

Upgrade to Junos OS Release 19.4R3 and 20.2R3 for SRX Series

IN THIS GUIDE

- [About this Guide | 1](#)
- [Why Upgrade Junos OS to 19.4R3 and 20.2R3 | 1](#)
- [Key Features in the Upgrade | 5](#)
- [Know the Upgrade Path for Junos OS Releases | 11](#)
- [How to Upgrade to Junos OS Release 19.4R3 and 20.2R3 | 16](#)
- [Migrate to vSRX3.0 | 29](#)
- [Start Using Unified Policies Post Upgrade | 41](#)
- [Explore New Features Post Upgrade | 47](#)
- [Appendix: Resources | 52](#)

About this Guide

Use the guide to upgrade your SRX Series devices from Junos OS Release 15.1X49 to 19.4R3 (SRX Series) and to 20.2R3 (SRX380, SRX1500, and vSRX instances).

Why Upgrade Junos OS to 19.4R3 and 20.2R3

SUMMARY

Read this topic to understand what you'll gain when you upgrade Junos OS Release 15.1X49 to 19.4R3 and to 20.2R3.

IN THIS SECTION

- [Reasons for Considering an Upgrade | 2](#)

- Important Reasons for Upgrading to Junos OS Release 19.4R3 or 20.2R3 | 2
- How Can You Get Started? | 4
- Where Can You Find More Information? | 5

Reasons for Considering an Upgrade

An updated version of the OS includes new features, enhancements, and bug fixes; many customers find the value of upgrading to a new version beneficial to their organization with immediate returns. Here are the top benefits of keeping your software up to date.



Increased Efficiency

New version has enhancements that increase efficiency and provide better compatibility and integration with other devices in your network



Customer Engagement

New version allows your organization to deploy new services that will help to gain new customers or increase loyalty of existing ones



Business Growth

Latest software helps you stay current with the latest technology and respond quickly and confidently to the changing business needs



Reduced Cost

New version helps in avoiding extra cost associated with maintaining older software version that requires more support, more attention, and more workarounds



Better Security

Latest software enhances your security positioning with software upgrades that include security patches



Increased Productivity

Today we have the enhancements that dramatically improve and simplify your security deployments increasing IT operational efficiency and freeing up valuable time and resources for business innovation

jin-000037

Important Reasons for Upgrading to Junos OS Release 19.4R3 or 20.2R3

In the rapidly changing era of mobile, cloud, and the Internet of Things (IoT) technologies, the legacy operating software for network infrastructure struggles to address the networking and security challenges that are becoming commonplace

today. Keeping an outdated version of software on your devices increases risk to both your users and network environment in addition to a higher risk of a threat or cyber attack impacting your business. Outdated operating systems not only compound the problem, but their complexity and time-consuming maintenance requirements can also impact your team's operational efficiency and cost other valuable resources such as time and money. You also run the risk of incurring business loss due to noncompliance with government and other organizational regulations because of outdated OS on your devices.

We understand that you might have concerns regarding upgrading to the latest OS including:

- Network downtime and maintenance affecting business continuity
- Impacts to an existing infrastructure that is otherwise operating
- Personnel impacts including learning curves, training, and more operational cost
- Configuration compatibility

However, the benefits of upgrading to the latest supported Junos OS often outweigh the potential risks you might encounter for not upgrading. Here are a few good reasons other customers are upgrading to Junos OS Release 19.4R3 or 20.2R3.



New features that are not available in the current version



Patches for security vulnerabilities



Bug fixes from the previous versions



Current version is going to end-of-life-soon



Compatibility with updated technologies in the network



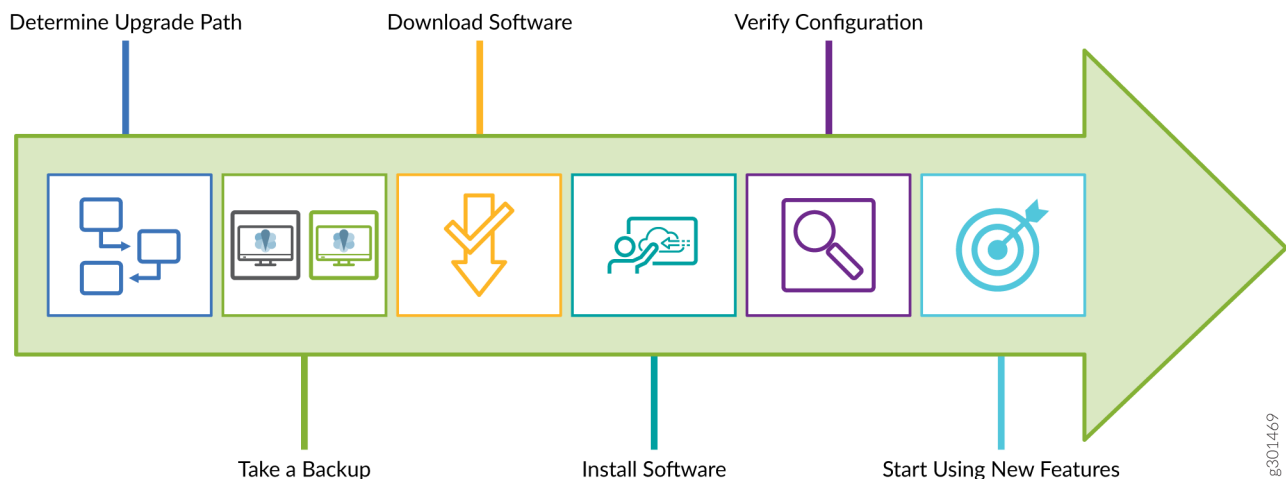
Regulatory and audit compliance requirements

How Can You Get Started?

We understand that upgrading on an infrastructure device may require a scheduled downtime as well as pre-and-post upgrade tasks, and planning and documenting to ensure a successful outcome.

If you perform the upgrade from Junos OS Release 15.1X49 to 19.4R3 on your SRX Series device and to 20.2R3 on the vSRX instance, you can complete your upgrade tasks in a few steps.

Juniper Networks is committed to making your Junos OS upgrade procedure a simple task. You can perform the upgrade as shown in the following illustration:



You can upgrade to the Junos OS Release for various use cases including advanced security, software-defined WAN (SD-WAN), and LTE backup, or to take advantage of many other new enhancements. We provide a simple upgrade path that allows you to quickly and easily upgrade your Junos OS and start using the advanced threat mitigation capabilities on your security device.

At Juniper Networks, we make Junos OS upgrade software available for free to our customers. You can find Junos OS images and related KB articles at our [Support](#) site.

To help you to get started with the Junos OS upgrades, read this guide to:

- Learn quickly about the important features introduced on SRX Series devices in newer Junos OS releases.
- Learn about the upgrade paths available to migrate from your Junos OS Release 15.1X49 to 19.4R3 (SRX Series) and to 20.2R3 (SRX380, SRX1500, and vSRX instances).
- Get step-by-step instructions on procedures and pre-and-post upgrade tasks to perform a successful upgrade.
- Know about the additional features and improvements that increase the usability of your security device.

The procedures documented in this guide will help provide a starting point for you to plan for all upgrades and migration paths.

Where Can You Find More Information?

You might also be interested to see the complete list of features in the [Feature Explorer](#). In addition to this guide, you can find detailed information on concepts, configuration, and examples in the Junos OS documentation. Want to tell us what you think about this guide?

E-mail us at:

techpubs-comments@juniper.net.

What's Next

Next, you'll learn about the key features that we've introduced in the latest Junos OS releases at "[Key Features in the Upgrade](#)" on [page 5](#).

Key Features in the Upgrade

SUMMARY

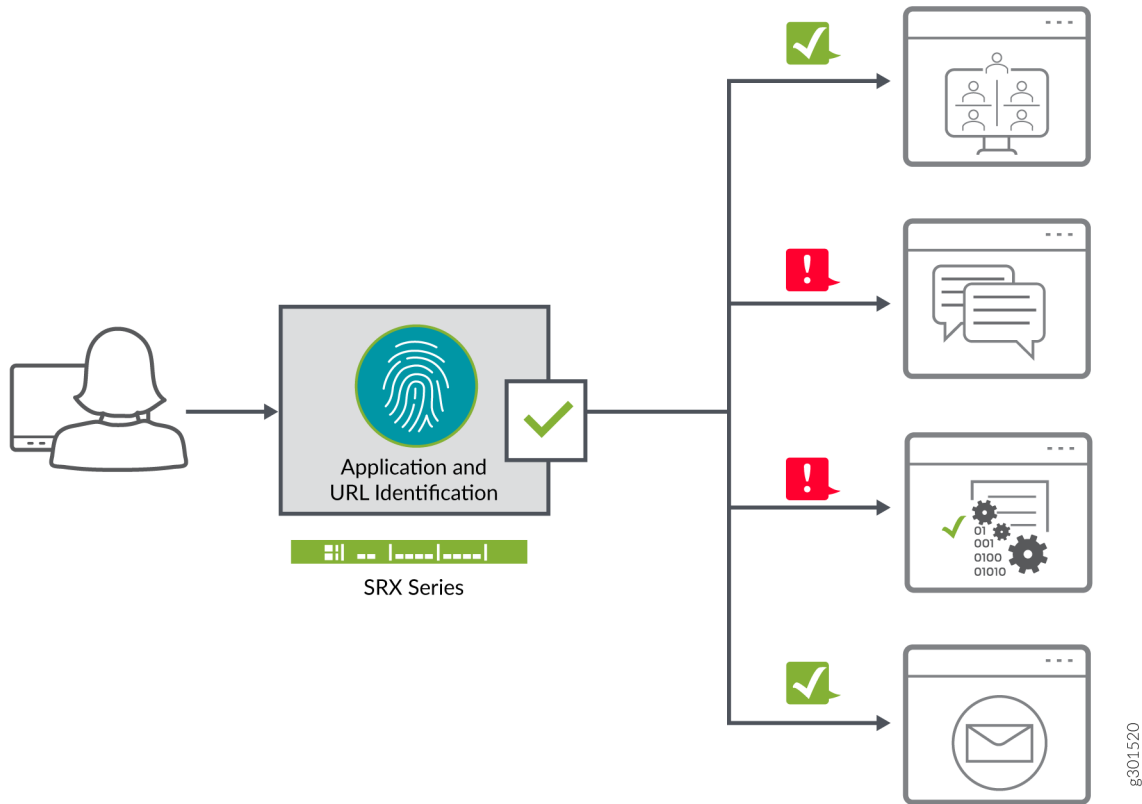
Junos OS software updates include new and enhanced features that improve your security posture, help you better mitigate risk, improve the stability of your software, and remove outdated features and security vulnerabilities. Read this topic to understand the key features in the new release.

IN THIS SECTION

- [Unified Policy | 6](#)
- [SD-WAN | 7](#)
- [Encrypted Traffic Insights | 8](#)
- [Adaptive Threat Profiling | 9](#)
- [Packet Capture for Unknown Applications | 10](#)
- [J-Web Getting Started Panel | 11](#)

We've introduced many key security features post Junos OS Release 15.1X49. These new features include abilities to provide policy-based awareness and control over applications, users, and content to stop advanced cyberthreats—all in a single device.

Unified Policy



8301520

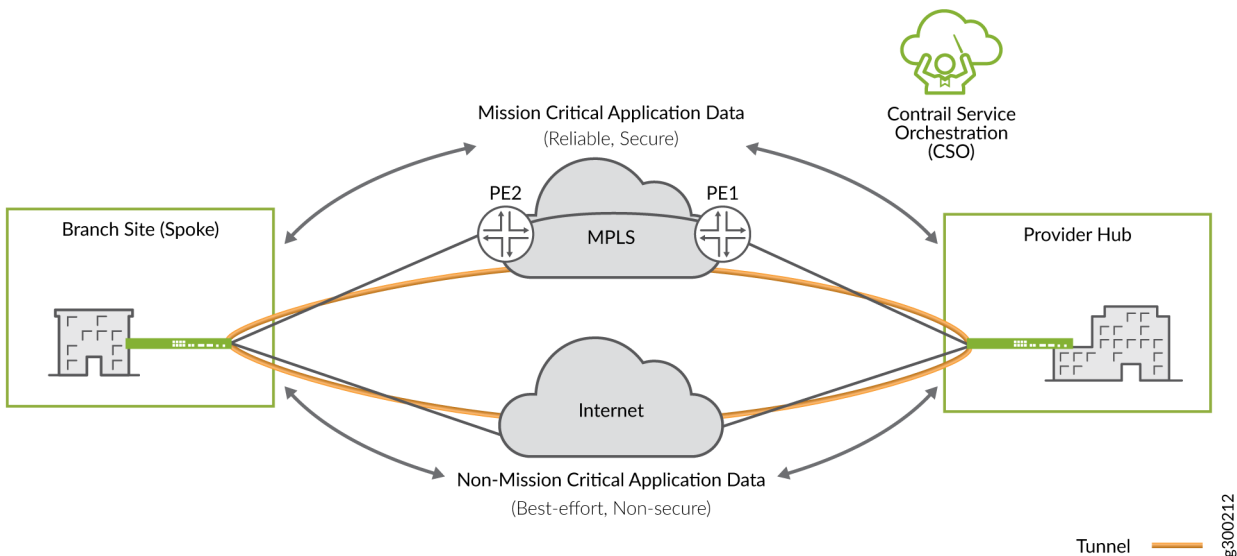
What's this? For the ease of use and adaptive policy management, you can now configure your security policies with dynamic applications and URLs as match conditions to react to changes in your network traffic over time.

Benefit: You can manage application traffic in your network with greater control and flexibility. Unified policies also simplify policy management at Layer 7 compared to the traditional security policies with application firewall rule sets.

First introduced in: Junos OS Release 18.4R1

Want to know more? See [Unified Security Policies](#).

SD-WAN



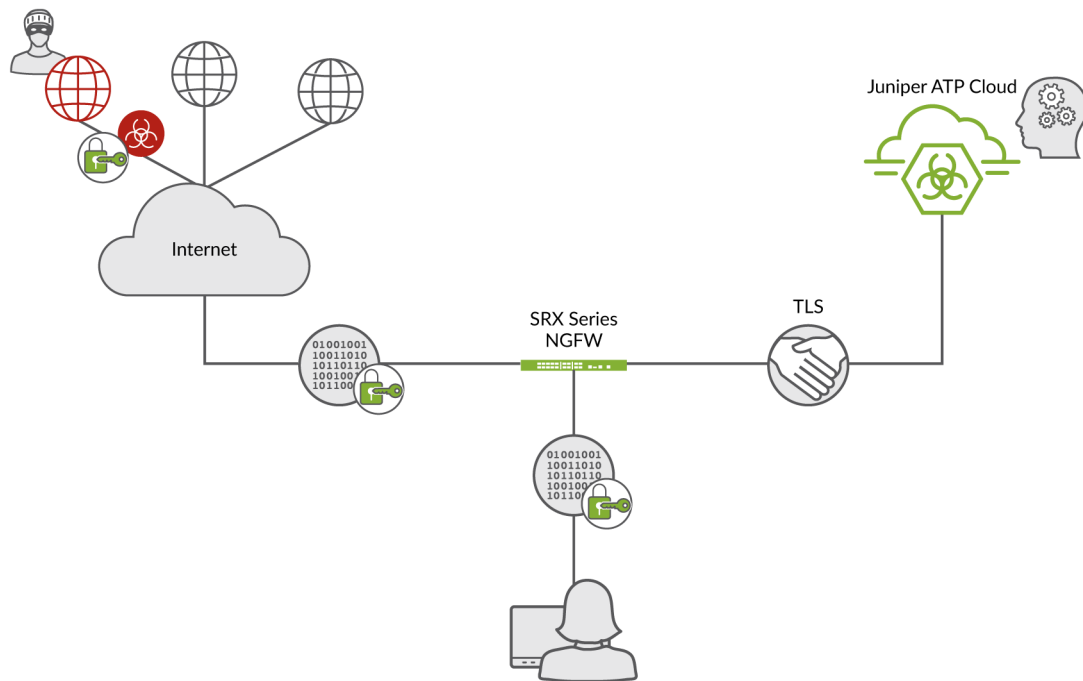
What's this? An SD-WAN implementation offers a flexible and automated way to route traffic from site to site. You can route traffic over different WAN links and assign higher priority to business-critical applications with advanced policy-based routing (APBR) and application quality of experience (AppQoE). In addition, the LTE and WiFi support adds wireless WAN connectivity over 3G and 4G/LTE networks.

Benefit: You can avail security and SD-WAN capabilities for distributed and branch locations with wired and wireless backup.

First introduced in: Junos OS Release 19.4R1 (LTE Mini-PIM)

Want to know more? See [Advanced Policy-Based Routing](#), [Application Quality of Experience](#).

Encrypted Traffic Insights



jn-000035

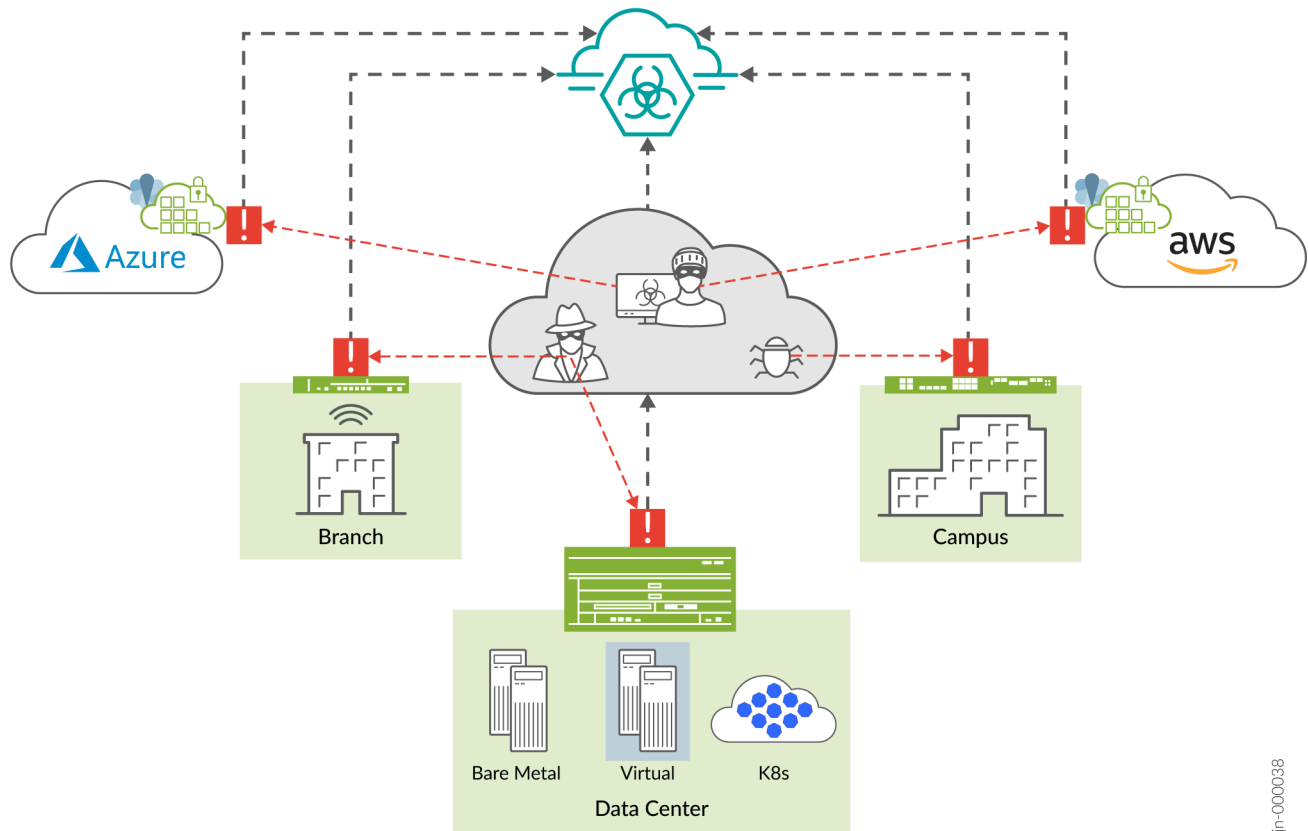
What's this? Encrypted Traffic Insights uses machine learning to analyze and detect malicious threats that are hidden in encrypted traffic without the need for decryption.

Benefit: Provides greater visibility to threats hidden in your network without breaking encryption, which means data privacy and security are no longer at odds.

First introduced in: Junos OS Release 20.2R1

Want to know more? See [Encrypted Traffic Insights](#).

Adaptive Threat Profiling



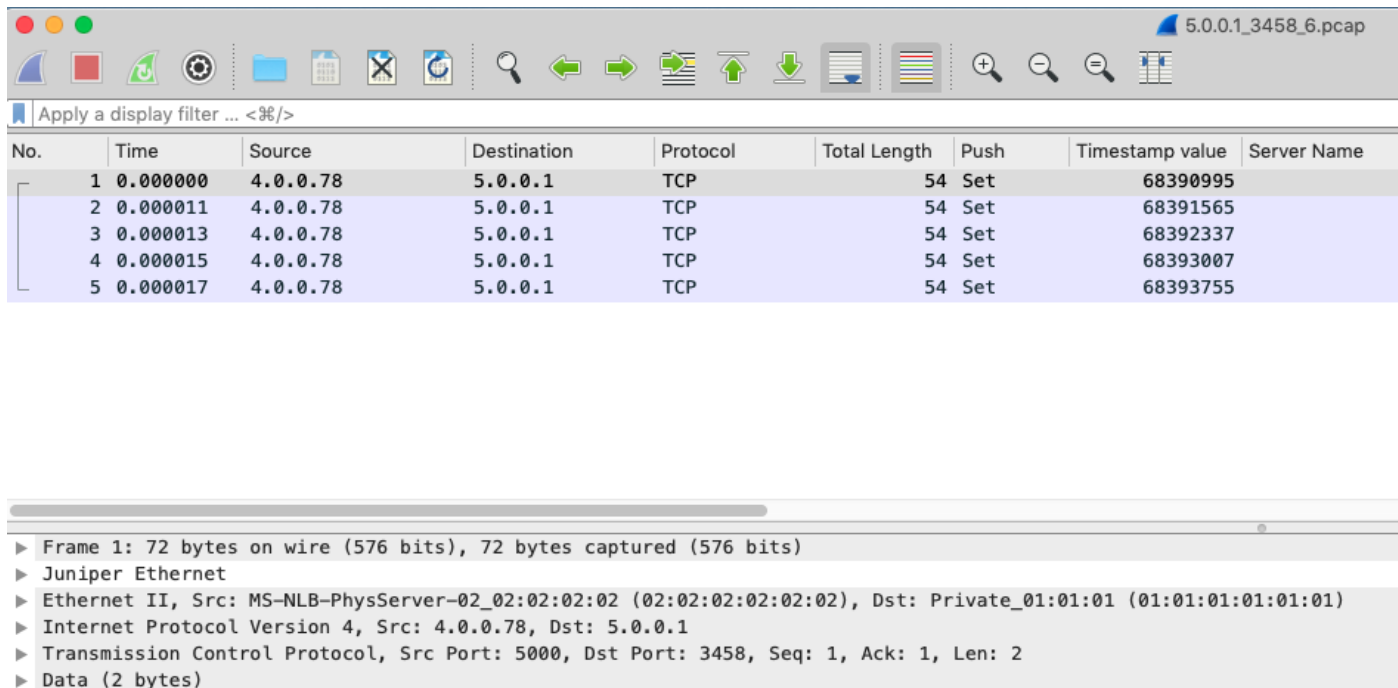
What's this? Adaptive Threat Profiling uses various detection capabilities of SRX Series devices to create security intelligence feeds based on real-time events in your network. With this feature, you can detect threat actors targeting your network, look for potential problems or suspicious activity, and even performs simple endpoint classification. By harnessing the power of Advanced Threat Protection and SecIntel, changes in your network and security posture can be coordinated and responded to in near-real time.

Benefit: You can generate, propagate, and consume threat feeds based on events happening in your network across the world. Allows administrators near-infinite adaptability to changing threats and network conditions for proactive management and threat mitigation.

First introduced in: Junos OS Release 20.2R1

Want to know more? See [Adaptive Threat Profiling Overview](#).

Packet Capture for Unknown Applications



The screenshot shows a packet capture tool interface. At the top, there's a toolbar with various icons for file operations, search, and display. Below the toolbar is a filter bar with the text "Apply a display filter ... <%/>". The main area displays a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Total Length, Push, Timestamp value, and Server Name. The first five packets are listed, all from source 4.0.0.78 to destination 5.0.0.1 using TCP. Below the table, there's a detailed view of the first packet, showing its structure: Frame 1 (72 bytes on wire, 72 bytes captured), Juniper Ethernet, Ethernet II (Src: MS-NLB-PhysServer-02_02:02:02:02, Dst: Private_01:01:01 (01:01:01:01:01:01)), Internet Protocol Version 4 (Src: 4.0.0.78, Dst: 5.0.0.1), Transmission Control Protocol (Src Port: 5000, Dst Port: 3458, Seq: 1, Ack: 1, Len: 2), and Data (2 bytes).

No.	Time	Source	Destination	Protocol	Total Length	Push	Timestamp value	Server Name
1	0.000000	4.0.0.78	5.0.0.1	TCP	54	Set	68390995	
2	0.000011	4.0.0.78	5.0.0.1	TCP	54	Set	68391565	
3	0.000013	4.0.0.78	5.0.0.1	TCP	54	Set	68392337	
4	0.000015	4.0.0.78	5.0.0.1	TCP	54	Set	68393007	
5	0.000017	4.0.0.78	5.0.0.1	TCP	54	Set	68393755	

▶ Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
▶ Juniper Ethernet
▶ Ethernet II, Src: MS-NLB-PhysServer-02_02:02:02:02 (02:02:02:02:02:02), Dst: Private_01:01:01 (01:01:01:01:01:01)
▶ Internet Protocol Version 4, Src: 4.0.0.78, Dst: 5.0.0.1
▶ Transmission Control Protocol, Src Port: 5000, Dst Port: 3458, Seq: 1, Ack: 1, Len: 2
▶ Data (2 bytes)

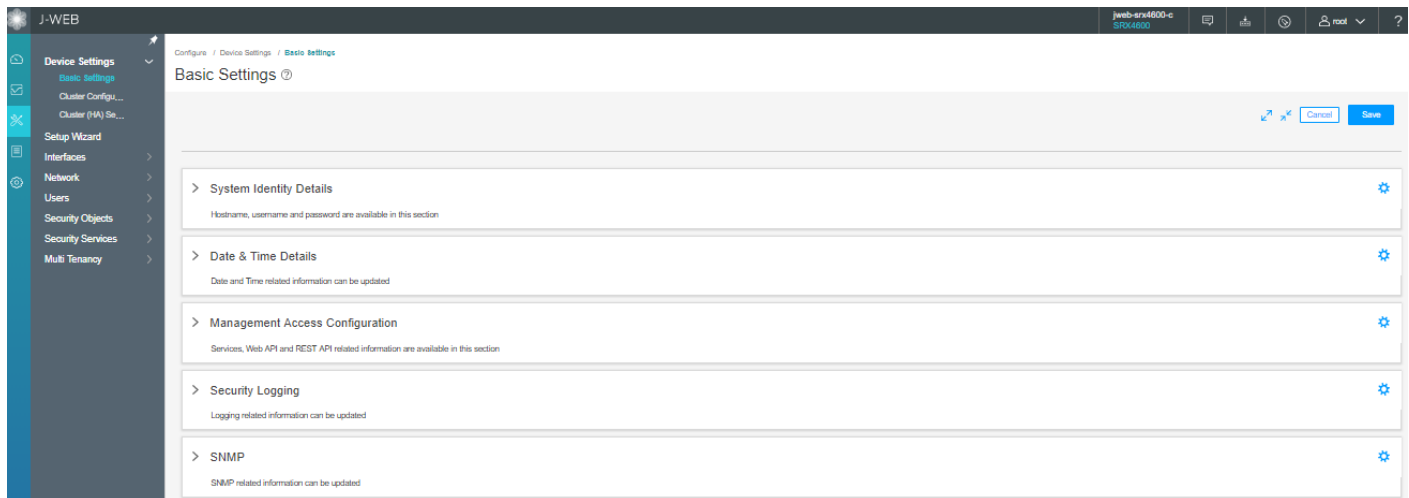
What's this? Custom applications are an unavoidable part of almost every enterprise network and can be difficult to identify and control. You can automatically capture packets from unknown applications and use the packet captures to gain additional insights to about your network, analyze it for potential threats, and help create custom application signatures when needed.

Benefit: You can manage your application traffic more efficiently and effectively by using the insights offered through packet captures on the unknown applications. Custom signatures or updates to the existing signatures are easier to identify and apply with multiple captures of traffic. For best results, you can use these captures in conjunction with Unified Policy to classify and control previously unknown traffic.

First introduced in: Junos OS Release 20.2R1

Want to know more? See [Packet Capture for Unknown Applications](#).

J-Web Getting Started Panel



What's this? You can easily set up and manage your SRX Series device using the enhanced Getting Started panel that provides an intuitive interface and the steps required to get you up and running quickly. We've added a Getting Started panel, HA mode wizards, and enhanced reporting options to make configuration, monitoring, general management, and troubleshooting easier than ever.

Benefit: By simply connecting your SRX Series device and your laptop or computer to the same network and then opening a browser, you can get started. We've streamlined the setup process using a naturally assistive tool to help you get the most out of all the features and functions the SRX Series device has to offer.

First introduced in: Junos OS Release 19.2R1

Want to know more? See [Getting Started Panel](#).

What's Next

Now that you've got a glimpse of key features that we've introduced in Junos OS release post 15.1X49, you can next figure out the upgrade path for your Junos OS. See "[Know the Upgrade Path for Junos OS Releases](#)" on [page 11](#).

Know the Upgrade Path for Junos OS Releases

SUMMARY

Read this topic to determine the upgrade path for Junos OS releases for your SRX Series devices and vSRX.

IN THIS SECTION

- [Upgrade Path for Your SRX Series](#) | 12
- [Upgrade Path for vSRX](#) | 15

Knowing the upgrade path helps you to choose the correct Junos OS package or packages to install.

You can consider upgrading from Junos OS Release 15.1X49 to 19.4R3 (SRX Series) or to 20.2R3 (vSRX and SRX380) as stated in [Table 1 on page 12](#).

Table 1: Junos OS Release for SRX Series

Devices	Junos OS Release
SRX300, SRX320, SRX340, SRX345, SRX550M, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800	19.4R3-S1
SRX380, SRX1500, vSRX, and cSRX	20.2R3

The details provided in the table are as per the recommendations at the time of publishing this document.

The best practice is to always check the most up-to-date version as suggested in Knowledge Base article. See [Junos Software Versions - Suggested Releases to Consider and Evaluate](#).

For information on upgrade path, see [Junos Upgrade Paths for SRX Platforms](#).

Upgrade Path for Your SRX Series

The following sections help you to determine the upgrade paths for the latest recommended versions of Junos OS releases.

Direct Upgrade

We support direct upgrade from Junos OS Release 15.1X49 to Junos OS Release 19.4R3-S1 for SRX Series devices.

[Table 2 on page 12](#) lists the direct upgrade paths supported for SRX Series devices.

Table 2: Direct Upgrade Paths for Junos OS Release

From Current Junos OS Release	Direct Upgrade Releases
15.1X49	19.4R3 Service release
18.4R3 or 18.4R3 Service releases	19.4R3 or 19.4R3 Service release.

Table 2: Direct Upgrade Paths for Junos OS Release (Continued)

From Current Junos OS Release	Direct Upgrade Releases
19.3	19.4, 20.1, and 20.2
19.4	20.1 and 20.2

Interim Upgrade Path for Junos OS Releases 19.4R3 and 20.2R3

[Table 3 on page 13](#) and [Table 4 on page 14](#) list the interim upgrade paths supported for SRX Series devices.

Use the tables to determine the upgrade path you must follow when upgrading to a newer version of Junos OS Release.

Table 3: Interim Upgrade Paths for Junos OS Release 19.4R3

Junos OS Release	Target Junos OS (First Hop)	Target Junos OS (Second Hop)	Target Junos OS (19.4R3)
15.1X49	19.4R3-S1	—	—
17.3	18.2	19.1	19.4R3
17.4	18.3	19.2	19.4R3
18.1	18.4	19.3	19.4R3
18.2	19.1	19.4R3	—
18.3	19.2	19.4R3	—
18.4	19.3	19.4R3	—
19.1	19.4R3	—	—
19.2	19.4R3	—	—
19.3	19.4R3	—	—
19.4	19.4R3	—	—

Table 4: Interim Upgrade Paths for Junos OS Release 20.2R3

Junos OS Release	Target Junos OS (First Hop)	Target Junos OS (Second Hop)	Target Junos OS (Third Hop)	Target Junos OS (20.2R3) (SRX380, SRX1500, vSRX, and cSRX)
15.1X49	19.4R3-S1 (direct upgrade)			20.2R3
17.3	18.2	19.1	19.4R3	20.2R3
17.4	18.3	19.2	19.4R3	20.2R3
18.1	18.4	19.3	20.2R3	
18.2	19.1	19.4R3	20.2R3	
18.3	19.2	19.4R3	20.2R3	
18.4	19.3	20.2R3	—	
19.1	19.4R3	20.2R3	—	
19.2	19.4R3	20.2R3	—	
19.3	20.2R3	—		
19.4	20.2R3	—		
20.1	20.2R3	—		

Example of Direct and Interim Upgrades:

To Upgrade From	Path
Junos 15.1X49-D170 to 19.4R3	15.1X49-D170 → 19.4R3 (direct upgrade)
Junos 17.3R1 to 19.4R3	17.3 → 18.2 → 19.1 → 19.4R3 (interim upgrade)
Junos 18.4R1 to 20.2R3	18.4 → 19.3 → 20.2R3 (interim upgrade)

If you are using SRX380 Services Gateways, note that the first supported version of Junos OS Release is 20.1R1. We support direct upgrade to Junos OS 20.2R3 from 20.1R1.

Upgrade Path for vSRX

Junos OS Release 18.4R1 supports a new software architecture called vSRX 3.0. We recommend upgrading to vSRX3.0 to quickly introduce new services, deliver customized services to the users, and scale security services based on dynamic needs.

Use [Table 5 on page 15](#) to know about the direct upgrade path supported for your Junos OS on vSRX instances.

Table 5: Upgrade Path for vSRX

Current Junos OS Release	Direct Upgrade To Release
15.1X49	17.4, 18.1, 18.2, 18.3, 18.4, 19.1, or 19.2

Note that we do not support direct upgrade of vSRX from Junos OS Release 15.1X49 Releases to 19.3 and higher releases.

We recommend Junos OS Release 20.2R3 for your vSRX instance.

We recommend that you deploy a new vSRX VM instead of performing a Junos OS upgrade. Upgrading to the latest VM enables you to move from vSRX to the newer and enhanced vSRX 3.0 architecture.

Downgrading Junos OS

We support downgrades up to three Junos OS releases at a time. You can downgrade to the Junos OS release that occurs directly before the currently Junos OS release, or to three Junos OS releases before. For example, you can downgrade directly from Junos OS Releases 20.2R1 to 19.4R3. If you want to downgrade from 20.2R1 to 18.4R1, you must first downgrade to 19.3R1 and then to 18.4R1.

What's Next

Now that you've determined the Junos OS version upgrade path, proceed to perform upgrade procedures. See ["How to Upgrade to Junos OS Release 19.4R3 and 20.2R3" on page 16](#).

How to Upgrade to Junos OS Release 19.4R3 and 20.2R3

SUMMARY

In this topic, you'll learn how to upgrade Junos OS software from Release 15.1X49 to Release 19.4R3 on SRX Series and learn about the upgrade options available for your vSRX VM.

IN THIS SECTION

- [Best Practices for Upgrading Junos OS | 16](#)
- [Follow Pre-Installation Steps | 17](#)
- [Upgrade Directly on Your Security Device \(CLI\) | 18](#)
- [Upgrade Directly on Your Security Devices in a Chassis Cluster \(CLI\) | 22](#)
- [Upgrade Junos OS Using a USB Flash Drive or J-Web | 23](#)
- [Upgrade Your vSRX VM | 24](#)
- [Upgrade Your cSRX Software Image | 24](#)
- [Upgrade Junos OS on SRX Series Devices Managed by Junos Space | 25](#)
- [Upgrade Junos OS on SRX Series Devices Managed by Juniper Sky™ Enterprise | 28](#)
- [After You Upgrade to Junos OS Release 19.4R3 or 20.2R3 | 28](#)

Best Practices for Upgrading Junos OS

We suggest you start with the following best practices to optimize your upgrade experience:

- Read Release Notes for Junos OS Release [19.4R3](#) and [20.2R3](#).
- Connect your device to the Internet.
- Back up the current configuration.
- Ensure that there are no uncommitted changes.
- Clear files and erase unwanted or unused configurations using the `request system storage cleanup` command.
- Ensure both nodes are online and have same version of Junos OS in case of a chassis cluster setup.
- Plan for an extended maintenance window preferably during non-business hours to minimize impact.
- Allocate sufficient time during the maintenance window for the upgrade, troubleshooting, and any post configuration procedures.
- Identify business contacts who will help verify application and network functionality after the upgrade.

Follow Pre-Installation Steps

Ensure that you complete the following tasks before you perform the upgrade to Junos OS Release 19.4R3 or Junos OS Release 20.2R3.

- Check the current Junos OS software version.

```
user@host> show version
```

```
Hostname: srx4200-02 Model: srx4200
Junos: 15.1X49-D170.4
JUNOS Software Release [15.1X49-D170.4]
```

- Check whether the system has sufficient storage for the upgrade.

```
user@host> show system storage
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/vtbd0s1a	501M	366M	95M	79%	/
devfs	1.0K	1.0K	0B	100%	/dev
/dev/md0	1.0G	1.0G	0B	100%	/junos
/cf	501M	366M	95M	79%	/junos/cf
devfs	1.0K	1.0K	0B	100%	/junos/dev/
procfs	4.0K	4.0K	0B	100%	/proc
/dev/vtbd1s1e	1.6G	82K	1.4G	0%	/config
/dev/vtbd1s1f	14G	141M	13G	1%	/var
/dev/vtbd3s2	91M	948K	90M	1%	/var/host
/dev/md1	320M	1.4M	293M	0%	/mfs
/var/jail	14G	141M	13G	1%	/jail/var
/var/jails/rest-api	14G	141M	13G	1%	/web-api/var
/var/log	14G	141M	13G	1%	/jail/var/log
.....					
.....					

From the sample output, **/dev/vtbd0s1a** and **/dev/vtbd1s1f** indicate storage available on the compact flash and hard disk.

- Save the active configuration and license keys. You can save the backup configuration file on your device or a USB drive connected to your device. You can also use TFTP or SCP server or on your system such as laptop to save the file.

Following example shows saving of an active configuration file on the device.

```
user@host> show configuration | save /var/tmp/filename
```

```
Wrote 273 lines of output to '/var/tmp/backup.txt'
```

The system saves the active configuration at the specified file location.

You can save license keys using the `user@host> request system license save filename` command.

You can create copies of the software running on your device using the system snapshot feature. Having a snapshot of software helps you to recover to a known, stable environment in case something goes wrong with the upgrade. See [Backing Up an Installation Using Snapshots](#).

- Ensure that there are no uncommitted changes.
- Remove the NTP configuration that has more than one source address.

```
user@host# delete system ntp source-address source-address;
```

- Remove chassis cluster fabric interface configuration if you have configured the enable or disable option.

```
user@host# set interfaces fab0 fabric-options member-interfaces sinterface-name enable/disable
```

Upgrade Directly on Your Security Device (CLI)

We'll use the following hardware and software combination in this example:

- SRX4200 device
- Junos OS Release 15.1X49-D170
- Available flash memory of 512 MB

Use this procedure to learn how to upgrade from Junos OS Release 15.1X49-D170 to Junos OS Release 19.4R3-S1:

1. Navigate to the Juniper Networks [Support](#) page for the SRX4200 and select OS as Junos SR and version as 19.4 as shown in [Figure 1 on page 19](#).

Figure 1: Download Junos OS Software

Download Results for: SRX4200

Select: OS **Junos SR** VERSION 19.4 [Expand All](#) +

✕ Install Package 8 File(s)

Description	Release	File Date	Downloads
SRX4100 and SRX4200	19.4R3-S2	04 Mar 2021	tgz (1197.37MB) Checksums
SRX4100 and SRX4200	19.4R3-S1	12 Dec 2020	tgz (1197.08MB) Checksums

2. Click **tgz (1197.08 MB)** under Downloads.
3. Enter your credentials to review and accept the End User License Agreement. You'll be guided to the software image download page.
4. You'll see the following two options in the download page. Use one of the options to download the Junos OS image file:
 - **To download the image directly on your device, use the following URL**—Directly downloads the image on your security device.

Example:

```
user@host> file copy "https://cdn.juniper.net/software/junossr/19.4R3-S1.3/junos-srxmr-x86-64-19.4R3-S1.3.tgz?
SM_USER=user-xyz&__gda__=1612849296_041be3207dec81353b9e2c02a67027b1" /var/tmp/junos-srxmr-x86-64-19.4R3-S1.3.tgz
```

Your security device downloads the image to the /var/tmp/image-name location. The image name is junos-srxmr-x86-64-19.4R3-S1.3.tgz in this example.

- **To download the image on your local host, CLICK HERE**—Downloads the image on your local system such as laptop. You can copy the software image from your local system to the security device using SCP or SFTP options.

```
user@host>
user@host> start shell
user@host%
```

```
user@host% cd /var/tmp
user@host% scp userabc@hostname:/path/junos-vsrx-x86-64-19.4R1-S3.2.tgz
```

In this procedure, we'll download the image directly on the security device. As per the instructions on the screen, copy the URL provided in the box. The URL string is copied to the clipboard.

5. Verify MD5 checksums on a Junos install package.

This step confirms that the Junos installation package downloaded from the Juniper Networks website is not modified in any way.

a. List the files to display the downloaded image.

```
user@host> file list /var/tmp
```

```
/var/tmp:
BSD.var.dist
appidd_trace_debug
eedebug_bin_file
install/
junos-srxmr-x86-64-19.4R3-S1.3.tgz
kmdchk.log
krt_rpf_filter.txt
mmcq_mmdb_rep_mmcq
nsd_restart
pc /
pfe_debug_commands
phone-home/
pics/
pkg_cleanup.log.err
policy_status
preinstall_boot_loader.conf
rtsdb/
sd-upgrade/
sec-download/
vi.recover/
```

b. Display the MD5 checksum value of your image file.

```
user@host> file checksum md5 /var/tmp/junos-srxmr-x86-64-19.4R3-S1.3.tgz
```

```
MD5 (/var/tmp/junos-srxmr-x86-64-19.4R3-S1.3.tgz) = 95cdd3b3e487664b48e55fbfde5965af
```

c. Compare the MD5 hash output with the MD5 hash provided on the download page when you click the checksums option:

Download Results for: SRX4200



Select: OS Junos SR

VERSION 19.4

Expand All +

X Install Package

8 File(s)

Description	Release	File Date	Downloads
SRX4100 and SRX4200	19.4R3-S2	04 Mar 2021	tgz (1197.37MB) Checksums
SRX4100 and SRX4200	19.4R3-S1	12 Dec 2020	tgz (1197.08MB) Checksums

Checksums



MD5 : 95cdd3b3e487664b48e55fbfde5965af

SHA1 : 0e894defea03cc1666f62bce34f8a886b983964d

SHA256 : 192731ec776656f910a1afc4c884f57b70ba8c809244a070a5180c83754ade79

SHA512 : d352ac7032f8551846633251d010869f3051e2016053aa12b1a8f23f7a9e0e1731ce03c48e
2bd9df7a6b3f7d57dccb1149626361228381c4e53c99ae8a353599

- d. Repeat the steps to calculate the SHA1, SHA256, and SHA512 values of the file.
6. Validate the Junos OS image to ensure that the existing configuration is compatible with the new image before you start the actual upgrade.

```
user@host> request system software validate /var/tmp/junos-srxmr-x86-64-19.4R3-S1.3.tgz
```

```
Checking compatibility with configuration
Initializing...
Verified manifest signed by PackageProductionEc_2019 method ECDSA256+SHA256
Using /var/tmp/junos-srxmr-x86-64-19.4R3-S1.3.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
```

The SRX1500 device, SRX4000-line devices, SRX5000-line devices with RE3, and vSRX instances do not support the `request system software validate` command to validate the software.

7. Install the image.

```
user@host> request system software add /var/tmp/junos-srxmr-x86-64-19.4R1-S3.2.tgz no-copy
```

```
NOTICE: Validating configuration against junos-srxmr-x86-64-19.4R3-S1.3.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
Checking compatibility with configuration
Initializing...
Verified manifest signed by PackageProductionEc_2019 method ECDSA256+SHA256
Using /var/tmp/junos-srxmr-x86-64-19.4R3-S1.3.tgz
```

8. Reboot your system.

```
Reboot the system ? [yes,no] (no)
```

Yes

```
Shutdown NOW! [pid 18475]

user@host>
*** FINAL System shutdown message from user@host***

System going down IMMEDIATELY
```

9. Check the Junos OS version after system reboots using the show version command.

Upgrade Directly on Your Security Devices in a Chassis Cluster (CLI)

We'll use the following hardware and software combination in this example:

- SRX4200 devices in a chassis cluster setup
- Junos OS Release 15.1X49-D170
- Available flash memory of 512 MB

Before you Begin

- Ensure that you have the same version of Junos OS on each node of the cluster.
- Ensure that both devices in the cluster are online at the same time.
- Remove the chassis cluster fabric interface configuration if you have configured the enable or disable option.

```
user@host# set interfaces fab0 fabric-options member-interfaces sinterface-name enable/
disable
```

1. Download and validate the Junos OS 19.4R3-S1 image. See Steps 1 to 6 provided in ["Upgrade Directly on Your Security Device \(CLI\)" on page 18](#) for details.

2. Install the Junos OS image on node 0.

```
{primary:node0}
```

```
user@host> request system software add /var/tmp/junos-srxmr-x86-64-19.4R1-S3.2.tgz no-copy
```

Do not reboot the device after installation completes.

3. Install the Junos OS image on node 1.

```
{{secondary:node1}}
```

```
user@host> request system software add /var/tmp/junos-srxmr-x86-64-19.4R1-S3.2.tgz no-copy
```

Do not reboot the device after installation completes.

4. Reboot both the nodes by using the **request system reboot** command on both the nodes separately.
After the reboot, both the nodes will have the same Junos OS image.
5. Check the Junos OS version after system reboots using the show version command.

Upgrade Junos OS Using a USB Flash Drive or J-Web

IN THIS SECTION

- [USB Flash Drive | 23](#)
- [J-Web | 23](#)

USB Flash Drive

You can use a USB flash drive to upgrade Junos OS images or recover an SRX Series device after boot media corruption in cases where there is no console access to an SRX Series device. For more information, see the KB article at [Install Software via CLI \(Method 3 - from Junos software copied to USB stick\)](#).

J-Web

You can upgrade your SRX Series device in a few steps using J-Web. For more information, see [Install Software Packages](#).

Upgrade Your vSRX VM

If you consider to upgrade Junos OS on your vSRX VM, note the following:

- We recommend that you deploy a new vSRX VM instead of performing a Junos OS upgrade. The new VM enables you to move from vSRX to the newer and more enhanced vSRX 3.0 version.
- Moving to the vSRX 3.0 software architecture enables you to quickly introduce new services, deliver customized services to users, and scale security services based on dynamic needs. Junos OS Release 18.4R1 and later releases support vSRX 3.0.

You can download the vSRX3.0 image from Juniper Networks [Support](#) page.

- Ensure to save the configuration, certificate, and license files before you perform the upgrade.

See the KB article [Overview of the Available Virtual SRX Models, vSRX and vSRX 3.0](#) for more details on vSRX 3.0 support.

Refer to the [vSRX Documentation](#) for instructions on installing a new VM.

Upgrade Your cSRX Software Image

Starting in Junos OS Release 20.2R1, the Juniper Networks® cSRX Container Firewall image is available for download from the Juniper Support site, similar to other Junos OS platform images. The cSRX container is packaged in a Docker image and runs in the Docker Engine on the Linux host.

To install cSRX in a bare-metal Linux server:

1. Review [Requirements](#) to verify the system software specifications for the Linux server required to deploy the cSRX container.
2. Install and configure Docker on your Linux host platform to implement the Linux container environment.

Docker installation requirements vary based on the platform and the host OS (Ubuntu, Red Hat Enterprise Linux (RHEL), or CentOS).

3. For docker installation instructions on the different supported Linux host operating systems, see:

- Docker Engine installation—<https://docs.docker.com/engine/installation/>
- Script to install Docker Engine—<https://get.docker.com/>
- Centos/Redhat—<https://docs.docker.com/install/linux/docker-ce/centos/>
- Debian—<https://docs.docker.com/install/linux/docker-ce/debian/>
- Fedora—<https://docs.docker.com/install/linux/docker-ce/fedora/>
- Ubuntu—<https://docs.docker.com/install/linux/docker-ce/ubuntu/>

- Download the cSRX software image from the Juniper Networks website and install it on your host. See [Loading the cSRX Image](#) for details.

For complete information about how to implement Juniper's cSRX on a server with Ubuntu OS, see [Day One: Building Containers with cSRX](#).

Upgrade Junos OS on SRX Series Devices Managed by Junos Space

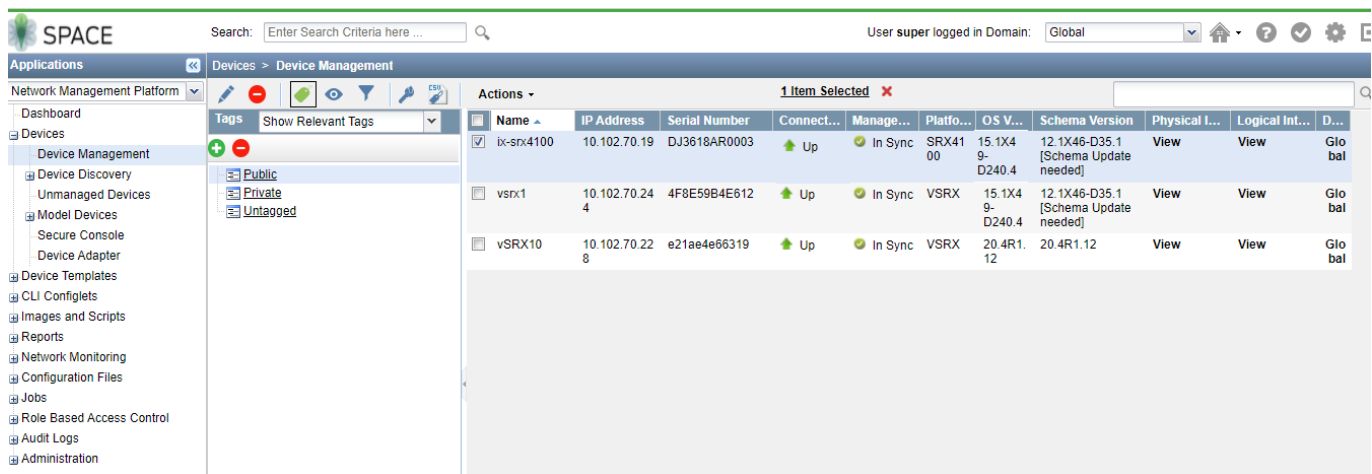
SUMMARY

We'll use the following simple steps to upgrade your security device managed by Junos Space. Watch the video [Junos Space Image Management](#) to understand the procedure.

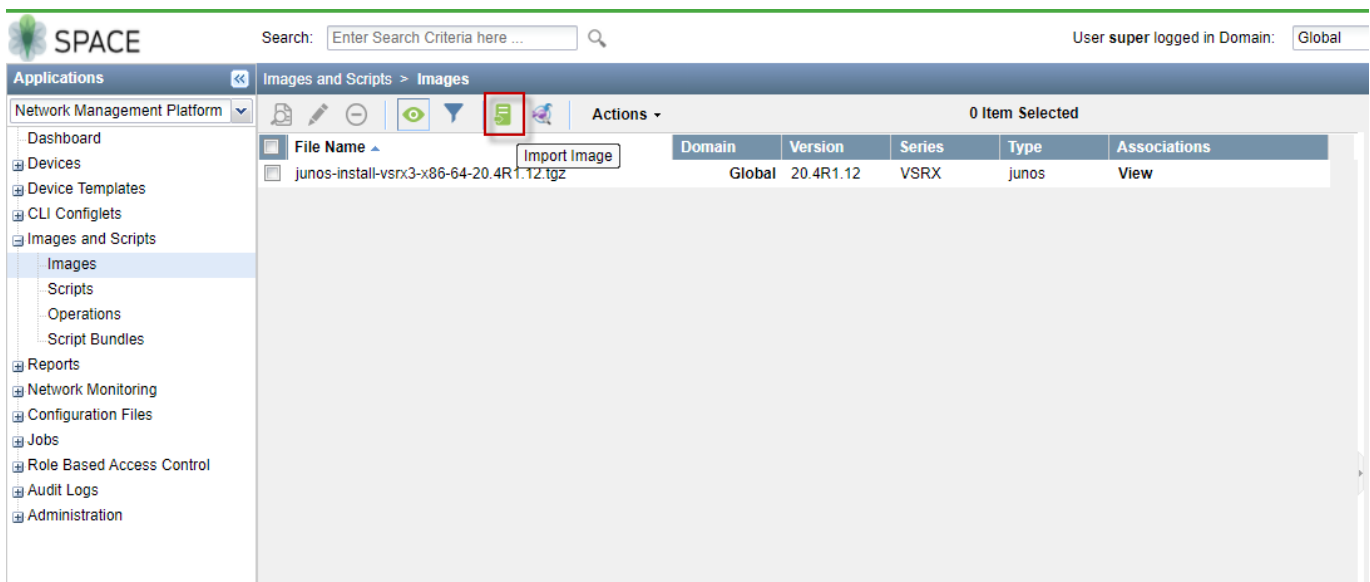
We'll use the following hardware and software combination in this example:

- SRX4100 device managed by Security Director
- Junos OS Release 15.1X49-D170

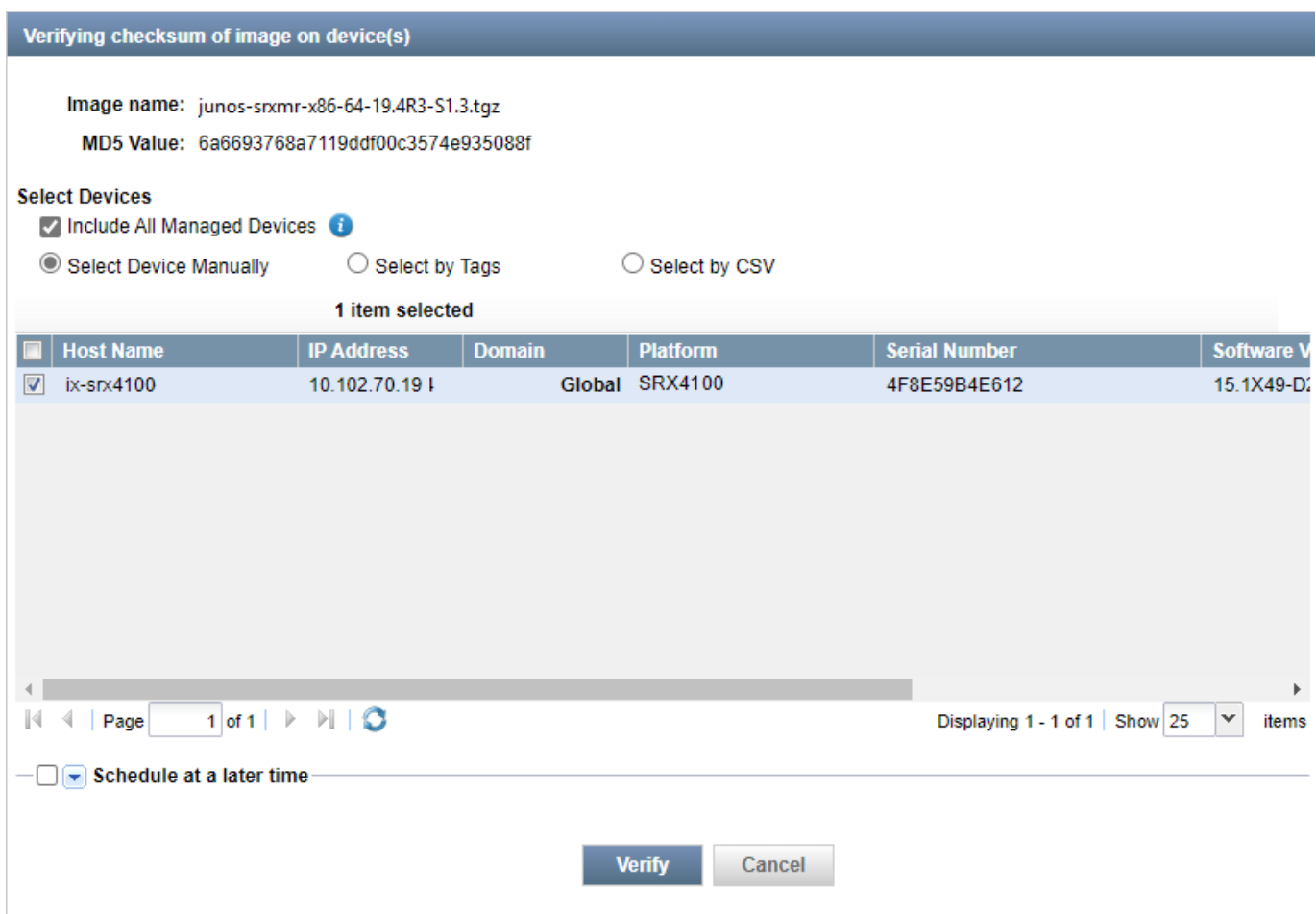
- On the Network Management Platform GUI, select **Devices > Device Management**. The Device Management page is displayed.



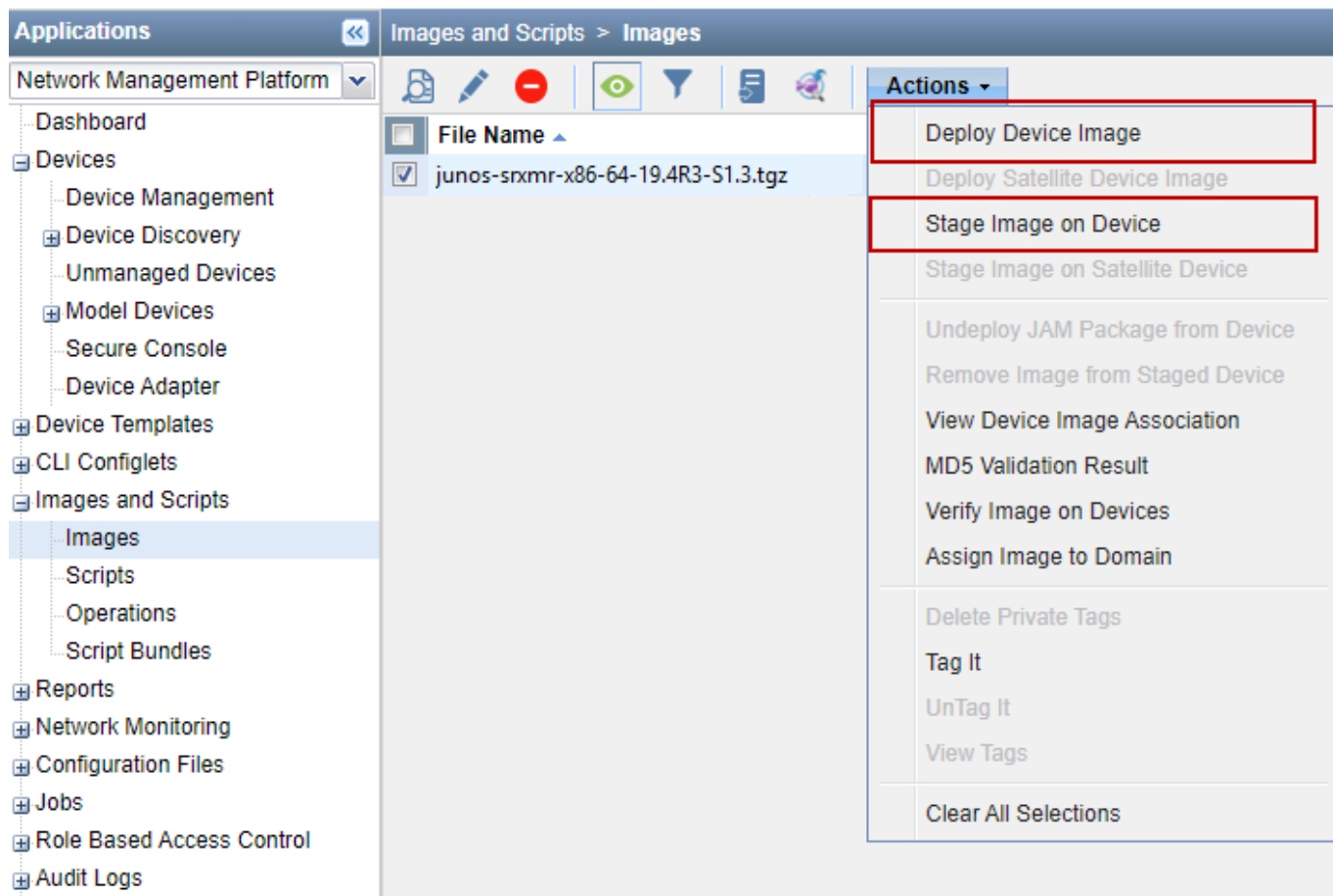
- Check the OS version running on the device.
- Navigate to the Juniper Networks [Support](#) page and download Junos OS version 19.4R3-S1 and save the file to your computer. See ["Upgrade Directly on Your Security Device \(CLI\)" on page 18](#) for instructions.
- Go to **Images and Scripts** and select **Images**. Click the Import Image icon to upload the image file into Junos Space Platform.



5. Validate the image by selecting the **Actions > Verify Image on Device** option.



6. Select the uploaded Junos OS image and choose the **Deploy Image** option from **Actions**. Alternatively, you can choose to stage the deploy at a later time by selecting the **Stage Image on Device** option.



7. In the Deploy Image on Devices page, select the device that you want to upgrade and specify the **Remove package after Successful Installation** and **Delete any existing image before download** options.

Image name: junos-srxmr-x86-64-19.4R3-S1.3.tgz
MD5 Value: 6a6693768a7119ddf00c3574e935088f

Select Devices

☐ Include All Managed Devices i

☒ Select Device Manually ☐ Select by Tags ☐ Select by CSV

0 items selected

Device Name	IP Address	Platform	Software Version	Staged Status	Checksum Sta...	Last Checksu...	Domain
ix-srx4100- RIMARY	10.102.70.19	SRX4100	15.1X49-D240.4	Not Staged			Global

Page 1 of 1

Displaying 1 - 2 of 2 | Show 25 items

☐ Show ISSU/ICU capable devices only

Common Deployment Options

☐ Use image already downloaded to device

☐ Archive data (Snapshot)

☒ Remove the package after successful installation

☒ Delete any existing image before download

8. Click **Deploy** to start installation.
9. Reboot the device after successful installation.

Complete the following checks after you install the new Junos OS version.

- Check the Junos OS version after the system reboots using the **show version** command.
- Ensure your device settings, network settings, and other configuration are in place using the **show configuration** command.

Upgrade Junos OS on SRX Series Devices Managed by Juniper Sky™ Enterprise

You can upgrade your Junos OS devices easily with images hosted by Juniper Sky Enterprise. Juniper Sky Enterprise streamlines the Junos OS image upgrade process using only a browser.

To perform Junos upgrade on a device:

1. Select a target device from the Juniper Sky Enterprise dashboard and select the Junos OS image version you want to upgrade.
2. Click **Upgrade** option.
3. Sky Enterprise checks for available disk space. If there is sufficient space, it enables the **New Upgrade** option to continue.

Sky Enterprise delivers the image directly from Juniper Networks, making the process fast and efficient. For more information, see [Juniper Sky Enterprise User Guide](#).

After You Upgrade to Junos OS Release 19.4R3 or 20.2R3

IN THIS SECTION

- [Licensing Requirements](#) | 29

Perform the following steps after you upgrade to Junos OS Release 19.4R3 or to Junos OS Release 20.2R3.

- Copy the device configuration files back to the device. We recommend to retain the configuration unless you are deploying a new vSRX VM.
- Download and install the latest IDP signature package. See [Updating the IDP Signature Database Manually](#).
- Download and install the latest application signature package. See [Downloading and Installing the Junos OS Application Signature Package Manually](#).

- Change GPRS tunneling protocol (GTP) settings. GTP distribution without GTP inspection does not work after an upgrade from Junos OS Releases 15.1X49 to 18.X releases. You can use one of the following workarounds:
 - Disable the GTP Distribution feature if possible.
 - Enable GTP Inspection on all GTP traffic which passes through the device, by configuring a GTP profile on all security policies which may carry GTP traffic. See [Example: Enabling GTP Inspection in Policies](#).
- Decide when you'd like to migrate to unified policy. See ["Start Using Unified Policies Post Upgrade" on page 41](#).

Licensing Requirements

Starting in January 2020, we've transitioned to the Flex Software Subscription Licensing Model for SRX Series and vSRX. If you are not currently using the legacy licenses model, see the [Flex Software License for SRX Series Devices](#).

If you have any questions, contact your Juniper Networks sales representative at <https://www.juniper.net/in/en/contact-us/> and they will assist you in choosing the best licensing model for your application.

If you have legacy license models, you can continue to use them when you upgrade to Junos OS release 19.4R3 or 20.2R3.

What's Next

Now you have installed the new Junos OS on your device. If you want to migrate to the unified policy configuration, see ["Start Using Unified Policies Post Upgrade" on page 41](#). Otherwise, learn about new features and enhancements that you can start using with your Junos OS. See ["Explore New Features Post Upgrade" on page 47](#).

Migrate to vSRX3.0

SUMMARY

Learn how to migrate vSRX software architecture from vSRX2.0 to vSRX3.0 and understand about the license requirements when you upgrade your vSRX.

IN THIS SECTION

- [Overview | 30](#)
- [Migrate to vSRX3.0 | 36](#)
- [What's Next? | 40](#)

In Junos OS Release 18.4R1, we've introduced a new software architecture vSRX3.0 for vSRX virtual firewalls. We recommend that you migrate to vSRX3.0 for your vSRX VM. If you are using vSRX2.0, you can migrate to the new vSRX3.0 in few steps. Note that the command-line interface (CLI) remains the same and the configuration that works on vSRX2.0 also works in vSRX3.0.

In this document, we use the following terms for vSRX architectures:

- Latest vSRX architecture (vSRX3.0) as **vSRX3.0**
- Architecture prior to vSRX3.0 as **vSRX2.0**

Overview

IN THIS SECTION

- [Introduction to vSRX3.0 | 30](#)
- [License Requirements for vSRX3.0 | 35](#)

Introduction to vSRX3.0

The new vSRX3.0 architecture is a streamlined virtual machine (VM) using FreeBSD 12.x / Junos OS as operating system. In vSRX3.0, the Routing Engine and the Packet Forwarding Engine run on FreeBSD 12.x or later version as single VM for improved performance and scalability. The vSRX3.0 uses DPDK to process the data packets in the data plane.

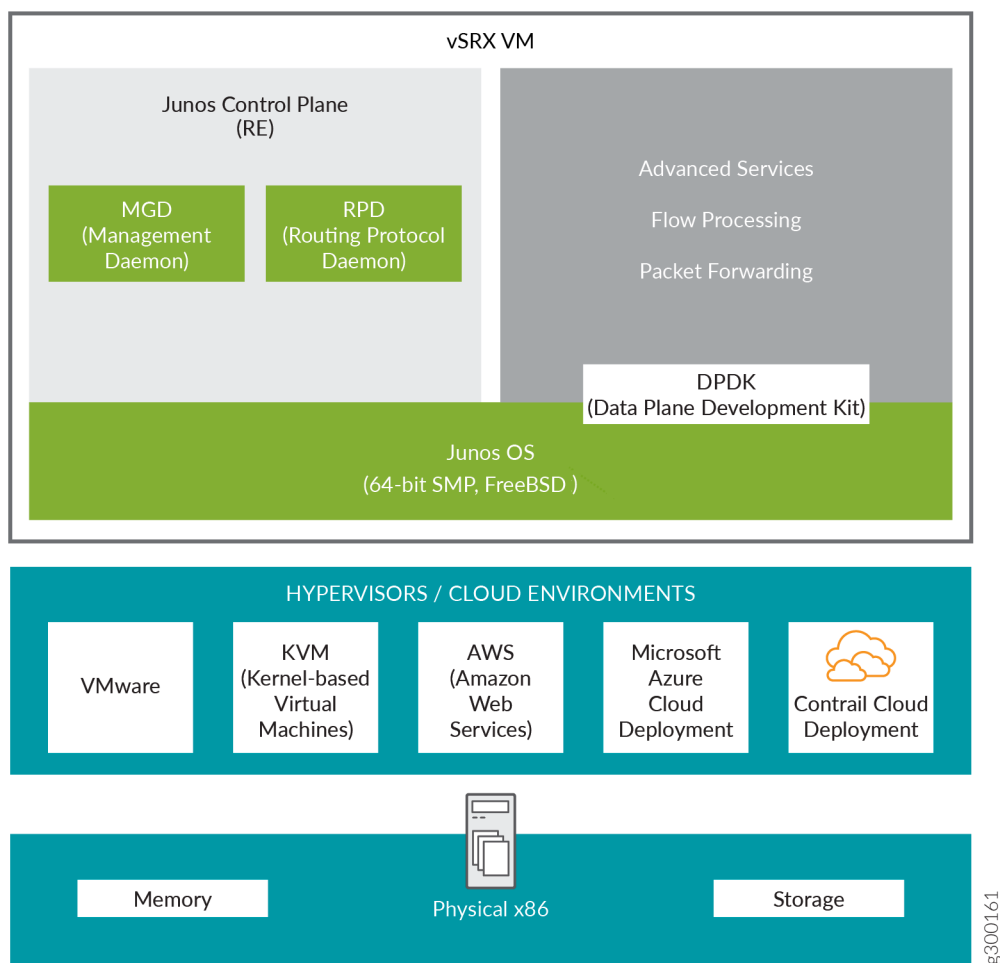
Benefits

Migrating to vSRX3.0 enables you to quickly introduce new services, deliver customized solutions, and scale security services dynamically due to:

- Faster boot-time and enhanced responsiveness of the control plane during management operations
- Increased operational benefits due to faster commits and CLI upgrades
- Increased agility and smaller image size due to elimination of dual OS and nested virtualization
- No special config required for enabling promiscuous mode on the management port and cluster control links
- Simplified and seamless deployments across different host environments

Figure 2 on page 31 shows vSRX architecture.

Figure 2: vSRX3.0 Architecture



Supported Junos OS Releases

Table 6 on page 31 provides a list of supported Junos OS releases for vSRX2.0 and vSRX3.0.

Table 6: Junos OS Release Support for vSRX2.0 and vSRX3.0

vSRX Architectures	Supported Junos OS Releases
vSRX2.0	15.1X49, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2
vSRX3.0	18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2

Feature Support in vSRX2.0 and vSRX3.0

Table 7 on page 32 and Table 8 on page 34 lists features supported in vSRX2.0 and vSRX3.0.

Table 7: Feature Support in vSRX2.0 and vSRX3.0

Features	vSRX2.0	vSRX3.0
2 vCPU / 4 GB RAM 5 vCPU / 8 GB RAM	Yes	Yes
9 vCPU / 16 GB RAM	Yes	Yes (Junos OS Release 19.1R1 onwards)
17 vCPU / 32 GB RAM	Yes	Yes (Junos OS Release 19.1R1 onwards)
Flexible flow session capacity scaling by an additional vRAM	Yes (from Junos 19.1R1 onwards)	Yes (Junos OS Release 19.2R1 onwards)
Multicore scaling support (Software RSS)	No	Yes (Junos OS Release 19.3R1 onwards)
Reserve additional vCPU cores for the Routing Engine	Yes	Yes
Virtio (virtio-net, vhost-net)	Yes	Yes
Supported Hypervisors		
VMware ESXi 5.5, 6.0, 6.5, 7.0	Yes	Yes
VMware ESXi 6.7	No	Yes (Junos OS Release 19.3R1 onwards)
KVM on Ubuntu 16.04, Centos 7.1, Redhat 7.2	Yes	Yes
Hyper-V	Yes	Yes (Junos OS Release 19.1R1 onwards)
Nutanix	Yes	Yes (Junos OS Release 19.1R1 onwards)
Contrail Networking 3.x	Yes	Yes

Table 7: Feature Support in vSRX2.0 and vSRX3.0 (*Continued*)

Features	vSRX2.0	vSRX3.0
Contrail Networking 5.x	No	Yes (Junos OS Release 19.3R1 onwards)
AWS	Yes	Yes
Azure	Yes	Yes (Junos OS Release 19.1R1 onwards)
Google Cloud Platform (GCP)	No	Yes (Junos OS Release 19.3R1 onwards)
Other Features		
Cloud-init	Yes	Yes
AWS ELB and ENA using C5 instances	Yes	Yes (Junos OS Release 20.1R1 onwards)
Powermode IPSec (PMI)	Yes	Yes
Chassis cluster	Yes	Yes
GTP TEID based session distribution using Software RSS	No	Yes (Junos OS Release 19.3R1 onwards)
On-device antivirus scan engine (Avira)	No	Yes (Junos OS Release 19.4R1 onwards)
LLDP	Yes	Yes (Junos OS Release 21.1R1 onwards)
Junos Telemetry Interface	Yes	Yes (Junos OS Release 20.3R1 onwards)
System Requirements		
Hardware acceleration/enabled VMX CPU flag in the hypervisor	Yes	No
Disk space	16 GB	18 GB

Table 8: vNIC Support in vSRX2.0 and vSRX3.0

vNICs	Supported On	vSRX2.0	vSRX3.0
VMXNET3 SA and HA	VMware	Yes	Yes
Virtio SA and HA	KVM	Yes	Yes
SR-IOV SA and HA over Intel 82599/X520 series	VMware and KVM	Yes	Yes
SR-IOV SA and HA over Intel X710/XL710/XXV710 series	VMware and KVM	Yes	Yes
SR-IOV SA over Intel E810 series	VMware and KVM	Yes	Yes
SR-IOV HA over Intel E810 series	VMware and KVM	No	No
SR-IOV SA and HA over Mellanox ConnectX-3	VMware and KVM	No	No
SR-IOV SA and HA over Mellanox ConnectX-4/5/6 (MLX5 driver only)	VMware	Yes	Yes (SA from Junos OS Release 21.2R1 onwards) (HA from Junos OS Release 21.2R2 onwards)
SR-IOV SA and HA over Mellanox ConnectX-4/5/6 (MLX5 driver only)	KVM	Yes	Yes (Junos OS Release 21.2R1 onwards)
PCI passthrough over Intel 82599/X520 series	VMware and KVM	No	No
PCI passthrough over Intel X710/XL710 series	VMware and KVM	Yes	No

License Requirements for vSRX3.0

Starting in Junos OS Release 21.1R1, we've transitioned to the Flex Software subscription licensing model for SRX Series and vSRX3.0. We now use Juniper Agile Licensing to support soft enforcement for virtual CPU (vCPU) usage on vSRX. Juniper Agile Licensing provides simplified and centralized license administration and deployment.

Junos OS Releases prior to 21.1 use licenses from a legacy Licensing Management System (LMS). If you apply the same license on vSRX3.0 with Junos OS 21.1 or later releases, the license expires after a grace period of 30 days. You must obtain a new license with Juniper Agile Licensing (JAL) portal (<https://license.juniper.net/licensemanage/>).

If you upgrade from vSRX2.0 (any Junos OS release) to vSRX3.0 (Junos OS Release 21.1 or higher), you must get a new license key. You can revoke the current license key and generate a new one for the higher Junos OS release. See [Knowledge Base Article](#) for details.

Figure 3 on page 35 summarizes license requirements for different upgrade scenarios.

Figure 3: License Requirements for vSRX3.0

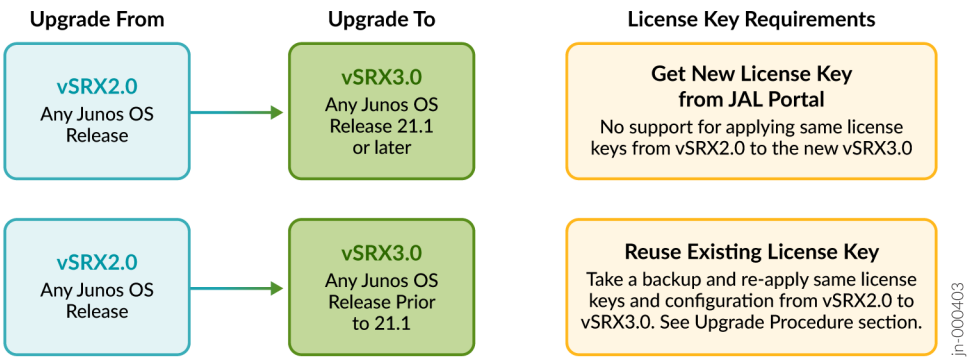


Table 9: License Requirements for vSRX3.0

Upgrade From	Upgrade To	Changes in License Keys
vSRX2.0 with any Junos OS Release	vSRX3.0 with Junos OS Releases 21.1 or later releases (21.1, 21.2, 21.3, 21.4, 22.1 and later releases)	Get a new license with Juniper Agile Licensing (JAL) portal (https://license.juniper.net/licensemanage/). See Release Notes: Junos OS Release 21.1R1 , Flex Software License for vSRX , and Licensing Guide for details. Ensure you specify the correct numbers of vCPUs in the license request.

Table 9: License Requirements for vSRX3.0 (*Continued*)

Upgrade From	Upgrade To	Changes in License Keys
vSRX2.0 with any Junos OS Release	vSRX3.0 with Junos OS Releases prior to 21.1 (18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 20.4)	<p>Re-use the existing license key with following steps:</p> <ul style="list-style-type: none"> • Take backup of license key and configuration file. • Install a new VM. • Reapply the license key and configuration file. <p>See "Migration Procedure" on page 38 in this topic.</p>

TIP: We recommend you upgrade to vSRX3.0 with Junos OS Release 21.1R1 or higher versions to avoid licensing issue when you do vSRX image upgrades in the future.

Migrate to vSRX3.0

IN THIS SECTION

- [Check vSRX Version | 36](#)
- [Pre-Migration Checklist | 37](#)
- [Migration Procedure | 38](#)
- [Post-Migration Tasks | 39](#)

You must deploy a new vSRX VM to migrate from the legacy vSRX2.0 to the new vSRX3.0. You do so by downloading a supported vSRX image from Juniper Support page and installing it on your server. Use the following steps to perform an upgrade:

Check vSRX Version

Check if your vSRX instance has vSRX2.0 or vSRX3.0 using the `show version` command:

Example-1

```
user@host-01> show version
Hostname: host-01
Model: vsrx
```

In the output, the field **Model: vsrx** with letters **srx** in lowercase represents vSRX2.0.

Example-2

```
user@host-01> show version
Hostname: host-01
Model: vSRX
Junos: 22.1R1.10
```

In the output, the field **Model: vSRX** with letters **SRX** in uppercase represents vSRX3.0.

Pre-Migration Checklist

Complete the following tasks before you migrate to vSRX3.0.

1. Check Junos OS version on your vSRX instance.

```
user@host-01> show version
Hostname: host-01
Model: vsrx
Junos: 19.4R3.1
```

The sample output indicates that your vSRX instance has Junos OS version 19.4R3 and with vSRX2.0.

2. Save the active configuration without any uncommitted changes.

```
user@host-01> show configuration | save /var/tmp/existingConfig.txt
Wrote 273 lines of output to '/var/tmp/existingConfig.txt'
```

The system saves the active configuration at the specified file location. Copy the saved file into your local workspace for later use.

3. Check your license requirements as per [Figure 3 on page 35](#). You might need a new license key, or you can re-apply the existing one.
 - If you require new license keys, obtain them from the Juniper Agile Licensing (JAL) portal (<https://license.juniper.net/licensemanage/>)

- If you can re-apply the existing license key, save a copy of license file using the following steps:
 - Display license keys installed on your vSRX from the operational mode:

```

user@host-01> show system license keys
DemolabJUNOS966777536 aeaqic beain4 vywmka bb3sxc zriaer ok4lgf
                        aattzl rmyuac ipfoft cqaj34 vywmka frembw
                        gaztem bsgiyd gmbzfv 4tkzcw hegbas tvnzux
                        azlseb ew45df ojxgc3 ahfbho wz2j2i fojb6m
                        z2jeif bwbm13 esqdkk dm4jxp j7o35h x6mvei
                        fd3sjp uubu3r udfzu

```

- Copy license keys or save license keys to a file or URL with the following command:

```

user@host-01> request system license save filename | url

```

4. Backup any other files on the vSRX2.0 VM, which you might require on the new vSRX3.0 VM (such as IPsec VPN certificates and scripts) (if applicable).
5. Ensure you have your server/host OS ready and setup the required virtual networks and storage pool in the host OS.
6. Power-off your vSRX2.0 VM before you start deploying the new vSRX3.0 VM.

Migration Procedure

Use the following steps to migrate from vSRX2.0 to vSRX3.0:

1. Navigate to the Juniper Networks Support page for the vSRX3.0 (<https://support.juniper.net/support/downloads/?p=vsrx3>) and select OS as vSRX3.0 and select the required versions shown in Figure 4 on page 39.

Figure 4: vSRX3.0 Download

Download Results for: VSRX 3.0

Select: OS **vSRX3.0** VERSION **21.2** SUPPORTING PLATFORMS **Show All** [Expand All](#)

Downloads Alerts

HIGH
Please refer to [KB37351](#) for important VCPU Scale licenses changes and messages in vSRX3.0 running Junos 21.1 and above.

Application Media 12 File(s)

Description	Release	File Date	Downloads
vSRX Hyper V Image	21.2R3	29 Mar 2022	vhd (1452.39MB) Checksums
vSRX KVM Appliance	21.2R3	29 Mar 2022	qcow2 (731.88MB) Checksums

2. Enter your credentials and review/accept the End User License Agreement. You'll be guided to the software image download page. Follow the instructions on the page and download the Junos OS image file.
3. Install the downloaded vSRX VM on your server.

When you download a vSRX3.0 image, the image file name includes **vsrx3**. Example: junos-install- vsrx3 - x86-64-21.2R3.8.tgz. See [vSRX Deployment Guide for Private and Public Cloud Platforms](#) for details on installation and launching of VM.

4. Check Junos OS and vSRX version after a reboot using the `show version` command.

```
user@host-01> show version
Hostname: host-01
Model: vSRX
Junos: 22.3R1.1
```

Post-Migration Tasks

Complete the following checks after you install new Junos OS with vSRX3.0.

1. Launch the new vSRX instance with vSRX3.0 on your server.

2. Enable network access (for example by configuring an IP address on the fxp0 interface). This step enables you to transfer files to the new vSRX3.0 VM.
3. Apply the license keys (the existing keys or new keys as per [Figure 3 on page 35](#)) on the newly launched vSRX instance.

```

user@host-01# request system license add terminal
[Type ^D at a new line to end input,
enter blank line between each license key]
DemolabJUNOS966777536 aeaqic beain4 vywmka bb3sxc zriaer ok4lgf
                        aattzl rmyuac ipfoft cqaj34 vywmka frembw
                        gaztem bsgiyd gmbzfv 4tkzcw hegbas tvnzux
                        azlseb ew45df ojxgc3 ahfbho wz2j2i fojb6m
                        z2jeif bwbml3 esqdkk dm4jxp j7o35h x6mvei
                        fd3sjp uubu3r udfzu
DemolabJUNOS966777536: successfully added
add license complete (no errors)

```

4. If you are using a chassis cluster setup, enable chassis cluster on the new vSRX3.0 using the `set chassis cluster cluster-id X node [0|1]` command and reboot VMs.
5. Transfer any other files that you have taken a backup from vSRX2.0 VM such as IPsec VPN certificates and scripts (If applicable).
6. Copy the config file you saved earlier back to the `/var/tmp` folder.
7. Run the **load override** `/var/tmp/existingConfig.txt` in the configuration mode to replace the current configuration with the saved configuration.

```

user@host-01# load override /var/tmp/existingConfig.txt
load complete

```

8. Commit the configuration.

```

user@host-01# commit

```

9. Ensure your device settings, network settings, and other configuration are available using the `show configuration` command.

What's Next?

Now that you have installed the new vSRX3.0, you can explore the new features and enhancements. See [Explore New Features Post Upgrade](#).

RELATED DOCUMENTATION

[Overview of the available virtual SRX models, vSRX and vSRX 3.0](#)
[Knowledge Base Article](#)

Start Using Unified Policies Post Upgrade

SUMMARY

Read this topic to understand how to get started using unified policies post upgrade to Junos OS Releases (19.4R3 or 20.2R3).

IN THIS SECTION

- [Unified Policies on SRX Series Devices Managed by Security Director | 41](#)
- [Unified Policies on SRX Series Devices | 44](#)

Starting in Junos OS Release 18.2R1, you can configure unified policies. When you configure a unified policy with a dynamic application as one of the matching conditions, the resulting configuration eliminates some of the additional steps required to configure application firewall (AppFW), IDP, and UTM configuration. See [An Introduction to Unified Policies for SRX-Series](#) video to learn about unified policies.

With introduction of unified policies in Junos OS Release 18.2, some of the commands are deprecated— rather than immediately removed—to provide backward compatibility. This enables you to bring your old configuration into compliance with the new configuration.

When you upgrade to Junos OS Releases 19.4R3 or 20.2R3, the security device displays the following warning when you try to commit the configuration that includes the deprecated commands:

```
# show security
application-firewall { ## Warning: 'application-firewall' is deprecated
```

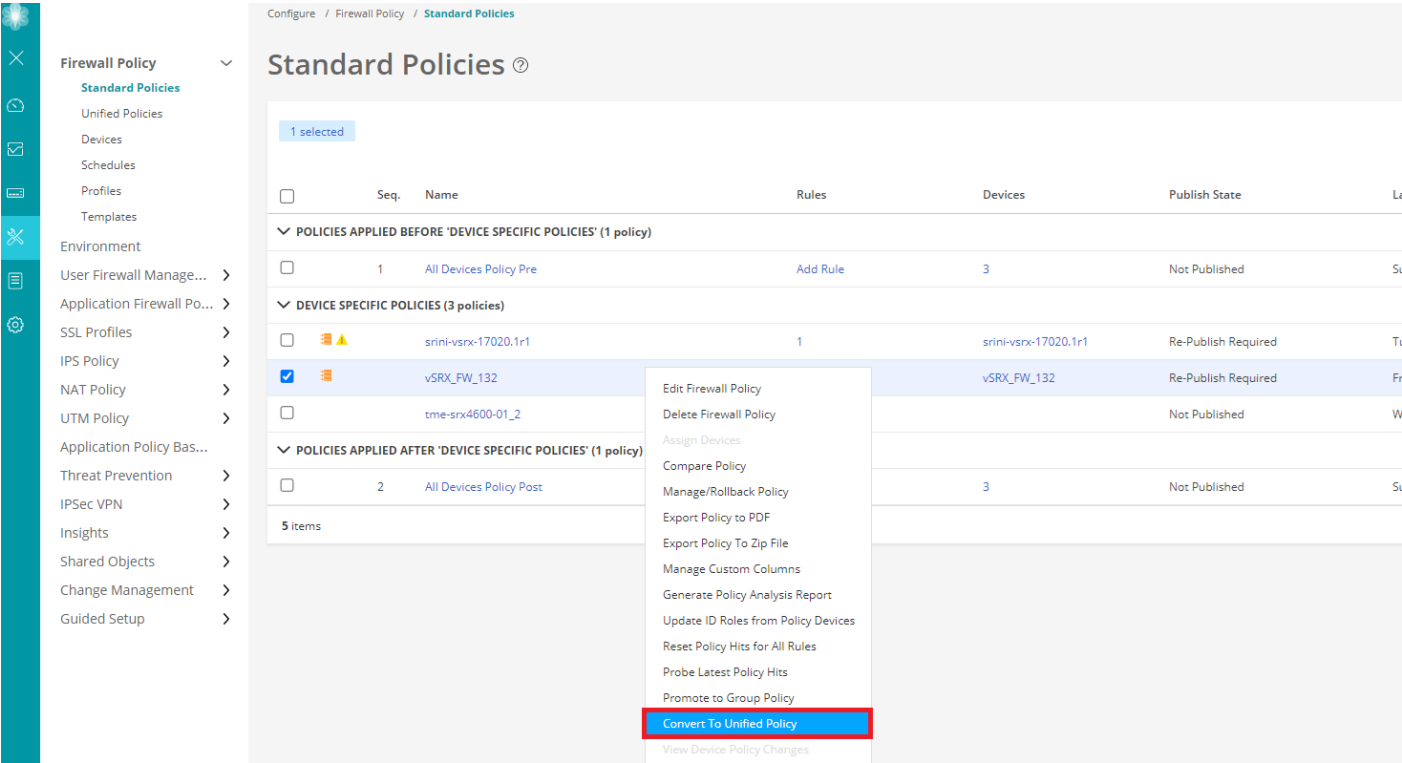
We recommend that you migrate to unified policies to bring your configuration up to date with supported features.

Unified Policies on SRX Series Devices Managed by Security Director

Security Director offers an easy migration tool which converts a traditional firewall policy to a unified policy. We recommend using Security Director Release 20.3 or later to convert a traditional security policy to a unified policy.

Figure 5 on page 42 shows the option available in Security Director that you can use to convert a security policy to a unified policy.

Figure 5: Security Director: Convert to Unified Policies



Example:

For more information about using the Security Director to aid with policy migration, see [\[Security Director\] Managing IDP, AppFW and UTM on SRX 18.2 and above with Security Director](#) and [In Focus Security Director](#).

You can use Security Director to quickly and accurately create policies as shown in the following examples:

To configure a unified policy, navigate to **Configure>Firewall Policy>Unified Policies** page.

The screenshot shows the 'policy-2 / Rules' configuration page. The left sidebar lists 'Firewall Policy' with sub-items: Standard Policies, Unified Policies (selected), Devices, Schedules, Profiles, Templates, Environment, User Firewall Mana..., Application Firewall..., SSL Profiles, IPS Policy, NAT Policy, UTM Policy, Application Policy B..., Threat Prevention, IPsec VPN, and Insights.

The main content area displays a table of rules for 'policy-2 / Rules'. The table has columns: Seq., Rule Name, Src. Zone, Dest. Zone, Action, Advanced Security, and URL Category. There are two sections: 'ZONE (2 Rules)' and 'GLOBAL (1 Rule)'.

Seq.	Rule Name	Src. Zone	Dest. Zone	Action	Advanced Security	URL Category
1	rule-allow-known-traffic	trust	untrust	Permit	-	-
2	check-known-http-traffic	trust	untrust	Permit	UTM wtf-policy IPS P...recommended	Facebook Commenting Facebook Events
1	block-unknown-traffic	untrust	Any	Deny	-	Media File Download Social Networking Mobile Malware

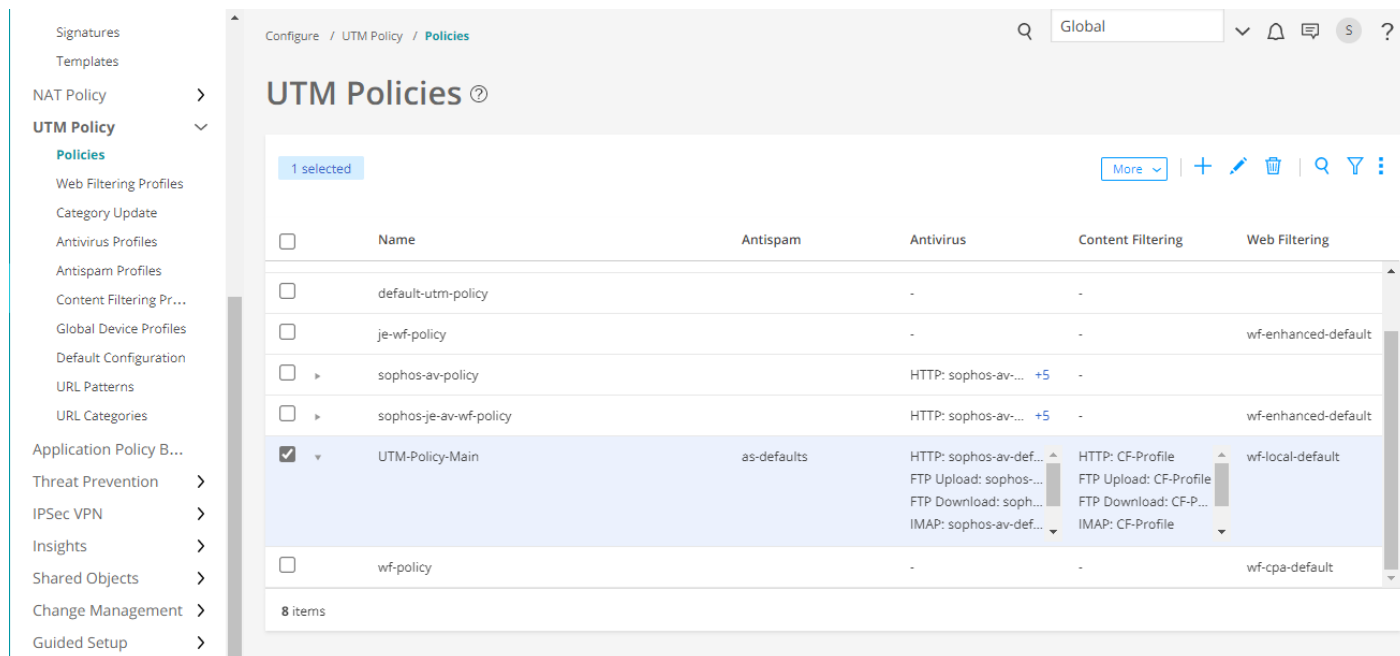
To configure an IPS policy, navigate to **Configure>IPS Policy>Policies** page.

The screenshot shows the 'IPS-Policy-Main / Rules' configuration page. The left sidebar lists 'Firewall Policy' with sub-items: Standard Policies, Unified Policies, Devices, Schedules, Profiles, Templates, Environment, User Firewall Mana..., Application Firewall..., SSL Profiles, IPS Policy (selected), Policies (selected), Devices, Signatures, and Templates.

The main content area displays a table of rules for 'IPS-Policy-Main / Rules'. The table has columns: Seq., Rule Name, Rule Type, Src. Zone, Dest. Zone, IPS Signature, Action, and IP Action. There are three rules listed.

Seq.	Rule Name	Rule Type	Src. Zone	Dest. Zone	IPS Signature	Action	IP Action
1	IPS-Policy-2	IPS	any	any	Additional Web Services - ...	Recommended	IP Action Target
2	IPS-Policy-3	IPS	any	any	All Attacks	Drop Connection	IP Action
3	IPS-Policy-1	IPS	any	any	Additional Web Services - ...	No Action	IP Action Target

To configure a UTM policy, navigate to **Configure>UTM Policy** page.



Unified Policies on SRX Series Devices

The following sections provide details about unsupported configurations in the older release and how you can enable them with the new release.

Application Security

Junos OS Release 15.1X49	Unified Policies (Post Junos OS Release 18.2)
<p>Configure individual application firewall rules to allow or reject traffic based on applications.</p> <ul style="list-style-type: none"> Configure rules and rule sets at the set security application-firewall hierarchy level. Apply application firewall functionality set security policies from-zone <zone> to-zone <zone> policy <policy> then permit application-services application-firewall rule-set. 	<p>Create security policies with dynamic applications as match criteria to get the same functionality as application firewall.</p> <pre>set security policies from-zone <zone> to-zone <zone> policy <policy> match dynamic-application <application-name></pre>

Example: The following samples show the difference in application firewall configuration with 15.1X49 and configuration in 19.4R3-S1 in unified policies. We're using an example of setting up application firewall rules to block Facebook applications.

Before Upgrade

```
set security policies from-zone untrust to-zone trust policy policy1 match source-address any
set security policies from-zone untrust to-zone trust policy policy1 match destination-address any
set security policies from-zone untrust to-zone trust policy policy1 match application junos-http
set security policies from-zone untrust to-zone trust policy policy1 then permit application-services
application-firewall rule-set rs1
set security application-firewall rule-sets rs1 rule r1 match dynamic-application [junos:FACEBOOK-ACCESS]
set security application-firewall rule-sets rs1 rule r1 then deny
set security application-firewall rule-sets rs1 default-rule permit
```

After Upgrade

```
set security policies from-zone trust to-zone untrust policy policy-1 match source-address any
set security policies from-zone trust to-zone untrust policy policy-1 match destination-address any
set security policies from-zone trust to-zone untrust policy policy-1 match application any
set security policies from-zone trust to-zone untrust policy policy-1 match dynamic-application junos:FACEBOOK-ACCESS
set security policies from-zone trust to-zone untrust policy policy-1 then reject profile profile1
```

IDP Policies

Junos OS Release 15.1X49	Unified Policies (Post Junos OS Release 18.2)
Assign an IDP policy as the active IDP policy and use it as match criteria in a security policy to perform intrusion detection and prevention.	Configure multiple IDP policies and apply them to the security policy. You can even define one of the IDP policies as the default policy.
<ul style="list-style-type: none"> Specify an active IDP policy: <pre>set security idp active-policy <IDP policy name></pre> Apply IDP policy in the security policy: <pre>set security policies from-zone <zone> to-zone <zone> policy <policy> then permit application-services idp</pre> 	<p>Specify multiple IDP policies per firewall rule:</p> <pre>set security policies from-zone <zone> to-zone <zone> policy <policy-1> then permit application-services <IDP-policy-name-1></pre> <pre>set security policies from-zone <zone> to-zone <zone> policy <policy-2> then permit application-services <IDP-policy-name-2></pre> <pre>set security idp default-policy <IDP-policy name></pre>

Example: The following samples show the difference in IDP configuration with 15.1X49 and configuration in 19.4R3 in unified policies. Note that, in unified policies, you have the flexibility to configure multiple IDP policies.

Before Upgrade

```
set security idp active-policy recommended
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 match source-address any
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 match destination-address any
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 match application junos:GMAIL
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 then permit application-services idp
```

After Upgrade

```
set security idp idp-policy recommended
set security idp idp-policy idpengine
set security idp default-policy recommended
set from-zone trust to-zone untrust policy P2 match source-address any
set from-zone trust to-zone untrust policy P2 match destination-address any
set from-zone trust to-zone untrust policy P2 match application junos-defaults
set from-zone trust to-zone untrust policy P2 match dynamic-application junos:GMAIL
set from-zone trust to-zone untrust policy P1 then permit application-services idp-policy recommended
set from-zone trust to-zone untrust policy P2 then permit application-services idp-policy idpengine
```

UTM

Junos OS Release 15.1X49	Unified Policies (Post Junos OS Release 18.2)
<p>Configure unified threat management (UTM) feature parameters under each feature profile.</p> <ul style="list-style-type: none"> • set security utm feature-profile anti-virus • set security utm feature-profile anti-spam • set security utm feature-profile web-filtering • set security utm feature-profile content-filtering 	<p>Configure UTM features under the default configuration. UTM default configuration applies parameters that you might have missed configuring for a specific UTM feature.</p> <ul style="list-style-type: none"> • set security utm default-configuration anti-virus • set security utm default-configuration anti-spam • set security utm default-configuration web-filtering • set security utm default-configuration content-filtering

Example: The following samples show the difference in UTM configuration with 15.1X49 and configuration in 19.4R3-S1 in unified policies. We're using an example of configuration of Sophos antivirus on your security device.

Before Upgrade

```
edit security utm feature-profile anti-virus mime-whitelist
```

```
edit security utm feature-profile anti-virus url-whitelist
edit security utm feature-profile anti-virus sophos-engine
```

After Upgrade

```
edit security utm default-configuration anti-virus mime-whitelist
edit security utm default-configuration anti-virus url-whitelist
edit security utm default-configuration anti-virus sophos-engine
```

For more information on configuring security features on your device, see [Product Documentation](#) and [Day One+](#).

What's Next

Now you are all set to explore new features and enhancements available with latest Junos OS Releases. See "[Explore New Features Post Upgrade](#)" on page 47.

Explore New Features Post Upgrade

SUMMARY

Read this topic to know about additional features available on your security device after you upgrade and access the links to start using them quickly and easily.

IN THIS SECTION

- [Simplified Configuration | 48](#)
- [Improved Security | 49](#)
- [SD-WAN Enhancements | 50](#)
- [Enhanced Reporting | 50](#)
- [Virtual and Container Firewall Features | 51](#)

Simplified Configuration

Feature	If You Want to	Go to
Dedicated management through the fxp0 interface (Junos OS Release 18.3R1)	Confine the management interface to a dedicated management instance in a non-default routing instance to improve security and make it easier to troubleshoot.	Management Interface in a Non-Default Instance
Junos telemetry interface (JTI) support for gRPC (Junos OS Release 19.2R1)	Use gRPCs in JTI to provision sensors and subscribe to receive telemetry data on your device.	Guidelines for gRPC and gNMI Sensors
HA mode wizard (Junos OS Release 19.2R1)	Use HA wizards to set up chassis cluster in a few steps using J-Web.	HA Mode Wizards
Juniper Agile Licensing (Junos OS Release 19.2R1)	Use Juniper Agile Licensing, a simplified and centralized license administration and deployment for your SRX Series.	Juniper Agile Licensing Guide Software Feature Licenses for SRX Series Devices
Multiple IDP policy support (Junos OS Release 18.3R1)	Have the flexibility to configure multiple IDP policies and set one of those policies as the default IDP policy on your device.	Understanding Multiple IDP Policies for Unified Policies
Packet captures from operational mode (Junos OS Release 19.3R1)	Execute the packet capture from the operational mode without committing the configurations.	Packet Capture from Operational Mode
Simplified VPN Configuration in J-Web (Junos OS Release 20.2R1)	Configure IPsec VPN in a few steps using J-Web.	About the IPsec VPN Page
SSL certificate management enhancements (Junos OS Release 19.2R1)	Easily manage the device certificates required for SSL.	Managing Device Certificates
SSL proxy troubleshooting commands (Junos OS Release 19.3R1)	Easily monitor SSL-related issues by using an extensive set of operational commands.	Operational Commands to Troubleshoot SSL Sessions

(Continued)

Feature	If You Want to	Go to
Tenant systems (Junos OS Release 18.3R1)	Reduce the number of physical devices and provide isolation and logical separation at the tenant system level.	Tenant Systems Overview
Unified policies (Junos OS Release 18.2R1)	Get greater control and extensibility to manage dynamic applications traffic within the security policy.	Unified Security Policies

Improved Security

Feature	If You Want to	Go to
Adaptive Threat Profiling (Junos OS Release 20.2R1)	Get your device ready to adapt to changing threats and network conditions with adaptive threat profiling.	Adaptive Threat Profiling
Express Path for SRX4600 devices (Junos OS Release 19.3R1)	Use Express Path functionality on SRX4600 devices for better throughput by reducing packet-processing latency.	Express Path
Symmetric fat tunnel support (Junos OS Release 19.4R1)	Get an improved IPsec tunnel throughput value—up to 10 times of current value—by using fat tunnel technology.	PMI Flow Based CoS functions for GTP-U
IDP sensor enhancements and intelligent inspection (Junos OS Release 19.2R1)	Use IDP sensor settings and IDP intelligent inspection to optimize system resource usage.	IDP Sensor Configuration
IDP signature language constructs (Junos OS Release 19.4R1)	Use signature language constructs to write more efficient signatures that helps in reducing false positives in IDP.	IDP Signature Language Enhancements
PowerMode IPsec (PMI) enhancements (Junos OS Release 19.1R1)	Enjoy the enhanced IPsec performance improvements using PMI.	Improving IPsec Performance with PowerMode IPsec

(Continued)

Feature	If You Want to	Go to
NP cache increase (Junos OS Release 20.2R1)	Experience an enhanced throughput with increased number of hash table entries for IOC3 and IOC4 on the SRX5000 line of devices and for IOC on the SRX4600.	Express Path
SSL performance enhancements (Junos OS Release 18.1R1)	Get enhanced SSL/TLS optimized for HTTPS traffic that results in improved website performance without compromising security, and maximizing user experience.	SSL Performance Enhancements
User Principal Name (UPN) support in JIMS and User Firewall Authentication (Junos OS Release 20.1R1)	Simplify the firewall authentication process by using UPN as the logon name	Understanding User Principal Name as User Identity in SRX Series Devices

SD-WAN Enhancements

Feature	If You Want to	Go to
Advanced policy-based routing (APBR) granularity enhancements (Junos OS Release 19.1R1)	Bypass the application services including security policies, application quality of service (AppQoS), Juniper ATP, IDP, Security Intelligence (SecIntel), and UTM using the APBR rule.	Bypassing Application Services in an APBR Rule
AppQoE enhancements (Junos OS Release 20.2R1)	Configure AppQoE for multihoming with active-active deployment.	Application Quality of Experience

Enhanced Reporting

Feature	If You Want to	Go to
Application identification enhancements for J-Web (Junos OS Release 18.1R1)	Use the enhanced Application Signature page to create, modify, clone, and delete application signature groups. You can view the details of predefined application signatures that are already downloaded.	About the Dynamic Applications Page
Dashboard enhancement (Junos OS Release 19.2R1)	View the Web filtering, Antispam, Content filtering, Application & Users, and Threat monitoring widgets in the J-Web dashboard for root, logical systems, and tenant users.	Monitoring the Dashboard
CLI enhancements to support J-Web (Junos OS Release 18.4R1)	Display alphabetical list application and application group, limit the number of entries in output, display details in a sorted order, and use filters on output columns to search applications easily in J-Web by configuring the show service application-identification command in CLI.	show services application-identification entries

Virtual and Container Firewall Features

Feature	If You Want to	Go to
vSRX 3.0 support (Junos OS Release 18.4R1)	Secure your private and public cloud environments with improved scalability and performance by using vSRX 3.0.	Overview of the available virtual SRX models, vSRX and vSRX 3.0
vSRX on Google Cloud Platform Marketplace (Junos OS Release 19.2R1)	Use the vSRX virtual firewall to extend your private cloud into public cloud environments, securely moving data and workloads with ease.	vSRX Deployment Guides

(Continued)

Feature	If You Want to	Go to
cSRX support (Junos OS Release 18.1R1)	Protect your containerized environments with advanced security services, including content security, intrusion prevention system (IPS), AppSecure, and unified threat management (UTM).	Building Containers with cSRX

What's Next

Now you can get started with configuring new features on your security device. See complete documentation at [TechLibrary](#). For additional references, see "[Appendix: Resources](#)" on page 52.

Appendix: Resources

SUMMARY

Read this topic to get additional details about Junos OS upgrade.

IN THIS SECTION

- [Additional References](#) | 52

Additional References

If you need more information on Junos OS upgrade, you can check out resources listed in the following table.

If Your Query Is About	See
Junos OS software support for features	Feature Explorer
Suggested Junos OS Release for the device	Junos Software Versions - Suggested Releases to Consider and Evaluate
Managing insufficient space on device during an upgrade	Verifying Available Disk Space on SRX Series Devices
Firmware Upgrade PoE	Understanding OS Upgrade versus Firmware Upgrade

(Continued)

If Your Query Is About	See
How to upgrade from Junos X version to Junos Y version?	"Know your Upgrade Paths" on page 11
How to handle if primary partition becomes corrupt?	How to Copy OS from Primary Partition to Secondary Partition if the Primary Partition is Corrupt
System outage during upgrade	Upgrading a Chassis Cluster Using In-Service Software Upgrade How to Upgrade an SRX Cluster with Minimal Down Time ISSU/ICU upgrade limitations on SRX firewalls
Licensing Information on SRX Series Devices	Flex Software License for SRX Series Devices
Configure advanced security features on SRX Series devices	Get Up and Running with Advanced Security Services
Hardening a Junos device and understanding the rationale for, and possible impact of, doing so.	<i>Hardening Junos Devices</i> at Day One Books
Get started with configuring security features.	Day One+

What's Next

Now you can get started with configuring new features on your security device. See complete documentation at [TechLibrary](#).