Antispam Profile" on page 870.
Content Filtering—Content Filtering Profiles by Traffic Protocol	
Apply to all protocols	Select the check box to apply the default profile to all protocols such as HTTP, FTP, IMAP, SMTP, and POP3. If you do not select the check box, you can apply different profiles to different protocols.
HTTP	Select an option from the list to specify the UTM policy for the HTTP protocol to be scanned.
FTP Upload	Select an option from the list to specify the UTM policy for the FTP protocol to be scanned.
FTP Download	Select an option from the list to specify the UTM policy for the FTP protocol to be scanned.
IMAP	Select an option from the list to specify the UTM policy for the IMAP protocol to be scanned.

Table 256: Fields on the Create UTM Policies Page *(Continued)*

Field	Action
SMTP	Select an option from the list to specify the UTM policy for the SMTP protocol to be scanned.
POP3	Select an option from the list to specify the UTM policy for the POP3 protocol to be scanned.
Create Another Profile	Click **Create Another Profile** to create content filtering Profile inline. For more information on the fields, see "Add a Content Filtering Profile" on page 876.

RELATED DOCUMENTATION

About the UTM Policies Page | **896**
Clone a UTM Policy | **901**
Edit a UTM Policy | **902**
Delete UTM Policy | **902**

Clone a UTM Policy

You are here: **Security Services** > **UTM** > **UTM Policies**.

To clone a UTM policy:

1. Select a UTM policy that you want to clone and select **Clone** from the More link.

   NOTE: Alternatively, you can right-click on the selected UTM policy and select **Clone**.

   The Clone UTM Policies page appears with editable fields. For more information on the fields, see "Add a UTM Policy" on page 898.

2. Click **OK** to save the changes.

   A cloned UTM policy is created for the selected UTM policy. By default, the name of the cloned UTM policy is in the format: ***<UTM policy name>***_**clone**.

RELATED DOCUMENTATION

About the UTM Policies Page | 896

Edit a UTM Policy | 902

Delete UTM Policy | 902

Edit a UTM Policy

You are here: **Security Services** > **UTM** > **UTM Policies**.

To edit a UTM policy:

1. Select an existing UTM policy that you want to edit on the UTM Policy page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit UTM Policy page appears with editable fields. For more information on the options, see "Add a UTM Policy" on page 898.

   NOTE: Alternatively, you can right-click on the selected UTM policy and select **Edit Policy**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the UTM Policies Page | 896

Delete UTM Policy | 902

Delete UTM Policy

You are here: **Security Services** > **UTM** > **UTM Policies**.

To delete a UTM policy:

1. Select a UTM policy that you want to delete on the UTM Policy page.
2. Click the delete icon available on the upper right side of the page.

   NOTE: Alternatively, you can right-click on the selected UTM policy and select **Delete Policy**.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the UTM Policies Page | **896**
- Clone a UTM Policy | **901**
- Add a UTM Policy | **898**

CHAPTER 78

IPS Policies

IN THIS CHAPTER

About the IPS Policies Page

IN THIS SECTION

You are here: **Security Services** > **IPS** > **Policies**.

An intrusion prevention system (IPS) policy defines how your device handles the network traffic. It allows you to enforce various attack detection and prevention techniques on traffic traversing your network. You can define policy rules to match a section of traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

Tasks You Can Perform

You can perform the following tasks from this page:

- Import predefined policies. See "Import IPS Predefined Policies" on page 906.
- Set an IPS policy as default policy. To do this, select an existing IPS policy and click **More** > **Set Default**.
- Create an IPS policy. See "Add an IPS Policy" on page 907.

  NOTE: IPS policies that are created by root users in root-logical-system are not displayed in security profile advanced settings if you have logged in as a logical system user.

- Edit an IPS policy. See "Edit an IPS Policy" on page 908.
- Delete an IPS policy. See "Delete an IPS Policy" on page 909.
- Clone an IPS policy. See "Clone an IPS Policy" on page 907.
- Add rules to the IPS policy. See "Add Rules to an IPS Policy" on page 909.
- Edit an IPS policy rule. See "Edit an IPS Policy Rule" on page 919.
- Delete an IPS policy rule. See "Delete IPS Policy Rule" on page 920.
- Search a policy. To do this:

  1. Click the search icon in the top right corner of the IPS Policies table.
  2. Enter the policy name that you want to find and click the search icon.

     Based on your input, a list of matching policies appears.

- Show or hide columns in the IPS Policies table. To do this, click the Show Hide Columns icon in the top right corner of the IPS Policies table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 257 on page 906 describes the fields on the IPS Policies page.

Table 257: Fields on the IPS Policies Page

Field	Description
Policy Name	Displays the IPS policy name.
Rules	Displays the number of rules that are configured for the policy or allows you to add new rules to the policy.
Predefined or Custom	Displays if the IPS policy is a predefined or a custom policy. **NOTE**: This option is not available for logical systems and tenants.

RELATED DOCUMENTATION

- Add an IPS Policy | **907**
- Add Rules to an IPS Policy | **909**
- Edit an IPS Policy | **908**
- Delete an IPS Policy | **909**
- Clone an IPS Policy | **907**

Import IPS Predefined Policies

The predefined policies are templates which can be used as a guideline. Each template is set of rules of a specific rulebase type that you can clone and then update to meet your needs. Use this page to import the IPS predefined policies.

NOTE: This option is not available for logical systems and tenants.

To import the predefined policy templates:

1. Click **Import Predefined Policies** at the top-right of the IPS Policies page.
   The Import Predefined Policies page appears.
2. Select the predefined policy templates from the Available column that you want to import.
3. Click on the right arrow to move the selected predefined policy templates to the Selected column.

4. Click **OK**.
   The imported predefined policy template are displayed in the IPS Policies page.

RELATED DOCUMENTATION

- About the IPS Policies Page | **904**
- Add an IPS Policy | **907**
- Add Rules to an IPS Policy | **909**

Add an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To add an IPS policy:

1. Click the add icon (**+**) on the upper right side of the IPS Policies page.
   The Create IPS Policy page appears.
2. Enter a name for the IPS policy.
   Name of the IPS policy must be a unique string of alphanumeric and special characters, including colons, periods, hyphens, and underscores; 250-character maximum.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
   The IPS policy is displayed on the IPS Policies page.

RELATED DOCUMENTATION

- About the IPS Policies Page | **904**
- Add Rules to an IPS Policy | **909**
- Edit an IPS Policy | **908**
- Delete an IPS Policy | **909**
- Clone an IPS Policy | **907**

Clone an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To clone an IDP policy:

1. Select an IPS policy that you want to clone and click **More** > **Clone** on the upper right side of the IPS Policies page.

   The Clone IPS Policy page appears with the editable name field. By default, the clone name will show as *<IPS policy name>*_clone.

2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
   You can see the cloned IPS policy on the IPS Policies page. You can edit the rules of the cloned IPS policy. For more information on the IPS policy and its rules, see "Add an IPS Policy" on page 907 and "Add Rules to an IPS Policy" on page 909.

RELATED DOCUMENTATION

About the IPS Policies Page | 904
Edit an IPS Policy | 908
Delete an IPS Policy | 909
Add Rules to an IPS Policy | 909
Edit an IPS Policy Rule | 919

Edit an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To edit an IPS policy:

1. Select an existing IPS policy that you want to edit on the IPS Policies page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit IPS Policy page appears with editable fields. For more information on the options, see "Add an IPS Policy" on page 907.

   NOTE: Alternatively, you can right-click on the selected IPS policy and select **Edit**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the IPS Policies Page | 904

Add an IPS Policy | 907
Add Rules to an IPS Policy | 909
Clone an IPS Policy | 907
Delete an IPS Policy | 909

Delete an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To delete an IPS policy:

1. Select an IPS policy that you want to delete on the IPS Policies page.
2. Click the delete icon available on the upper right side of the page.

   NOTE: Alternatively, you can right-click on the selected IPS policy and select **Delete**.

3. Click **Yes** to delete or click **No** to retain the policy.

RELATED DOCUMENTATION

About the IPS Policies Page | 904
Add an IPS Policy | 907
Add Rules to an IPS Policy | 909
Edit an IPS Policy | 908
Clone an IPS Policy | 907

Add Rules to an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To add rules to an IPS policy:

NOTE: You can only add rules for the custom IPS policies.

1. Click **Add Rules** or on the rule number available next to the column of your IPS policy name.
   The IPS Rules page appears.
2. Click the add icon (**+**) on the upper right side of the IPS Rules or Exempt Rules page.
   The IPS Rules or Exempt Rules page with the inline editable fields will appear.
3. Complete the configuration according to the guidelines provided in Table 258 on page 910.
4. Click the tick icon on the right-side of the row once done with the configuration.
   Once you configure the IPS policy rules, you can associate the IPS policy with the security policy.

Table 258: Fields on the IPS Rules or Exempt Rules Page

Field	Action
Rule Name	Enter the rule name for the IPS policy.
Description	Enter the description for the rule.
Network Criteria	
Sources	
Source zone	Select a source zone to be associated with the IPS policy: • Not configured—Matches the configured source zone from firewall policy. • Any—Matches any source zone from firewall policy. • Specific—Select a source zone from the list where network traffic originates.
Source addresses	Select a source address to be associated with the IPS policy: • Not configured—Matches the configured source IP address from firewall policy. • Any—Matches any source IP address from firewall policy. • Specific—A source IP address from which network traffic originates. Select the addresses from the Available column and then click the right arrow to move it to the Selected column. You can select **Exclude Selected** to exclude only the selected address from the list.
Destinations	

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Destination zone	Select a destination zone to be associated with the IPS policy: • Not configured—Matches the configured destination zone from firewall policy. • Any—Matches any destination zone from firewall policy. • Specific—Select a destination zone from the list to which network traffic is sent.
Destination addresses	Select a destination address to be associated with the IPS policy: • Not configured—Matches the configured destination IP address from firewall policy. • Any—Matches any destination IP address from firewall policy. • Specific—A destination IP address to which the network traffic is sent. Select the addresses from the Available column and then click the right arrow to move it to the Selected column. You can select **Exclude Selected** to exclude only the selected address from the list.
IPS Signatures	
Add	Select predefined or custom signatures from the list to add it to the IPS policy rules.
Delete	Select the IPS signatures you do not want to add to the IPS policy rules and click the delete icon.
Name	Displays name of the IPS predefined or custom signatures.
Category	Displays the predefined attack or attack groups categories. For example, App, HTTP, and LDAP.
Severity	Displays the attack severity level that the signature reports.
Attack Type	Displays the attack type (signature or anomaly).

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Recommended Action	Displays the specified action taken from the device when it detects an attack. For example, ignore and drop.
Type	Displays if the IPS signature type is predefined or custom.
Add Predefined Signatures	
View by	View and select the desired predefined attacks or attack groups and click **OK** to add it to the selected IPS policy.
Show or Hide Columns	Use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
Name	Displays name of the predefined attack objects or attack object group.
Category	Displays the predefined attack or attack groups categories. For example, App, HTTP, and LDAP.
Severity	Displays the attack severity level that the signature reports.
Type Attack	Displays the attack type (signature or anomaly).
Recommended	Displays the added predefined attacks recommended by Juniper Networks to the dynamic attack group.
Recommended Action	Displays the specified action taken from the device when it detects an attack. For example, ignore and drop.
Performance	Displays a performance filter (fast, normal, slow, and unknown) to add attack objects based on the performance level that is vulnerable to the attack.
Direction	Displays the connection direction (any, client-to-server, or server-to-client) of the attack.

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Add Custom Signatures	
View by	View and select the desired custom attacks, static groups, or dynamic groups and click **OK** to add it to the selected IPS policy.
Custom Signatures—Custom Attacks	
Name	Displays the custom attack object name.
Severity	Displays the attack severity level that the signature reports.
Attack Type	Displays the attack type (signature or anomaly).
Recommended Action	Displays the specified action taken from the device when it detects an attack. For example, ignore and drop.
Custom Signatures—Static Group	
Name	Displays static group name for the custom signatures.
Group Members	Displays the name of the attack object or group attack object. The members can be predefined attacks, predefined attack groups, custom attacks, or custom dynamic groups.
Custom Signatures—Dynamic Groups	
Name	Displays dynamic group name for the custom signatures.
Attack Prefix	Displays prefix match for attack names. For example: HTTP:*
Severity	Displays the attack severity level that the signature reports.

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Attack Type	Displays the attack type (signature or anomaly).
Category	Displays the dynamic attack groups categories. For example, App, HTTP, and LDAP.
Direction	Displays the connection direction (any, client-to-server, or server-to-client) of the attack.

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Action	**NOTE**: This option is not available for exempt rules. Select any one of the actions from the list: • Recommended (default)—All predefined attack objects have a default action associated with them. This is the action that we recommend when that attack is detected. • No Action—No action is taken. Use this action when you want to only generate logs for some traffic. • Drop Connection—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address. • Close Client—Closes the connection and sends an RST packet to the client but not to the server. • Close Server—Closes the connection and sends an RST packet to the server but not to the client. • Close Client & Server—Closes the connection and sends an RST packet to both the client and the server. • Ignore Connection—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. • Mark DiffServ—Assigns the indicated service-differentiation value to the packet in an attack, then passes them on normally.
Options **NOTE**: This option is not available for exempt rules.	
Log Attacks	Enable the log attacks to create a log record that appears in the log viewer.

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Log Packets	Enable the log packets to capture the packets received before and after the attack for further offline analysis of attacker behavior.
Advanced **NOTE**: This option is not available for exempt rules.	
Threat Profiling **NOTE**: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, `request services security-intelligence download`.	
Add attacker to feed	Select from the list to add the attackers IP addresses to the feed to configure IPS rule with threat profiles.
Add target to feed	Select from the list to add the target IP addresses to the feed to configure IPS rule with threat profiles.
Notifications	
Packets before	Enter the number of packets processed before the attack is captured. Range: 1 through 255. Default is 1. **NOTE**: This option is available when you enable Log Packets.
Packets after	Enter the number of packets processed after the attack is captured. Range: 0 through 255. Default is 1. **NOTE**: This option is available when you enable Log Packets.
Post window timeout	Enter the time limit for capturing post-attack packets for a session. No packet capture is conducted after the timeout has expired. Range: 0 through 1800 seconds. Default is 1 second. **NOTE**: This option is available when you enable Log Packets.

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Alert Flag	Enable this option to set an alert flag in the Alert column of the Log Viewer for the matching log record. **NOTE**: This option is available when you enable Log Attacks.
IP Actions	
Action	Specifies the action that IPS takes against future connections that use the same IP address. Select an IP action from the list: • None—Do not take any action, which is the default setting. • Notify—Don't take any action on future traffic but log the event. • Close—Close future connections of new sessions that match the IP address by sending RST packets to the client and server. • Block—Block future connections of any session that matches the IP address.

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
IP Target	Configure how the traffic should be matched to the configured IP actions. Select an IP target from the list: • None—Do not match any traffic. • Destination address—Match traffic based on the destination IP address of the attack traffic. • Service—For TCP and UDP, match traffic based on the source IP address, source port, destination IP address, and destination port of the attack traffic. • Source address—Match traffic based on the source IP address of the attack traffic. • Source zone—Match traffic based on the source zone of the attack traffic. • Source zone address—Match traffic based on the source zone and source IP address of the attack traffic. • Zone service—Match traffic based on the source zone, destination IP address, destination port, and protocol of the attack traffic.
Refresh timeout	Enable refresh of the IP action timeout (that you specify in the Timeout field) if future traffic matches the configured IP actions.
Timeout	Specifies the number of seconds the IP action should remain effective before new sessions are initiated within that specified timeout value. Enter the timeout value, in seconds. The maximum value is 65,535 seconds. Default is 300 seconds.
Log IP-Action hits	Enable to log information about the IP action against the traffic that matches a rule. By default, this setting is disabled.
Log IP-Action rule creation	Enable to generate an event when the IP action filter is triggered. By default, this setting is disabled.
Rule Modifiers	

Table 258: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

Field	Action
Severity override	Severity level (None, Critical, Info, Major, Minor, Warning) to override the inherited attack severity in the rules. The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational level is least dangerous and is used by network administrators to find flaws in their security systems.
Terminal matching	Enable to mark an IPS rule as terminal. When a terminal rule is matched, the device stops matching for the remaining rules in that IPS policy.

RELATED DOCUMENTATION

- About the IPS Policies Page | **904**
- Edit an IPS Policy Rule | **919**
- Delete IPS Policy Rule | **920**
- Add an IPS Policy | **907**
- Clone an IPS Policy | **907**
- Delete an IPS Policy | **909**

Edit an IPS Policy Rule

You are here: **Security Services** > **IPS** > **Policies**.

To edit an IPS policy rule:

1. Click on the existing IPS policy rule on the IPS Policies page.
   The IPS Rules page appears.
2. Select the IPS or exempt rules you want to edit.
3. Click the pencil icon available on the upper right side of the page.
   Editable fields on the IPS Rules or Exempt Rules page appears.

> **NOTE**: Alternatively, you can right-click on the selected IPS policy and select **Edit**.

4. Edit the required options and click the tick icon on the right-side of the row once done with the configuration.

   For more information on the rules options, see "Add Rules to an IPS Policy" on page 909.

   The selected IPS policy rules are edited.

RELATED DOCUMENTATION

- About the IPS Policies Page | **904**
- Delete IPS Policy Rule | **920**
- Add an IPS Policy | **907**
- Add Rules to an IPS Policy | **909**
- Clone an IPS Policy | **907**
- Delete an IPS Policy | **909**

Delete IPS Policy Rule

You are here: **Security Services** > **IPS** > **Policies**.

To delete an IPS policy rule:

1. Click on the existing IPS policy rule on the IPS Policies page.
   The IPS Rules page appears.
2. Select the IPS or exempt rules you want to delete.
3. Click the delete icon available on the upper right side of the page.
4. Click **Yes** to delete or click **No** to retain the rule.

RELATED DOCUMENTATION

- About the IPS Policies Page | **904**
- Edit an IPS Policy Rule | **919**
- Add an IPS Policy | **907**
- Add Rules to an IPS Policy | **909**
- Clone an IPS Policy | **907**
- Delete an IPS Policy | **909**

CHAPTER 79

IPS Sensor

IN THIS CHAPTER

About the Sensor Page

IN THIS SECTION

You are here: **Security Services** > **IPS** > **Sensor**.

You can configure sensor settings to limit the number of sessions running application identification and also to limit memory usage for application identification.

Field Descriptions

Table 259 on page 921 describes the fields on the Sensor page.

Table 259: Fields on the Sensor Page

Field	Description
Basic Settings	Select to configure basic IPS sensor settings.
IDP Protection Mode	

Table 259: Fields on the Sensor Page *(Continued)*

Field	Description
Protection Mode	Select an option to specify the inspection parameters for efficient inspection of traffic in the device. The options available are: • DataCenter—Disables all STC traffic inspection. • Datacenter Full—Disables all STC traffic inspection. • Perimeter—Inspects all STC (Server To Client) traffic. • Perimeter Full—Inspects all STC traffic.
Intelligent Inspection	
IDP By Pass	Enable or disable the IDP Intelligent Bypass option.
IDP By Pass CPU Threshold	Enter the threshold value. Range: 0 through 99. Default value: 85.
IDP By Pass CPU Tolerance	Enter the CPU tolerance value. Range: 1 through 99. Default value: 5.

Table 259: Fields on the Sensor Page *(Continued)*

Field	Description
Intelligent Inspection	Enable or disable this option. If you enable this option, enter the following details: • Ignore Content Decompression— Enable this option to enable payload content decompression. • Signature Severity—Select the severity level of the attack from the list that the signature will report for IDP processing. The available options are minor, major, and critical. **NOTE**: Click **Clear All** to clear all the selected severity values. • Protocols—Select the protocols from the list that needs to be processed in Intelligent Inspection mode. **NOTE**: Click **Clear All** to clear all the selected protocols. • CPU Threshold (%)—Enter the value of CPU usage threshold percentage for intelligent inspection. Range: 0 through 99 percent. • CPU Tolerance (%)—Enter the value of CPU usage tolerance percentage for intelligent inspection. Range: 1 through 99 percent. • Memory Tolerance—Enter the value of memory tolerance percentage for intelligent inspection. Range: 1 through 100 percent. • Free Memory Threshold—Enter the value of free memory threshold percentage for intelligent inspection. Range: 1 through 100 percent. • Session Bytes Depth—Enter the value of session bytes scanning depth. Range: 1 through 1000000 bytes.
Memory Lower Threshold	Enter the memory lower threshold limit percentage. Range: 1 through 100.

Table 259: Fields on the Sensor Page *(Continued)*

Field	Description
Memory Upper Threshold	Enter the memory upper threshold limit percentage. Range: 1 through 100.
Flow	
Drop On Limit	Enable this option to specify the dropped connections on exceeding resource limits.
Drop On Failover	Enable this option to specify the dropped traffic on HA failover sessions.
Drop If No Policy Loaded	Enable this option to specify all the dropped traffic till IDP policy gets loaded.
Packet Log **NOTE**: Starting in Junos OS Release 19.2R1, Packet Log configuration is available.	
IP Address	Enter the IP address of the destination host to send packet log.
Port	Enter the UDP port number. Range: 0 through 65535.
Source Address	Enter the source IP address used to transport packet log to a host.
Advanced Settings	
IDP Flow	
Log Errors	Enable this option to specify if the flow errors have to be logged. Select an option from the list.
Flow FIFO Max Size	Enter a value to specify the maximum FIFO size. Range: : 1 through 65535. Default value is 1.

Table 259: Fields on the Sensor Page *(Continued)*

Field	Description
Hash Table Size	Enter a value to specify the hash table size. Range: 1024 through 1,000,000. Default value is 1024.
Max Timers Poll Ticks	Enter a value to specify the maximum amount of time at which the timer ticks at a regular interval. Range: 0 through 1000 ticks. Default value is 1000 ticks.
Reject Timeout	Enter a value to specify the amount of time in milliseconds within which a response must be received. Range: 1 through 65,535 seconds. Default value is 300 seconds.
Global	
Enable All Qmodules	Select an option from the list to specify all the qmodules of the global rulebase IDP security policy are enabled.
Enable Packet Pool	Select an option from the list to specify the packet pool is enabled to be used when the current pool is exhausted.
Policy Lookup Cache	Select an option from the list to specify the cache is enabled to accelerate IDP policy lookup.
Memory Limit Percent	Enter a value to specify the limit IDP memory usage at this percent of available memory. Range: 10 through 90 percent.
HTTP X-Forwarded	When you enable this option, during traffic flow, IDP saves the source IP addresses (IPv4 or IPv6) from the contexts of HTTP traffic, and displays it in the attack logs. **NOTE**: Starting in Junos OS Release 20.2R1, HTTP X-Forwarded option is supported.
IPS	

Table 259: Fields on the Sensor Page *(Continued)*

Field	Description
Detect Shellcode	Select an option from the list to specify if shellcode detection has to be applied.
Ignore Regular Expression	Select an option from the list to specify if the sensor has to bypass DFA and PCRE matching.
Process Ignore Server-to-Client	Select an option from the list to specify if the sensor has to bypass IPS processing for server-to-client flows.
Process Override	Select an option from the list to specify if the sensor has to execute protocol decoders even without an IDP policy.
Process Port	Enter an integer to specify a port on which the sensor executes protocol decoders. Range: 0 through 65535.
IPS FIFO Max Size	Enter an integer to specify the maximum allocated size of the IPS FIFO. Range: 1 through 65535.
Minimum Log Supercade	Enter an integer to specify the minimum number of logs to trigger the signature hierarchy feature. Range: 0 through 65535.
Log	
Cache Size	Enter a value to specify the size in bytes for each user's log cache.
Disable Suppression	Enable this option to specify if the log suppression has to be disabled.
Include Destination Address	Select an option from the list to specify if combine log records for events with a matching source address.
Max Logs Operate	Enter a value to specify the maximum number of logs on which log suppression can operate. Range is 255 through 65536.

Table 259: Fields on the Sensor Page *(Continued)*

Field	Description
Max Time Report	Enter a value to specify the time (seconds) after which suppressed logs will be reported. IDP reports suppressed logs after 5 seconds by default.
Start Log	Enter a value to specify the number of log occurrences after which log suppression begins. Log suppression begins with the first occurrence by default. Range is 1 through 128.
Reassembler	
Ignore Memory Overflow	Select an option from the list to specify if the user has to allow per-flow memory to go out of limit.
Ignore Reassembly Memory Overflow	Select an option from the list to specify if the user has to allow per-flow reassembly memory to go out of limit.
Ignore Reassembly Overflow	Enable this option to specify the TCP reassembler to ignore the global reassembly overflow to prevent the dropping of application traffic.
Max Flow Memory	Enter an integer to specify the maximum per-flow memory for TCP reassembly in kilobytes. Range: 64 through 4,294,967,295 kilobytes.
Max Packet Memory	Enter an integer to specify the maximum packet memory for TCP reassembly in kilobytes. Range: 64 through 4,294,967,295 kilobytes
Max Synacks Queued	Enter an integer to specify the maximum limit for queuing Syn/Ack packets with different SEQ numbers. Range: 0 through 5
Packet Log	

Table 259: Fields on the Sensor Page *(Continued)*

Field	Description
Max Sessions	Enter an integer to specify the maximum number of sessions actively conducting pre-attack packet captures on a device at one time. Range: 1 through 100 percent
Total Memory	Enter an integer to specify the maximum amount of memory to be allocated to packet capture for the device. Range: 1 through 100 percent
Detectors	Click **+** and enter the following fields.
Protocol	Select the name of the protocol from the list to enable or disable the detector.
Tunable Name	Select the name of the specific tunable parameter from the list to enable or disable the protocol detector for each of the services.
Tunable Value	Enter the protocol value of the specific tunable parameter to enable or disable the protocol detector for each of the services. Range: 0 to 4294967295

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
20.2R1	Starting in Junos OS Release 20.2R1, HTTP X-Forwarded option is supported.
19.2R1	Starting in Junos OS Release 19.2R1, Packet Log configuration is available.

RELATED DOCUMENTATION

About the IPS Policies Page | 904

CHAPTER 80

ALG

IN THIS CHAPTER

About the ALG Page

IN THIS SECTION

You are here: **Security Services** > **ALG**.

Use this page to configure Application Layer Gateway (ALG).

Field Descriptions

Table 260 on page 929 describes the fields on the ALG page.

Once the configuration is complete, click **OK** to save the changes or click **Reset** to revert back the changes.

Table 260: Fields on the ALG Page

Field	Description
Main	

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Enable PPTP	Select the check box to enable the Point-to-Point Tunneling Protocol (PPTP) for ALG. PPTP is a Layer 2 protocol that tunnels PPP data across TCP/IP networks. The PPTP client is freely available on Windows systems and is widely deployed for building VPNs.
Enable RSH	Select the check box to enable RSH for ALG. The RSH ALG handles TCP packets destined for port 514 and processes the RSH port command. The RSH ALG performs NAT on the port in the port command and opens gates as necessary.
Enable RTSP	Select the check box to enable the Real-Time Streaming Protocol (RTSP) for ALG.
Enable SQL	Select the check box to enable Structured Query Language (SQL) for ALG. The SQLNET ALG processes SQL TNS response frames from the server side. It parses the packet and looks for the (HOST=ipaddress), (PORT=port) pattern and performs NAT and gate opening on the client side for the TCP data channel.
Enable TALK	Select the check box to enable the TALK protocol for ALG. The TALK protocol uses UDP port 517 and port 518 for control-channel connections. The talk program consists of a server and a client. The server handles client notifications and helps to establish talk sessions. There are two types of talk servers: ntalk and talkd. The TALK ALG processes packets of both ntalk and talkd formats. It also performs NAT and gate opening as necessary.
Enable TFTP	Select the check box to enable the Trivial File Transfer Protocol (TFTP) for ALG. The TFTP ALG processes TFTP packets that initiate a request and opens a gate to allow return packets from the reverse direction to the port that sends the request.
DNS	
Enable DNS	Select the check box to enable the domain name system (DNS) for ALG. The DNS ALG monitors DNS query and reply packets and closes the session if the DNS flag indicates the packet is a reply message.

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Doctoring	Select one of the following options: • Sanity Check—Performs only DNS ALG sanity checks. • None—Disables all DNS ALG doctoring.
Maximum Message length	Select a number to specify the maximum DNS message length. Range: 512 through 8192 bytes.
Enable Oversize message drop.	Select the check box to enable oversize message drop.
FTP	
Enable FTP	Select the check box to enable the File Transfer Protocol (FTP) for ALG. The FTP ALG monitors PORT, PASV, and 227 commands. It performs Network Address Translation (NAT) on IP/port in the message and gate opening on the device as necessary. The FTP ALG supports FTP put and FTP get command blocking. When FTP_NO_PUT or FTP_NO_GET is set in the policy, the FTP ALG sends back a blocking command and closes the associated opened gate when it detects an FTP STOR or FTP RETR command.
Enable allow mismatch IP address	Select the check box to allow any mismatch in IP address.
Enable FTPs Extension	Select the check box to enable secure FTP and FTP SSL protocols.
Enable line Break Extension	Select the check box to enable line-break-extension. This option will enable the FTP ALG to recognize the LF as line break in addition to the standard CR+LF (carriage return, followed by line feed).
H323	

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Enable H323	Select the check box to enable the H.323 ALG.
Application Screen	Specify the security screens for the H.323 protocol ALG. Enter the following details: • Message Flood Gatekeeper Threshold—Enter a value. The value range is 1 to 50000 messages per second. Limits the rate per second at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped. This feature is disabled by default. • Action on receiving unknown message: • Enable Permit NAT Applied—Select the check box to specify how unidentified H.323 (unsupported) messages are handled by the device. The default is to drop unknown messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown H.323 messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped. This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing. • Enable Permit Routed—Select the check box to specify that unknown messages be allowed to pass if the session is in route mode. Sessions in transparent mode are treated as though they are in route mode.
DSCP Code Rewrite	Code Point—Select a 6-bit string from the list. Specifies a rewrite-rule for the traffic that passes through a voice over IP Application Layer Gateway (VoIP ALG). The value of code point is in binary format. The VoIP rewrite rules modifies the appropriate class of service (CoS) bits in an outgoing packet through Differentiated Services Code Point (DSCP) mechanism that improves the VoIP quality in a congested network.

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Endpoints	Enter the following details: • Timeout For Endpoint—Enter a timeout value in seconds for entries in the NAT table. Range: 10 through 50,000 seconds Controls the duration of the entries in the NAT table. • Enable Permit Media From Any Source Port—Select this option to allow media traffic from any port number.
IKE-ESP	
Enable IKE-ESP	Select the check box to enable IKE-ESP.
ESP Gate Timeout (sec)	Select the gate timeout from 2 to 30 seconds.
ESP Session Timeout (sec)	Select the ESP timeout session from 60 to 2400 seconds.
ALG State Timeout (Sec)	Select the ALG state time out from 180 to 86400 sec.
MGCP	
Enable MGCP	Select the check box to enable the Media Gateway Control Protocol (MGCP).
Inactive Media Timeout	Select a value to specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected. range is from 10 through 2,550 seconds. Specifies the maximum time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the temporary openings (pinholes) in the firewall MGCP ALG opened for media are closed. The default setting is 120 seconds; the range is from 10 to 2550 seconds. Note that, upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Maximum Call Duration	Select a value from 3 through 720 minutes. Sets the maximum length of a call. When a call exceeds this parameter setting, the MGCP ALG tears down the call and releases the media sessions. The default setting is 720 minutes; the range is from 3 to 720 minutes.
Transaction Timeout	Enter a value from 3 through 50 seconds to specify Specifies a timeout value for MGCP transactions. A transaction is a signaling message, for example, a NTFY from the gateway to the call agent or a 200 OK from the call agent to the gateway. The device tracks these transactions and clears them when they time out.
Application Screen	Enter the following details: • Message Flood Threshold—Enter a value from 2 through 50,000 seconds per media gateway. Limits the rate per second at which message requests to the Media Gateway are processed. Messages exceeding the threshold are dropped by the Media Gateway Control Protocol (MGCP). This feature is disabled by default. • Connection Flood Threshold—Enter a value from 2 through 10,000. Limits the number of new connection requests allowed per Media Gateway (MG) per second. Messages exceeding the ALG. • Action On Receiving Unknown Message—Enter any of the following: • Enable Permit NAT Applied—Select the check box to specify how unidentified MGCP messages are handled by the Juniper Networks device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown MGCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped. • Enable Permit Routed—Select the check box. Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.)

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
DSCP Code Rewrite	Specifies a code-point alias or bit set to apply to a forwarding class for a rewrite rule. Code Point—Enter a six-bit DSCP code point value.
MSRPC	
Enable MSRPC	Select the check box to enable the MSRPC. Provides a method for a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service program's Universal Unique IDentifier (UUID). The specific UUID is mapped to a transport address.
Maximum Group Usage (%)	Select the group usage % from 10 to 100%.
Map Entry Timeout (min)	Select the map entry timeout session from 5 to 4320 minutes.
SCCP	
Enable SCCP	Select the check box to enable the Skinny Client Control Protocol.
Inactive Media Timeout	Select a value from 10 through 600 seconds. Indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the gates opened for media are closed.
Application Screen	Call Flood Threshold—Select a value from 2 through 1,000. Protects SCCP ALG clients from flood attacks by limiting the number of calls they attempt to process.

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Action On Receiving Unknown Messages	• Enable Permit NAT Applied—Select the check box. Specifies how unidentified SCCP messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SCCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped. This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing. • Enable Permit Routed—Select the check box. Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as though they are in route mode.)
DSCP Code Rewrite	Code Point—Enter a six-bit DSCP code point value.
SIP	
Enable SIP	Select the check box to enable Session Initiation Protocol (SIP).
Enable Retain Hold Resource	Select the check box to enable whether the device frees media resources for a SIP, even when a media stream is placed on hold. By default, media stream resources are released when the media stream is held.
Maximum Call Duration	Select a value from 3 through 720 minutes. Sets the absolute maximum length of a call. When a call exceeds this parameter setting, the SIP ALG tears down the call and releases the media sessions. The default setting is 720 minutes, the range is from 3 to 720 minutes.

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
C Timeout	Select a value from 3 through 10 minutes. Specifies the INVITE transaction timeout at the proxy, in minutes; the default is 3. Because the SIP ALG is in the middle, instead of using the INVITE transaction timer value B (which is (64 * T1) = 32 seconds), the SIP ALG gets its timer value from the proxy.
T4 Interval	Select a value from 5 through 10 seconds. Specifies the maximum time a message remains in the network. The default is 5 seconds; the range is 5 through 10 seconds. Because many SIP timers scale with the T4-Interval (as described in RFC 3261), when you change the value of the T4-Interval timer, those SIP timers also are adjusted.
Inactive Media Timeout	Select a value from 10 through 2,550 seconds. Specifies the maximum time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the temporary openings (pinholes) in the firewall SIP ALG opened for media are closed. The default setting is 120 seconds; the range is 10 through 2550 seconds. Note that, upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.
T1 Interval	Select a value from 500 through 5000 milliseconds. Specifies the round-trip time estimate, in seconds, of a transaction between endpoints. The default is 500 milliseconds. Because many SIP timers scale with the T1-Interval (as described in RFC 3261), when you change the value of the T1-Interval timer, those SIP timers also are adjusted.

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Application Screen	Action On Receiving Unknown Message: • Enable Permit NAT Applied—Select the check box to enable handling unidentified SIP messages by the device. This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing. • Enable Permit Routed—Select the check box to enable to allow unknown messages to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.)
Protect Options	• SIP Invite Attack Table Entry Timeout—Enter a value from 1 through 3,600 seconds. Specifies the time (in seconds) to make an attack table entry for each INVITE, which is listed in the application screen. • Enable Attack Protection—Select one of the options: All Servers, Selected Servers, or None. Protects servers against INVITE attacks. Configures the SIP application screen to protect the server at some or all destination IP addresses against INVITE attacks. When you select Selected Servers, enter the destination IP address and click **+**. You can select the destination IP address and click **X** to delete it.
DSCP Code Rewrite	Code Point—Enter a six-bit DSCP code point value.
SUNRPC	
Enable SUNRPC	Select the check box to enable SUNRPC. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service's program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.

Table 260: Fields on the ALG Page *(Continued)*

Field	Description
Maximum Group Usage (%)	Select the maximum group usage % from 10 to 100%.
Map Entry Timeout	Select the map entry timeout session from 5 to 4320 minutes.

CHAPTER 81

Advanced Threat Prevention

IN THIS CHAPTER

About the Advanced Threat Prevention Page

IN THIS SECTION

You are here: **Security Services** > **Advanced Threat Prevention**.

You can view and configure threat prevention policies. Threat prevention policies provide protection and monitoring for configured threat profiles, including command and control server, infected hosts, and malware. Using threat intelligence feeds in policies, ingress and egress traffic is monitored for suspicious content and behavior.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a threat prevention policy. See "Add a Threat Prevention Policy" on page 942.
- Edit a threat prevention policy. See "Edit a Threat Prevention Policy" on page 944.

- Delete a threat prevention policy. See "Delete Threat Prevention Policy" on page 944.
- Filter the threat prevention policies based on select criteria. To do this, select the filter icon at the top right-hand corner of the Threat Prevention Policies table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the Threat Prevention Policies table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advance search for threat prevention policies. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 261 on page 941 describes the fields on the Threat Prevention Policies page.

Table 261: Fields on the Threat Prevention Policies Page

Field	Description
Name	Enter a threat prevention policy name. Name must begin with an alphanumeric character; dashes and underscores are allowed; cannot exceed 63 characters.

Table 261: Fields on the Threat Prevention Policies Page *(Continued)*

Field	Description
C&C Server	Displays the range value of threat score set for this policy on a C&C server. A C&C profile would provide information on C&C servers that have attempted to contact and compromise hosts on your network. If the threat score of a feed is between this range, the feed will be blocked or permitted based on the threat score.
Infected Host	Displays the range value of threat score set for this policy if . An infected host profile would provide information on compromised hosts and their associated threat levels.
Malware HTTP	A malware profile would provide information on files downloaded by hosts and found to be suspicious based on known signatures or URLs.
Malware SMTP	A malware profile would provide information on files downloaded by hosts and found to be suspicious based on known signatures or URLs.
Log	All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged.
Description	Enter a description for the threat prevention policy.

RELATED DOCUMENTATION

- Add a Threat Prevention Policy | 942
- Edit a Threat Prevention Policy | 944
- Delete Threat Prevention Policy | 944

Add a Threat Prevention Policy

You are here: **Security Services** > **Advanced Threat Prevention**.

To add a threat prevention policy:

1. Click the add icon (**+**) on the upper right side of the Threat Prevention Policy page.

   The Create Threat Prevention Policy page appears.

2. Complete the configuration according to the guidelines provided in Table 262 on page 943.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 262: Fields on the Create Threat Prevention Policy Page

Field	Action
Name	Displays the threat prevention policy name.
Description	Displays the threat prevention policy description.
Profiles	
Include C&C profile in policy	Select the check box.
Include infected host profile in policy	Select the check box.
Include malware profile in policy	Select the check box.
Log Setting	
Log Setting	Select an option from the list. The available options are: • Log all traffic • Log only blocked traffic • Do not log any traffic

RELATED DOCUMENTATION

About the Advanced Threat Prevention Page | 940

Edit a Threat Prevention Policy | 944

Delete Threat Prevention Policy | 944

Edit a Threat Prevention Policy

You are here: **Security Services** > **Advanced Threat Prevention**.

To edit a threat prevention policy:

1. Select the existing a threat prevention that you want to edit on the Threat Prevention Policies page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit a Threat Prevention page appears with editable fields. For more information on the options, see "Add a Threat Prevention Policy" on page 942.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Advanced Threat Prevention Page | **940**
- Add a Threat Prevention Policy | **942**
- Delete Threat Prevention Policy | **944**

Delete Threat Prevention Policy

You are here: **Security Services** > **Advanced Threat Prevention**.

To delete a threat prevention policy:

1. Select a threat prevention policy that you want to delete on the Threat Prevention Policies page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Advanced Threat Prevention Page | **940**
- Add a Threat Prevention Policy | **942**
- Edit a Threat Prevention Policy | **944**

CHAPTER 82

SSL Initiation Profiles

IN THIS CHAPTER

About the SSL Initiation Profile Page

IN THIS SECTION

You are here: **Security Services** > **SSL Profiles** > **SSL Initiation**.

You can configure SSL Initiation profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an SSL initiation profile. See "Add an SSL Initiation Profile" on page 947.
- Edit an SSL initiation profile. See "Edit an SSL Initiation Profile" on page 950.
- Delete SSL initiation profile. See "Delete SSL Initiation Profile" on page 951.

- Show or hide columns in the SSL Initiation Profile table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advance search for SSL initiation profile. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 263 on page 946 describes the fields on the SSL Initiation Profile page.

Table 263: Fields on the SSL Initiation Profile Page

Field	Description
Name	Displays the name of the SSL initiation profile.
Flow Tracing	Displays whether flow trace is enabled or disabled for troubleshooting policy-related issues.
Protocol Version	Displays the accepted protocol SSL version.

Table 263: Fields on the SSL Initiation Profile Page *(Continued)*

Field	Description
Preferred Cipher	Displays the preferred cipher which the SSH server uses to perform encryption and decryption function.
Session Cache	Displays whether SSL session cache is enabled or not.
Server Authentication Failure	Displays the action that will be performed if errors are encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).
Certificate Revocation	Displays the criterion for certificate revocation for the SSL initiation profile.

RELATED DOCUMENTATION

Add an SSL Initiation Profile | 947
Edit an SSL Initiation Profile | 950
Delete SSL Initiation Profile | 951

Add an SSL Initiation Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Initiation**.

To add an SSL initiation profile:

1. Click the add icon (**+**) on the upper right side of the SSL Initiation Profile page.
   The Create SSL Initiation Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 264 on page 948.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 264: Fields on the Create SSL Initiation Profile Page

Field	Action
General Information	
Name	Enter a unique name of the SSL initiation profile. The string must consist of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Flow Tracing	Select this option to enable flow trace for troubleshooting policy-related issues for this profile.
Protocol Version	Specifies the accepted protocol SSL version. Select the protocol from the list: None, All, TSLv1, TSLv1.1, or TSLv1.2.
Preferred Cipher	Specify the cipher depending on their key strength. Select a preferred cipher from the list: • Custom—Configure custom cipher suite and order of preference. • Medium—Use ciphers with key strength of 128 bits or greater. • Strong—Use ciphers with key strength of 168 bits or greater. • Weak—Use ciphers with key strength of 40 bits or greater.
Custom Ciphers	Select one or more Ciphers from the list. Click **Clear All** to clear the selected ciphers from the list.
Session Cache	Select this option to enable SSL session cache.
Certificate	

Table 264: Fields on the Create SSL Initiation Profile Page *(Continued)*

Field	Action
Trusted CA	Select the trusted certificate authority profile from the list. Specify the set of ciphers the SSH server can use to perform encryption and decryption functions. If this option is not configured, the server accepts any supported suite that is available.
Client Certificate	Specify a client certificate that is required to effectively authenticate the client. Select the appropriate client certificate from the list. • None • SSLRP_Automation_Cert_2 • SSLFP_Automation_Cert_1 • SSLRP_Automation_Cert_1 • SSLFP_Automation_Cert_2 • SSL2
Actions	
Server Authentication Failure	Select this option to ignore server authentication completely. In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry). We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.

Table 264: Fields on the Create SSL Initiation Profile Page *(Continued)*

Field	Action
CRL Validation	Enable this option to disable CRL validation.
Action	Select an action from the list if CRL info is not present: • None • Allow • Drop
Hold Instruction Code	Select Ignore if you want to keep the instruction code on hold for this profile.

RELATED DOCUMENTATION

About the SSL Initiation Profile Page | **945**

Edit an SSL Initiation Profile | **950**

Delete SSL Initiation Profile | **951**

Edit an SSL Initiation Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Initiation**.

To edit an SSL initiation profile:

1. Select the existing SSL initiation profile that you want to edit on the SSL Initiation Profile page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit an SSL Initiation Profile page appears with editable fields. For more information on the options, see "Add an SSL Initiation Profile" on page 947.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the SSL Initiation Profile Page | 945
- Add an SSL Initiation Profile | 947
- Delete SSL Initiation Profile | 951

Delete SSL Initiation Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Initiation**.

To delete an SSL initiation profile:

1. Select an SSL initiation profile that you want to delete on the SSL Initiation Profile page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the SSL Initiation Profile Page | 945
- Add an SSL Initiation Profile | 947
- Edit an SSL Initiation Profile | 950

CHAPTER 83

SSL Proxy Profiles

IN THIS CHAPTER

About the SSL Proxy Page

IN THIS SECTION

You are here: **Security Services** > **SSL Profiles** > **SSL Proxy**.

You can create, add, edit, and delete SSL proxy or global policy configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure global policy. To do this, click **Global Config** at the upper right of the table and enter the session cache timeout in seconds.
- Add an SSL proxy profile. See "Add an SSL Proxy Profile" on page 955.
- Edit na SSL proxy profile. See "Edit an SSL Proxy Profile" on page 962.

- Delete SSL proxy profile. See "Delete SSL Proxy Profile" on page 962.
- Clone an SSL proxy profile. See "Clone an SSL Proxy Profile" on page 961.
- View the details of an SSL proxy profile—To do this, select the SSL proxy profile for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected SSL proxy profile and select **Detailed View**.
  - Mouse over to the left of the selected SSL proxy profile and click **Detailed View**.
- Deselect the selected SSL proxy profiles. To do this, click **More** and select **Clear All Selections**.
- Show or hide columns in the SSL Proxy Profiles table. To do this, click the Show Hide Columns icon in the top right corner of the custom objects table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for SSL proxy profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 265 on page 954 describes the fields on the SSL Proxy page.

Table 265: Fields on the SSL Proxy Page

Field	Description
Name	Displays the name of the SSL Proxy profile.
Protection Type	Displays the type of protection the profile provides. One is client protection and the other one is server protection. Client protection is for SSL forward proxy and server protection is for reverse proxy.
Preferred Cipher	Displays the category of the profile depending on their key strength.
Custom Cipher	Displays the custom cipher which the SSH server uses to perform encryption and decryption function.
Flow Tracing	Displays whether flow trace is enabled or disabled for troubleshooting policy-related issues.
Exempted Addresses	Displays the addresses to whitelists that bypass SSL forward proxy processing.
Server Auth Failure	Displays the action that will be performed if errors are encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).
Session Resumption	Displays whether the session resumption is disabled or not.
Interface	Displays the name of the interface associated with the VLAN.
MAC Address	Displays the MAC address associated with the VLAN.

RELATED DOCUMENTATION

Add an SSL Proxy Profile | 955

Add an SSL Proxy Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Proxy**.

To add an SSL proxy profile:

1. Click the add icon (**+**) on the upper right side of the SSL Proxy Profile page.
   The Create SSL Proxy Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 266 on page 955.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 266: Fields on the Create SSL Proxy Profile Page

Field	Action
General Information	
Name	Enter a name of the SSL proxy profile. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Preferred Cipher	Specifies the cipher depending on their key strength. Select a preferred cipher from the list: • Medium—Use ciphers with key strength of 128 bits or greater. • Strong—Use ciphers with key strength of 168 bits or greater. • Weak—Use ciphers with key strength of 40 bits or greater. • Custom—Configure custom cipher suite and order of preference.

Table 266: Fields on the Create SSL Proxy Profile Page *(Continued)*

Field	Action
Custom Ciphers	Specifies the set of ciphers the SSH server can use to perform encryption and decryption functions. If this option is not configured, the server accepts any supported suite that is available. Select the set of ciphers from the list: 1. rsa-with-RC4-128-md5—RSA, 128-bit RC4, MD5 hash 2. rsa-with-RC4-128-sha—RSA, 128-bit RC4, SHA hash 3. rsa-with-des-cbc-sha—RSA, DES/CBC, SHA hash 4. rsa-with-3DES-ede-cbc-sha—RSA, 3DES EDE/CBC, SHA hash 5. rsa-with-aes-128-cbc-sha—RSA, 128-bit AES/CBC, SHA hash 6. rsa-with-aes-256-cbc-sha—RSA, 256-bit AES/CBC, SHA hash 7. rsa-export-with-rc4-40-md5—RSA-export, 40-bit RC4, MD5 hash 8. rsa-export-with-des40-cbc-sha—RSA-export, 40-bit DES/CBC, SHA hash 9. rsa-with-aes-256-gcm-sha384—RSA, 256-bit AES/GCM, SHA384 hash 10. rsa-with-aes-256-cbc-sha256—RSA, 256-bit AES/CBC, SHA256 hash 11. rsa-with-aes-128-gcm-sha256—RSA, 128-bit AES/GCM, SHA256 hash 12. rsa-with-aes-128-cbc-sha256—RSA, 256-bit AES/CBC, SHA256 hash 13. ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE, RSA, 256-bit AES/GCM, SHA384 hash

Table 266: Fields on the Create SSL Proxy Profile Page *(Continued)*

Field	Action
	14. ecdhe-rsa-with-aes-256-cbc-sha—ECDHE, RSA, 256-bit AES/CBC, SHA hash **15.** ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE, RSA, 256-bit AES/CBC, SHA384 hash **16.** ecdhe-rsa-with-aes-3des-ede-cbc-sha—ECDHE, RSA, 3DES, EDE/CBC, SHA hash **17.** ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE, RSA, 128-bit AES/GCM, SHA256 hash **18.** ecdhe-rsa-with-aes-128-cbc-sha—ECDHE, RSA, 128-bit AES/CBC, SHA hash **19.** ecdhe-rsa-with-aes-128-cbc-sha256—ECDHE, RSA, 128-bit AES/CBC, SHA256 hash
Flow Trace	Select the check box to enable flow trace for troubleshooting policy-related issues. Else leave it blank.
Certificate Type	Specifies whether the certificate that you want to associate with this profile is a root CA or server certificate. Server certificate is used for SSL reverse proxy. If you choose server certificate, the trusted CA, CRL, and server auth failure options will not be available. For forward proxy profile, choose the root CA In a public key infrastructure (PKI) hierarchy, the root CA is at the top of the trust path. The root CA identifies the server certificate as a trusted certificate.
Certificate	Select the certificate that you want to associate with this SSL proxy profile from the list. Specifies the certificate that you created in the Administration > Certificate Management page of J-Web. In a public key infrastructure (PKI) hierarchy, the CA is at the top of the trust path. The CA identifies the server certificate as a trusted certificate.

Table 266: Fields on the Create SSL Proxy Profile Page *(Continued)*

Field	Action
Trusted Certificate Authorities	Select the trusted CA that are available on the device from the following options: All, None, Select specific. If you choose Select specific, you need to select the Certificate Authorities from the Available column and move it to the Selected column.
Exempted Addresses	Specifies addresses to create whitelists that bypass SSL forward proxy processing. Select the addresses from the from the Available column and move it to the Selected column. Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass SSL proxy processing for some sessions. Such sessions mostly include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under whitelists.
Exempted URL Categories	Specifies URL categories to create whitelists that bypass SSL forward proxy processing. Select URL categories from the from the Available column and move it to the Selected column. These URL categories are exempted during SSL inspection. Only the predefined URL categories can be selected for the exemption.
Actions	

Table 266: Fields on the Create SSL Proxy Profile Page *(Continued)*

Field	Action
Server Auth Failure	Select the check box to ignore server authentication completely. In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry). We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.
Session Resumption	Select the check box if you do not want session resumption. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a session caching mechanism so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and server.
Logging	Select an option from the list to generate logs. You can choose to log All events, Warning, Info, Errors, or different sessions (whitelisted, Allowed, Dropped, or Ignored).

Table 266: Fields on the Create SSL Proxy Profile Page *(Continued)*

Field	Action
Renegotiation	After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. SSL forward proxy supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) renegotiation. You can specify whether to Allow nonsecure renegotiation, Allow-secure renegotiation, or Drop renegotiation. When session resumption is enabled, session renegotiation is useful in the following situations: • Cipher keys need to be refreshed after a prolonged SSL session. • Stronger ciphers need to be applied for a more secure connection. Select if a change in SSL parameters requires renegotiation. The options are: None (selected by default), Allow, Allow-secure, and Drop.
Certificate Revocation	Select the check box if you want to revoke the certificate.
If CRL info not present	Specifies if you want to allow or drop if CRL info is not present. Select the following actions from the list if CRL info is not present : Allow session, Drop session, or None.
Hold Instruction Code	Select Ignore if you want to keep the instruction code on hold.
Mirror Decrypt Traffic	

Table 266: Fields on the Create SSL Proxy Profile Page *(Continued)*

Field	Action
Interface	Select an SSL decryption port mirroring interface from the list. This is an Ethernet interface on SRX Series device through which the copy of the SSL decrypted traffic is forwarded to a mirror port.
Only after Security Policies Enforcement	Select the check box to enable forwarding the copy of the decrypted traffic to the external mirror traffic collector after enforcing the Layer 7 security services through a security policy.
MAC Address	Enter the MAC address of the external mirror traffic collector port.

RELATED DOCUMENTATION

About the SSL Proxy Page | 952

Edit an SSL Proxy Profile | 962

Delete SSL Proxy Profile | 962

Clone an SSL Proxy Profile | 961

Clone an SSL Proxy Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Proxy**.

To clone an SSL proxy profile:

1. Select an SSL Proxy profile that you want to clone and select **Clone** from the More link.

   NOTE: Alternatively, you can right-click on the selected SSL Proxy profile and select **Clone**.

   The Clone SSL Proxy Profile page appears with editable fields. For more information on the options, see "Add an SSL Proxy Profile" on page 955.

2. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

- About the SSL Proxy Page | **952**
- Edit an SSL Proxy Profile | **962**
- Delete SSL Proxy Profile | **962**

Edit an SSL Proxy Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Proxy**.

To edit an SSL proxy profile:

1. Select the existing SSL proxy profile that you want to edit on the SSL Proxy Profile page.
2. Click the pencil icon available on the upper right side of the page.

   The Update SSL Initiation Profile page appears with editable fields. For more information on the options, see "Add an SSL Proxy Profile" on page 955.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the SSL Proxy Page | **952**
- Delete SSL Proxy Profile | **962**
- Clone an SSL Proxy Profile | **961**

Delete SSL Proxy Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Proxy**.

To delete SSL proxy profile:

1. Select one or more SSL proxy profiles that you want to delete on the SSL Proxy page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the SSL Proxy Page | **952**
- Add an SSL Proxy Profile | **955**
- Edit an SSL Proxy Profile | **962**
- Clone an SSL Proxy Profile | **961**

CHAPTER 84

Firewall Authentication—Access Profile

IN THIS CHAPTER

About the Access Profile Page

IN THIS SECTION

You are here: **Security Services** > **Firewall Authentication** > **Access Profile**.

Use this page to configure Access Profile. Access profiles enable you to define the authentication and accounting servers and their priorities.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an access profile. See "Add an Access Profile" on page 966.
- Edit an access profile. See "Edit an Access Profile" on page 971.
- Delete an access profile. See "Delete an Access Profile" on page 972.

- View the details of the Access profile—To do this, select the Access profile for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected Access profile and select **Detailed View**.
  - Mouse over to the left of the selected Access profiles and click **Detailed View**.
- Show or hide columns in the Access Profile table. To do this, click Show Hide Columns icon in the top right corner of the Access Profiles table and select the columns you want to display or deselect the columns you want to hide on the page.
- Advance search for Access profile. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 267 on page 965 describes the fields on the Access Profile page.

Table 267: Fields on the Access Profile Page

Field	Description
Profile Name	Displays the name of an access profile.

Table 267: Fields on the Access Profile Page *(Continued)*

Field	Description
Order 1	Shows the order in which Junos OS tries different authentication methods when verifying that a client can access the devices.
Order 2	Shows the next authentication method if the authentication method included in the authentication order option is not available, or if the authentication is available but returns a reject response.
Local Users	Displays the usernames that are created for accessing the application.
LDAP Servers	Displays the IP address of the LDAP authentication server.
RADIUS Servers	Displays the RADIUS server configuration.

RELATED DOCUMENTATION

Add an Access Profile | **966**

Edit an Access Profile | **971**

Delete an Access Profile | **972**

Add an Access Profile

You are here: **Security Services** > **Firewall Authentication** > **Access Profile**.

To add an access profile:

1. Click the add icon (**+**) on the upper right-side of the Access Profile page.

   The Create Access Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 268 on page 967.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 268: Fields on the Access Profile Page

Field	Description
Access Profile Name	Enter a name for the access profile. The name must be a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 64 characters.
Address Assignment	Select an address pool from the list that can be used by different client applications. Click **Create Address Pool** to add a new address pool. For more information on creating a new address pool, see "Add an Address Pool" on page 975.
Authentication	
Local	Select **Local** to configure local authentication services. To create a new local authentication user: 1. Click **+**. The Create Local Authentication User page appears. 2. Enter the following details: • **Username**—Enter the user name of the user requesting access. • **Password**—Enter the user password. • **XAUTH IP Address**—Enter the IPv4 address for the client. • **Group**—Enter the group name to store several user accounts together. 3. Click **OK** to save changes. To edit, select the local authentication user configuration and click the pencil icon. To delete, select the local authentication user configuration and click the delete icon.

Table 268: Fields on the Access Profile Page *(Continued)*

Field	Description
RADIUS	Select **RADIUS** to configure RADIUS authentication services. To create a new RADIUS server: **1.** Click **+**. The Create RADIUS Server page appears. **2.** Enter the following details: • **Address**—Enter the IPv4 or IPv6 address of the RADIUS server. • **Secret**—Enter the secret password to access the RADIUS server. • **Port**—Enter the port number on which to contact the RADIUS server. Range is 1 through 65535. Default is 1812. • **Retry**—Enter the number of retries that a device can attempt to contact a RADIUS server. Range is 1 through 100 seconds. • **Routing Instance**—Select the routing instance from the list for managing the routing instance. • **Source Address**—Enter a source IP address configured on one of the device's interfaces. • **Timeout**—Enter the amount of time that the local device waits to receive a response from a RADIUS authentication server. Range is 1 through 1000 seconds. **3.** Click **OK** to save changes. To edit, select the RADIUS server configuration and click the pencil icon. To delete, select the RADIUS server configuration and click the delete icon.

Table 268: Fields on the Access Profile Page *(Continued)*

Field	Description
LDAP	Select **LDAP** to configure LDAP authentication services. To create a new LDAP server: **1.** Click **+**. The Create LDAP Server page appears. **2.** Enter the following details: • **Address**—Enter the IPv4 or IPv6 address of the LDAP server. • **Port**—Enter the port number on which to contact the LDAP server. Range is 1 through 65535. Default is 389. • **Retry**—Enter the number of retries that a device can attempt to contact an LDAP server. Range is 1 through 10 seconds. • **Routing Instance**—Select the routing instance from the list for managing the routing instance. • **Source Address**—Enter a source IP address configured on one of the device's interfaces. • **Timeout**—Enter the amount of time that the local device waits to receive a response from an LDAP authentication server. Range is 3 through 90. **3.** Click **OK** to save changes. To edit, select the LDAP server configuration and click the pencil icon. To delete, select the LDAP server configuration and click the delete icon.
LDAP Options	
Base Distinguished Name	Enter the base distinguished name that defines user's basic properties. For example, in the base distinguished name o=juniper, c=us, where c stands for country, and o for organization.

Table 268: Fields on the Access Profile Page *(Continued)*

Field	Description
Revert Interval	Specifies the amount of time that elapses before the primary server is contacted if a backup server is being used. Use top/bottom arrows to provide the revert interval. Range is 60 through 4294967295.
LDAP Option Type	Select an LDAP option from the list: • **None**—No user LDAP distinguished name (DN). • **Assemble**—Indicates that a user's LDAP DN is assembled through the use of a common name identifier, the username, and base distinguished name. • **Search**—Indicates that a search is used to get a user's LDAP DN. The search is performed based on the search filter and the search text typed in by the user during authentication.
Common Name	Enter a common name identifier used as a prefix for the username during the assembly of the users distinguished name. This option is available when you select **Assemble** LDAP option type.
Search Filter	Enter the name of the filter to find the users LDAP distinguished name. This option is available when you select **Search** LDAP option type.
Admin Search	Enable this option to perform an LDAP administrator search. By default, the search is an anonymous search. This option is available when you select **Search** LDAP option type.
Distinguished Name	Enter the distinguished name of an administrative user. The distinguished name is used in the bind for performing the LDAP search. This option is available when you select **Admin Search** is enabled.
Secret	Enter the plain-text password for the administrative user. This option is available when you select **Admin Search** is enabled.

Table 268: Fields on the Access Profile Page *(Continued)*

Field	Description
Authentication Order	
Order 1	Select one or more of the following authentication methods: • **NONE**—No authentication for the specified user. • **Local**—Use local authentication services. • **LDAP**—Use LDAP. The SRX Series Firewall uses this protocol to get user and group information necessary to implement the integrated user firewall feature. • **Radius**—Use RADIUS authentication services. If RADIUS servers fail to respond or return a reject response, try local authentication, because it is explicitly configured in the authentication order.
Order 2	Select the authentication method from the list.

RELATED DOCUMENTATION

About the Access Profile Page | 964
Edit an Access Profile | 971
Delete an Access Profile | 972

Edit an Access Profile

You are here: **Security Services** > **Firewall Authentication** > **Access Profile**.

To edit an access profile:

1. Select an existing access profile that you want to edit on the Access Profile page.
2. Click the pencil icon available on the upper right-side of the page.

   The Edit Access Profiles page appears with editable fields. For more information on editing the fields, see "Add an Access Profile" on page 966.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

About the Access Profile Page | 964
Add an Access Profile | 966
Delete an Access Profile | 972

Delete an Access Profile

You are here: **Security Services** > **Firewall Authentication** > **Access Profile**.

To delete an access profile:

1. Select an access profile that you want to delete on the Access Profiles page.
2. Click the delete icon available on the upper right-side of the page.
3. Click **Yes** to delete access profiles or click **No** to retain access profiles.

RELATED DOCUMENTATION

About the Access Profile Page | 964
Add an Access Profile | 966
Edit an Access Profile | 971

CHAPTER 85

Firewall Authentication—Address Pools

IN THIS CHAPTER

About the Address Pools Page

IN THIS SECTION

You are here: **Security Services** > **Firewall Authentication** > **Address Pools**.

Use this page to get configure Address Pools.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add Address Pool. See "Add an Address Pool" on page 975.
- Edit Address Pool. See "Edit an Address Pool" on page 976.
- Delete Address Pool. See "Delete Address Pool" on page 977.

- Search for Text in an Address Pools table. See "Search for Text in an Address Pools Table" on page 977.
- View the details of an address pool—To do this, select the address pool for which you want to view the details and follow the available options:
  - Click **More** and select **Detailed View**.
  - Right-click on the selected address pool and select **Detailed View**.
  - Mouse over to the left of the selected address pool and click **Action_Detail_View**.
- Filter the address pool based on select criteria. To do this, select the filter icon at the top right-hand corner of the address pool table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the address pool table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

Field Descriptions

Table 269 on page 974 describes the fields on the Address Pools page.

Table 269: Fields on the Address Pools Page

Field	Description
Name	Specifies the name of the address pool.
Network Address	Specifies the network address used by the address pool.
Primary DNS	Specifies the primary-dns IP address.
Secondary DNS	Specifies the secondary-dns IP address.
Primary WINS	Specifies the primary-wins IP address.
Secondary WINS	Specifies the secondary-wins IP address.

Table 269: Fields on the Address Pools Page *(Continued)*

Field	Description
Address Range	Specifies the name of the address range.

RELATED DOCUMENTATION

- Add an Address Pool | **975**
- Edit an Address Pool | **976**
- Delete Address Pool | **977**
- Search for Text in an Address Pools Table | **977**

Add an Address Pool

You are here: **Security Services** > **Firewall Authentication** > **Address Pools**.

To add an address pool:

1. Click the add icon (**+**) on the upper right side of the Address Pools page.
   The Create Address Pool page appears.
2. Complete the configuration according to the guidelines provided in Table 270 on page 975.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 270: Fields on the Create Address Pool Page

Field	Description
General	
Pool Name	Enter the address pool name.
Network Address	Enter an IPv4 address for the address pool.
XAUTH Attributes	

Table 270: Fields on the Create Address Pool Page *(Continued)*

Field	Description
Primary DNS Server	Enter the primary-dns IPv4 address.
Secondary DNS Server	Enter the secondary-dns IPv4 address.
Primary WINS Server	Enter the primary-wins IPv4 address.
Secondary WINS Server	Enter the secondary-wins IPv4 address.
Address Ranges	
Add	Click **+** to add a new address range for the address pool.
Name	Enter a name for the IP address range.
Lower Limit	Enter the lower limit of the address range.
High Limit	Enter the upper limit of the address range.
Delete	Click the delete icon to delete the address range for the address pool.

RELATED DOCUMENTATION

- About the Address Pools Page | **973**
- Edit an Address Pool | **976**
- Delete Address Pool | **977**
- Search for Text in an Address Pools Table | **977**

Edit an Address Pool

You are here: **Security Services** > **Firewall Authentication** > **Address Pools**.

To edit an address pool:

1. Select an existing address pool that you want to edit on the Address Pools page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit Address Pool page appears with editable fields. For more information on the options, see "Add an Address Pool" on page 975.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Address Pools Page | 973

Add an Address Pool | 975

Delete Address Pool | 977

Search for Text in an Address Pools Table | 977

Delete Address Pool

You are here: **Security Services** > **Firewall Authentication** > **Address Pools**.

To delete an address pool:

1. Select an address pool that you want to delete on the Address Pools page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Address Pools Page | 973

Add an Address Pool | 975

Edit an Address Pool | 976

Search for Text in an Address Pools Table | 977

Search for Text in an Address Pools Table

You are here: **Security Services** > **Firewall Authentication** > **Address Pools**.

You can use the search icon in the top right corner of the Address Pools page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.

   The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

- About the Address Pools Page | **973**
- Add an Address Pool | **975**
- Edit an Address Pool | **976**
- Delete Address Pool | **977**

CHAPTER 86

Firewall Authentication Settings

IN THIS CHAPTER

About the Authentication Settings Page

IN THIS SECTION

You are here: **Security Services** > **Firewall Authentication** > **Authentication Settings**.

Use this page to configure firewall authentication. You can click the arrow pointing outwards icon to expand all the options or click the arrow pointing inwards to collapse or hide all the options.

To edit this page, configure minimum one access profile under **Security Services** > **Firewall Authentication** > **Access Profile**.

Field Description

To configure a firewall authentication:

1. Complete the configuration according to the guidelines provided in Table 271 on page 980.
2. Click **Save** to save the changes.

Table 271 on page 980 describes the fields on the Firewall Authentication page.

Table 271: Fields on the Firewall Authentication Page

Field	Description
Pass-through Settings	
Default Profile	Select a profile from the list that the policies use to authenticate users.
FTP Banners	
Login	Displays the login prompt for users logging in using FTP. Maximum characters are 250.
Success	Displays a successful login prompt for users logging in using FTP. Maximum characters are 250.
Fail	Displays failed login prompt for users logging in using FTP. Maximum characters are 250.
Telnet Banners	
Login	Displays the login prompt for users logging in using telnet. Maximum characters are 250.
Success	Displays a successful login prompt for users logging in using telnet. Maximum characters are 250.
Fail	Displays failed login prompt for users logging in using telnet. Maximum characters are 250.
HTTP Banner	
Login	Displays the login prompt for users logging in using HTTP.

Table 271: Fields on the Firewall Authentication Page *(Continued)*

Field	Description
Success	Displays a successful login prompt for users logging in using HTTP.
Fail	Displays failed login prompt for users logging in using HTTP.
Web-auth-settings	
Default Profile	Select a profile that the policies use to authenticate users.
Success	Displays a successful login prompt for users logging in using Web authentication banner.
Logo Image Upload	
Logo File	Indicates an image to be chosen for the Web authentication logo. **NOTE**: For the good logo image, the image format must be in .gif and the resolution must be 172x65.
Browse	Click the button to navigate to the logo image on the user's local disk.
Sync	Click the button to sync the logo image.
Restore	Click the button to restore the Web authentication logo.

RELATED DOCUMENTATION

About the UAC Settings Page | **982**

CHAPTER 87

Firewall Authentication—UAC Settings

IN THIS CHAPTER

About the UAC Settings Page

IN THIS SECTION

You are here: **Security Services** > **Firewall Authentication** > **UAC Settings**.

Use this page to configure UAC Settings.

Field Description

To configure UAC settings:

1. Complete the configuration according to the guidelines provided in Table 272 on page 982.
2. Click **Save** to save the changes.

Table 272 on page 982 describes the fields on the UAC Setting page.

Table 272: Fields on the UAC Setting Page

Field	Description
Global Settings	

Table 272: Fields on the UAC Setting Page *(Continued)*

Field	Description
Certificate Verification	Determines whether server certificate verification is required when initiating a connection between a device and an Access Control Service in a UAC configuration. Select the following options from the list: • **None**—Certificate verification is not required. • **Optional**—Certificate verification is not required. If the CA certificate is not specified in the ca-profile option, the commit check passes and no warning is issued. • **Required**—Certificate verification is required. If the CA certificate is not specified in the ca-profile option, an error message is displayed, and the commit check fails. Use this option to ensure strict security. • **Warning**—Certificate verification is not required. A warning message is displayed during commit check if the CA certificate is not specified in the ca-profile option.
Interval	Specifies the value in seconds that the device should expect to receive a heartbeat signal from the IC Series device. Enter the heartbeat interval in seconds. Range: 1 through 9999.
Test Only Mode	Allows all traffic and log enforcement result. Enable the Test Only Mode option.
Timeout	Specifies (in seconds) that the device should wait to get a heartbeat response from an IC Series UAC Appliance. Enter the timeout in seconds. Range: 2 through 10000.
Timeout Action	Specifies the action to be performed when a timeout occurs and the device cannot connect to an Infranet Enforcer. Select the timeout action from the list.
Infranet Controller	

Table 272: Fields on the UAC Setting Page *(Continued)*

Field	Description
Infranet Controller	Click **+** to add an infranet controller. Click pencil icon to edit a selected infranet controller. Click delete icon to delete the selected infranet controller.
Name	Enter a name for the Infranet Controller.
IP address	Enter an IP address for the Infranet Controller.
Interface	Select an interface used for the Infranet Controller.
Interface	Enter the password to use for the Infranet Controller
CA Profiles	Select a CA from the list in the **CA Profiles** column and then click the right arrow to move them to the **Selected** column. **NOTE**: To deselect a CA, select the CA in the **Selected** column and then click the left arrow to move them to the **CA Profiles** column.
Port	Specifies the port number to be associated with this Infranet Controller for data traffic. Enter a value from 1 through 65,535.
Server Certificate Subject	Enter the server certificate subject name of the Infranet Controller certificate to match.
Captive Portal	
Captive Portal	Specifies the preconfigured security policy for captive portal on the Junos OS Enforcer. Click **+** to add a captive portal. Click pencil icon to edit a selected captive portal. Click delete icon to delete the selected captive portal.

Table 272: Fields on the UAC Setting Page *(Continued)*

Field	Description
Name	Enter a name for the captive portal.
Redirect Traffic	Select a traffic type to be redirected.
Redirect URL	Enter the URL to which the captive portal should be directed.

RELATED DOCUMENTATION

About the Application Tracking Page | **790**

CHAPTER 88

Firewall Authentication—Active Directory

IN THIS CHAPTER

About the Active Directory Page

You are here: **Security Services** > **Firewall Authentication** > **Active Directory**.

You can configure Active directory.

Table 273 on page 986 describes the fields on the Active Directory page.

Table 273: Fields on the Active Directory Page

Field	Description
General Information	
General	
No on Demand Probe	Enable the manual on-demand probing of a domain PC as an alternate method for the SRX Series device to retrieve address-to-user mapping information.
Timeout	

Table 273: Fields on the Active Directory Page *(Continued)*

Field	Description
Authentication Entry Timeout	Set the timeout to 0 to avoid having the user's entry being removed from the authentication table after the timeout. **NOTE**: When a user is no longer active, a timer is started for that user's entry in the Active Directory authentication table. When the time is up, the user's entry is removed from the table. Entries in the table remain active as long as there are sessions associated with the entry. The default authentication entry timeout is 30 minutes. Starting in Junos OS Release 19.2R1, the default value is 60 minutes. To disable timeout, set the interval to zero. The range is 10 through 1440 minutes.
WMI Timeout	Enter the number of seconds that the domain PC has to respond to the SRX Series device's query through Windows Management Instrumentation (WMI) or Distributed Component Object Module (DCOM). If no response is received from the domain PC within the wmi-timeoutinterval, the probe fails and the system either creates an invalid authentication entry or updates the existing authentication entry as invalid. If an authentication table entry already exists for the probed IP address, and no response is received from the domain PC within the wmi-timeout interval, the probe fails and that entry is deleted from the table. The range is 3 through 120 seconds.
Invalid Authentication Entry Timeout	Enter a value. The range is 10 through 1440 minutes. When a user is no longer active, a timer is started for that user's entry in the Active Directory authentication table. When the time is up, the user's entry is removed from the table. If this value is not configured, all the invalid auth entry from Active Directory will use the default value as 30 minutes. The range is 10 through 1440 minutes.
Firewall Authentication Forced Timeout	Enter a value. The range is 10 through 1440 minutes. This is the firewall authentication fallback time. Set the timeout to 0 to avoid having the user's entry being removed from the authentication table after the timeout.
Filter	

Table 273: Fields on the Active Directory Page *(Continued)*

Field	Description
Include	Enable to include IP addresses from the Available column. Click the Add icon (**+**) to create a new IP address and add it as either include or exclude from monitoring. Click the Delete icon to delete a new IP address and add it as either include or exclude from monitoring.
Exclude	Enable to exclude IP addresses from the Available column. Click the Add icon (**+**) to create a new IP address and add it as either include or exclude from monitoring. Click the Delete icon to delete a new IP address and add it as either include or exclude from monitoring.
Domain Settings	
Test	Click **Test** to check the Domain Connection status. test:Status page appears and displays the status.
+	Click **+** to add a domain. The Add Domain page appears. **NOTE**: • Starting in Junos OS Release 19.2R1, for SRX4200, SRX1500, SRX550M, and vSRX devices, and for the SRX5000 and SRX3000 lines of devices, you can configure the integrated user firewall in a maximum of two domains. For the other SRX Series devices, you can create only one domain. You can select the pencil icon to edit the domain or select delete icon to delete the domain.
General	
Domain Name	Enter the name of the domain. The range for the domain name is 1 through 64 characters.

Table 273: Fields on the Active Directory Page *(Continued)*

Field	Description
Username	Enter the password for the Active Directory account password. The range for the username is 1 through 64 characters. Example: admin
Password	Enter the username for the Active Directory account name. The range for the password is 1 through 128 characters. Example: A$BC123
Domain Controller(s)	
Domain Controller(s)	Click the add icon (**+**) to add domain controller settings. • Domain Controller Name—Enter the domain controller name. Name can range from 1 through 64 characters. You can configure up to maximum of 10 domain controllers. • IP Address—Enter the IP address of the domain controller.
User Group Mapping (LDAP)	
User Group Mapping (LDAP)	Click the add icon (**+**): • IP Address—Enter the IP address of the LDAP server. If no address is specified, the system uses one of the configured Active Directory domain controllers. • Port—Enter the port number of the LDAP server. If no port number is specified, the system uses port 389 for plaintext or port 636 for encrypted text. Default value is port 443.
Base Distinguish Name	Enter the LDAP base distinguished name (DN). Example: DC=example,DC=net
Username	Enter the username of the LDAP account. If no username is specified, the system will use the configured domain controller's username.

Table 273: Fields on the Active Directory Page *(Continued)*

Field	Description
Password	Enter the password for the account. If no password is specified, the system uses the configured domain controller's password.
Use SSL	Enable Secure Sockets Layer (SSL) to ensure secure transmission with the LDAP server. Disabled by default, then the password is sent in plaintext.
Authentication Algorithm	Enable this option to specify the algorithm used while the SRX Series device communicates with the LDAP server. By default, simple is selected to configure simple(plaintext) authentication mode.
IP User Mapping	
Discovery Method (WMI)	Enable the method of discovering IP address-to-user mappings. WMI—Windows Management Instrumentation (WMI) is the discovery method used to access the domain controller. This option should be enabled only for internal hosts or trusted hosts.
Event Log Scanning Interval	Enter the scanning interval at which the SRX Series device scans the event log on the domain controller. The range is 5 through 60 seconds. Default value is 60 seconds.
Initial Event Log TimeSpan	Enter the time of the earliest event log on the domain controller that the SRX Series device will initially scan. This scan applies to the initial deployment only. After WMIC and the user identification start working, the SRX Series device scans only the latest event log. The range is 1 through 168 hours. Default value is 1 hour.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.2R1	Starting in Junos OS Release 19.2R1, the default value is 60 minutes.

19.2R1	Starting in Junos OS Release 19.2R1, for SRX4200, SRX1500, SRX550M, and vSRX devices, and for the SRX5000 and SRX3000 lines of devices, you can configure the integrated user firewall in a maximum of two domains. For the other SRX Series devices, you can create only one domain.

RELATED DOCUMENTATION

About the Authentication Priority Page | 995

CHAPTER 89

Firewall Authentication—Local Authentication

IN THIS CHAPTER

About the Local Authentication Page

IN THIS SECTION

You are here: **Security Services** > **Firewall Authentication** > **Local Authentication**.

Use this page to enable or disable authentication priority configuration options.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a local auth entry. See "Add a Local Auth Entry" on page 993.
- Delete a local auth entry. See "Delete a Local Auth Entry" on page 994.
- Clear all the local auth entry. To do this, select the local auth entries you want to clear and click **Clear All** at the top right of the table.

Field Descriptions

Table 274 on page 993 describes the fields on the Local Auth page.

Table 274: Fields on the Local Auth Page

Field	Description
Filter by	Displays the local authentication configuration based on the selected filter.
IP	Displays the IP address.
Username	Displays the name of the user.
Role Name	Displays the list of roles assigned to the username.
Search	Select the filter you want and enter your inputs based on the filter type. Then, click the search icon to display the output based on your selected filter.

RELATED DOCUMENTATION

Add a Local Auth Entry | 993

Delete a Local Auth Entry | 994

Add a Local Auth Entry

You are here: **Security Services** > **Firewall Authentication** > **Local Authentication**.

To add a local auth entry:

1. Click the add icon (**+**) on the upper right side of the Local Auth page.

   The Add Local Auth Entry page appears.
2. Complete the configuration according to the guidelines provided in Table 275 on page 994.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 275: Fields on the Add Local Auth Page

Field	Action
IP Address	Enter an IP address for the local authentication.
Username	Enter a username for the local authentication.
Role List	Enter roles for the local authentication entry. Enter the role and click **+** to add a role. To delete a role, select the role and click the delete **(X)** icon. To edit a role, hover over the role name and click the pencil icon. **NOTE**: You can configure only maximum of 200 roles for a local authentication entry.

RELATED DOCUMENTATION

About the Local Authentication Page | 992
Delete a Local Auth Entry | 994

Delete a Local Auth Entry

You are here: **Security Services** > **Firewall Authentication** > **Local Authentication**.

To delete a local auth entry:

1. Select a local auth entry that you want to delete on the Local Auth Entry page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

About the Local Authentication Page | 992
Add a Local Auth Entry | 993

CHAPTER 90

Firewall Authentication—Authentication Priority

IN THIS CHAPTER

About the Authentication Priority Page

You are here: **Security Services** > **Firewall Authentication** > **Authentication Priority**.

Use this page to enable or disable authentication priority configuration options.

Table 276 on page 995 describes the fields on the Auth Priority page.

Table 276: Fields on the Auth Priority Page

Field	Description
Enable local authentication	Select the **Enable local authentication** check box to enable local authentication.
Priority	Enter a priority value (1 through 65,535) in the **Priority** field. **NOTE**: The default local authentication priority value is 100.
Enable firewall authentication	Select the check box to enable firewall authentication.
Priority	Enter a priority value (1 through 65,535) in the **Priority** field. **NOTE**: The default firewall authentication priority value is 150.
Enable unified access control	Select the check box to enable UAC authentication.

Table 276: Fields on the Auth Priority Page *(Continued)*

Field	Description
Priority	Enter a priority value (1 through 65,535) in the **Priority** field. **NOTE**: The default local authentication priority value is 200.
Enable active directory	Select the check box to enable UAC authentication.
Priority	Enter a priority value (1 through 65,535) in the **Priority** field. **NOTE**: The default local authentication priority value is 125.
OK	Click **OK** to save the configuration changes.
Reset	Click **Reset** to set the priority values and enable options to the default configuration.

RELATED DOCUMENTATION

About the Local Authentication Page | 992

CHAPTER 91

Firewall Authentication—JIMS

IN THIS CHAPTER

About the Juniper Identity Management Service Page

IN THIS SECTION

You are here: **Security Services** > **Firewall Authentication** > **JIMS**.

NOTE: Starting in Junos OS Release 21.4R1, the Identity Management menu is renamed as JIMS.

You can add, edit or delete a Juniper Identity Management Services (JIMS) profile. You can also view the connection status of this SRX Series Firewall with the JIMS.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Juniper Identity Management Service profile. See "Add a Juniper Identity Management Service Profile" on page 998.

- Edit a Juniper Identity Management Service profile. See "Edit a Juniper Identity Management Service Profile" on page 1002.
- Delete a Juniper Identity Management Service profile. See "Delete a Juniper Identity Management Service Profile" on page 1003.

RELATED DOCUMENTATION

Add a Juniper Identity Management Service Profile | 998

Add a Juniper Identity Management Service Profile

You are here: **Security Services** > **Firewall Authentication** > **JIMS**.

To add a Juniper Identity Management Service (JIMS) profile:

1. Click **Configure** on the Juniper Identity Management Service page.
   The Configure Juniper Identity Management Service Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 277 on page 998.
3. Click **Finish** to save the changes. If you want to discard your changes, click **Cancel**.

Table 277: Fields on the Configure Juniper Identity Management Service Profile Page

Field	Action
General Information	
Connection for Primary and Secondary Juniper Identity Management Service	
Connection Type	Select a connection type from the list. The options available are: HTTPS and HTTP.
Port	Enter the port number or press up or down arrow to either increment or decrement the port number. The default value is 443.
Primary IP Address	Enter a primary IP address of JIMS server.

Table 277: Fields on the Configure Juniper Identity Management Service Profile Page *(Continued)*

Field	Action
Primary CA Certificate	Specifies the primary certificate of the JIMS. SRX Series Firewall will use it to verify JIMS's certificate for SSL connection. Select Upload **CA certificate to device** or **specify the path of the file on device**.
Primary CA Certificate file upload	Enables you to locate and upload the CA certificate. Click **Browse** to locate the CA certificate on your device and click **Upload** the selected CA certificate.
Primary CA Certificate file path	Enter a file path of the primary CA certificate.
Primary Client ID	Enter a primary client ID of the SRX Series Firewall to obtain access token. It must be consistent with the configuration of the API client created on JIMS.
Primary Client Secret	Enter a password which enables you to access the primary identity management server. Specifies the client secret of the SRX Series Firewall to obtain access token. It must be consistent with the configuration of the API client created on JIMS.
Secondary Juniper Identity Management Service Server	Enables a secondary JIMS server, its IP address, CA certificate, client ID, and client secret. **NOTE**: If you enable, the Secondary IP Address, Secondary CA Certificate file upload, Secondary Client ID, Secondary Client Secret rows are displayed. Enter the IP address of the secondary server, browse and upload the secondary CA certificate, enter the secondary client ID and secret in the respective fields.

Table 277: Fields on the Configure Juniper Identity Management Service Profile Page *(Continued)*

Field	Action
Token API	Enter the token API to specify the path of the URL for acquiring access token. Default is 'oauth_token/oauth'.
Query API	Enter the path where the URL for querying user identities is located. Default is 'user_query/v2'. Click Next. The Advanced Settings page is displayed.
Advanced Settings	
Batch Query	
Item Per Batch	Specifies the maximum number of items in one batch query. Enter the number of items. Range is 100 to 1000 and the default number is 200.
Query Interval	Specifies the interval for querying the newly generated user identities. Enter the number of seconds you need between each query. The range is 1 through 60 (seconds), and the default value is 5.
IP Query	
Query Delay Time	Specifies the time delay to send individual IP query. Enter the time in seconds. The range is 0~60 (seconds). The default value is 15 seconds, which depends on the delay time of auth entry retrieved from JIMS to SRX.
No IP Query	Select the check box if you want to disable the IP query function that is enabled by default.

Table 277: Fields on the Configure Juniper Identity Management Service Profile Page *(Continued)*

Field	Action
Authentication Timeout	
Authentication Entry Timeout	Enter the value in minutes. The value range is 0 or 10~1440 (minutes). 0 means no need for a timeout. the default value is 60. Specifies the time out value for authentication entry in identity management. The timeout interval begins from when the authentication entry is added to the identity-management authentication table. If a value of 0 is specified, the entries will never expire.
Invalid Authentication Entry Timeout	Enter the value in minutes. The value range is 0 or 10~1440 (minutes). 0 means no need for a timeout. the default value is 60. Specifies the timeout value of invalid auth entry in the SRX Series authentication table for either Windows active directory or Aruba ClearPass.
Filter **NOTE**: You can select address set with maximum of 20 IP addresses and address set with wild card addresses.	
Include IP Address Book	Select an IP address book from the predefined address book in which an address set must be selected as IP filter.
Include IP Address Set	Specifies the predefined address set selected as IP filter. Select an IP address set from the list. To add a new address set for the IP address book, click **Add New Address Set**.
Exclude IP Address Book	Select an IP address book that you want identity management profile to exclude.

Table 277: Fields on the Configure Juniper Identity Management Service Profile Page *(Continued)*

Field	Action
Exclude IP Address Set	Select the predefined address set that you want identity management profile to exclude.
Filter to Domain	Enter one or more active directory domains, to the SRX Series device. You can specify up to twenty domain names for the filter.

RELATED DOCUMENTATION

- About the Juniper Identity Management Service Page | 997
- Edit a Juniper Identity Management Service Profile | 1002
- Delete a Juniper Identity Management Service Profile | 1003

Edit a Juniper Identity Management Service Profile

You are here: **Security Services** > **Firewall Authentication** > **JIMS**.

To edit a Juniper Identity Management Service (JIMS) profile:

1. Select the existing JIMS profile that you want to edit on the Juniper Identity Management Service page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit a Juniper Identity Management Service Profile page appears with editable fields. For more information on the options, see "Add a Juniper Identity Management Service Profile" on page 998.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

- About the Juniper Identity Management Service Page | 997
- Add a Juniper Identity Management Service Profile | 998
- Delete a Juniper Identity Management Service Profile | 1003

Delete a Juniper Identity Management Service Profile

You are here: **Security Services** > **Firewall Authentication** > **JIMS**.

To delete a Juniper Identity Management Service (JIMS) profile:

1. Click the delete icon available on the upper right side of the Juniper Identity Management Service page.
2. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Juniper Identity Management Service Page | **997**
- Add a Juniper Identity Management Service Profile | **998**
- Edit a Juniper Identity Management Service Profile | **1002**

CHAPTER 92

ICAP Redirect

IN THIS CHAPTER

About the ICAP Redirect Profile Page

IN THIS SECTION

You are here: **Security Services** > **ICAP Redirect**.

You can configure ICAP Redirect Profile.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an ICAP redirect profile. See "Add an ICAP Redirect Profile" on page 1006.
- Edit an ICAP redirect profile. See "Edit an ICAP Redirect Profile" on page 1009.
- Delete an ICAP redirect profile. See "Delete ICAP Redirect Profile" on page 1009.

- Filter the ICAP redirect profiles based on select criteria. To do this, select the filter icon at the top right-hand corner of the ICAP redirect profiles table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the ICAP redirect profiles table. To do this, click the Show Hide Columns icon in the top right corner of the ICAP redirect profiles table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for ICAP redirect profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

  For an advanced search:

  1. Enter the search string in the text box.

     Based on your input, a list of items from the filter context menu appears.

  2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

     NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

  3. Press Enter to display the search results in the grid.

Field Descriptions

Table 278 on page 1005 describes the fields on the ICAP Redirect Profile page.

Table 278: Fields on the ICAP Redirect Profile Page

Field	Description
Name	Displays the ICAP Service profile name.
Timeout	Displays the server response timeout in milliseconds.
Server	Displays the ICAP Redirection Server.

Table 278: Fields on the ICAP Redirect Profile Page *(Continued)*

Field	Description
Fallback Option	Specifies the request timeout action when the request is sent to the server.
HTTP Redirect	Enables redirect service on HTTP request/HTTP response.

RELATED DOCUMENTATION

- Add an ICAP Redirect Profile | **1006**
- Edit an ICAP Redirect Profile | **1009**
- Delete ICAP Redirect Profile | **1009**

Add an ICAP Redirect Profile

You are here: **Security Services** > **ICAP Redirect**.

To add an ICAP redirect profile:

1. Click the add icon (**+**) on the upper right side of the ICAP Redirect Profiles page.
   The Create ICAP Redirect Profile page appears.
2. Complete the configuration according to the guidelines provided in Table 279 on page 1006.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 279: Fields on the Create ICAP Redirect Profile Page

Field	Action
Name	Enter a unique ICAP Service profile name. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Timeout	Enter the server response timeout in milliseconds. The range is between 100 milliseconds to 50000 milliseconds.

Table 279: Fields on the Create ICAP Redirect Profile Page *(Continued)*

Field	Action
HTTP Redirect Option	
Request	Select to enable redirect service on HTTP request.
Response	Select to enable redirect service on HTTP response.
ICAP Server You can configure ICAP Redirection server by the following options: **Add**—Create an ICAP Redirect server. Enter information as specified in Table 280 on page 1007. **Edit**—Edit an ICAP Redirect server configuration. Enter information as specified in Table 280 on page 1007.	
Fallback Option	
Timeout Action	Select the timeout action from the list. The available options are: None, Permit, Log Permit, and Block.
Connectivity Action	Select the connectivity action from the list that the request cannot be sent out due to connection issues.
Default Action	Select a default action from the list to be taken when there are scenarios other than the above two mentioned ones.

Table 280: Fields on the Create ICAP Redirect Server Page

Field	Action
Name	Enter an ICAP Redirect server name. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Host Type*	Select Name or IP address.

Table 280: Fields on the Create ICAP Redirect Server Page *(Continued)*

Field	Action
Host	Enter the host name or host IP address depending on what host type you choose.
Port	Specifies the port in the server. This is the server listening post and the default port will be reached according to protocol defined. Enter the port number. The range is 1025 through 65534.
Sockets	Specifies the number of connections to be created. Enter the number of connections. The range is 1 through 64.
Authentication	
Authorization Type	Specifies the type of authentication.
Credentials Type	Select the credential type as ASCII or Base64. Based on the Credential Type that you choose, enter the ASCII string or Base64 string.
URL	
Request MOD	Enter the reqmod uri that can be configured for ICAP server only.
Response MOD	Enter the respmod uri that can be configured for ICAP server only.
Routing Instance	Specifies the virtual router that is used for launching. Select a routing instance from the list.
SSL Initiation Profile	Select an SSL initiation profile from the list.

RELATED DOCUMENTATION

About the ICAP Redirect Profile Page | **1004**

Edit an ICAP Redirect Profile

You are here: **Security Services** > **ICAP Redirect**.

To edit an ICAP redirect profile:

1. Select the existing ICAP redirect profile that you want to edit on the ICAP Redirect page.
2. Click the pencil icon available on the upper right side of the page.

   The Edit ICAP Redirect Profile page appears with editable fields. For more information on the options, see "Add an ICAP Redirect Profile" on page 1006.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

Delete ICAP Redirect Profile

You are here: **Security Services** > **ICAP Redirect**.

To delete ICAP redirect profile:

1. Select one or more ICAP redirect profile that you want to delete on the ICAP Redirect page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION