

# Upgrade to Junos OS Release for SRX Series

## IN THIS GUIDE

- [About this Guide | 1](#)
- [Why Upgrade Junos OS Releases | 2](#)
- [Upgrade to 21.2R3 | 5](#)
- [Upgrade to 19.4R3 | 40](#)
- [Migrate to vSRX3.0 | 69](#)
- [Start Using Unified Policies Post Upgrade | 82](#)
- [Appendix: Resources | 88](#)

## About this Guide

Use the guide to find an upgrade path and upgrade your SRX Series Firewalls to the newer version of supported Junos OS release.

### RELATED DOCUMENTATION

Know the Upgrade Path for Junos OS Release 19.4R3 and 20.2R3

Upgrade Path for Junos OS Release 21.2R3

# Why Upgrade Junos OS Releases

## SUMMARY

Read this topic to understand what you'll gain when you upgrade Junos OS Release on SRX Series Firewalls.

## IN THIS SECTION

- [Reasons for Considering an Upgrade | 2](#)
- [Important Reasons for Upgrading Junos OS Release | 3](#)
- [How Can You Get Started? | 4](#)
- [Where Can You Find More Information? | 5](#)

## Reasons for Considering an Upgrade

A newer version of the OS includes new features, enhancements, and bug fixes; many customers find the value of upgrading to a new version beneficial to their organization with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 Junos OS Release

In the rapidly changing era of mobile, cloud, and the Internet of Things (IoT) technologies, the legacy operating system 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 for upgrading Junos OS release:



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

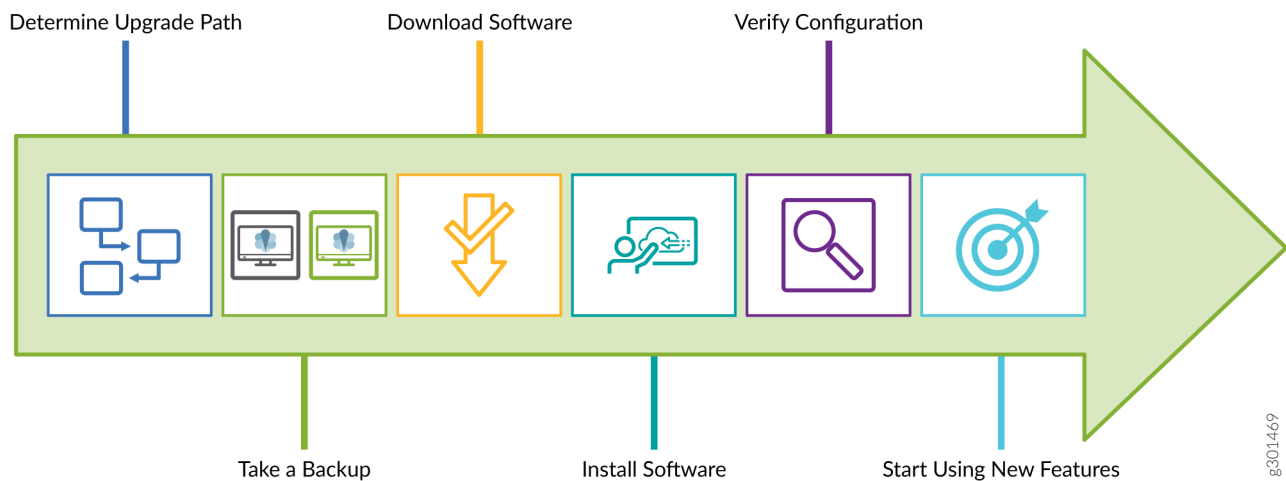


Regulatory and audit compliance requirements

# 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.

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 Firewalls in newer Junos OS releases.
- Learn about the upgrade paths available to migrate from your Junos OS Release .
- 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](mailto: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 [Release Notes](#).

# Upgrade to 21.2R3

## IN THIS SECTION

- [Key Features Through Junos OS Release 21.2R3 Upgrade | 5](#)
- [Upgrade Path for Junos OS Release 21.2R3 | 14](#)
- [How to Upgrade to Junos OS Release 21.2R3 | 17](#)
- [Explore New Features After Upgrading to Junos OS Release 21.2R3 | 32](#)

## Key Features Through Junos OS Release 21.2R3 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.

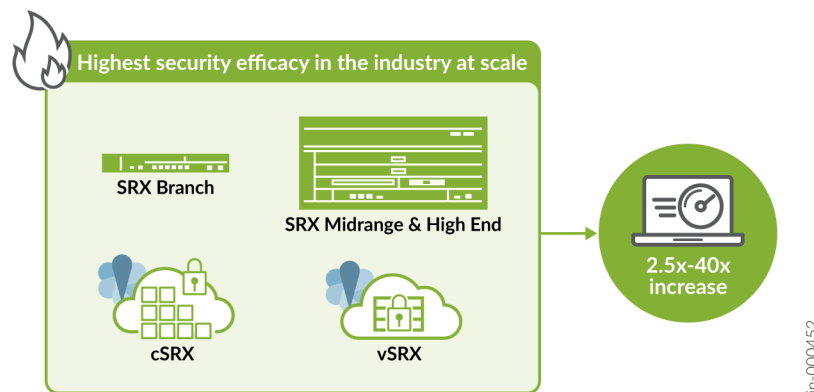
### IN THIS SECTION

- [General Performance and Efficiency Improvements | 6](#)
- [Express Path + | 7](#)
- [DNS Security | 8](#)
- [VXLAN Tunnel Inspection | 9](#)

- Improved Usability, Reporting, and Interoperability for IDP | 10
- Enhanced Security Reporting and IPsec Monitoring in J-Web | 11
- cSRX Container Firewall Support on AWS | 12
- NSX-T Integration with Security Director and vSRX Virtual Firewall for Service Chaining | 13

Between Junos OS releases 20.3R1 and 21.2R3, we've introduced many key security features. You can use these new features to provide policy-based awareness and control over applications, users, and content to stop advanced cyberthreats—all in a single device.

## General Performance and Efficiency Improvements



### What's This Feature About?

Provides holistic improvements to SRX Series Firewall performance and availability with built-in intelligence to better manage resources without user intervention. In addition, you can use validation checks to see which service plug-ins are interested in a flow session.

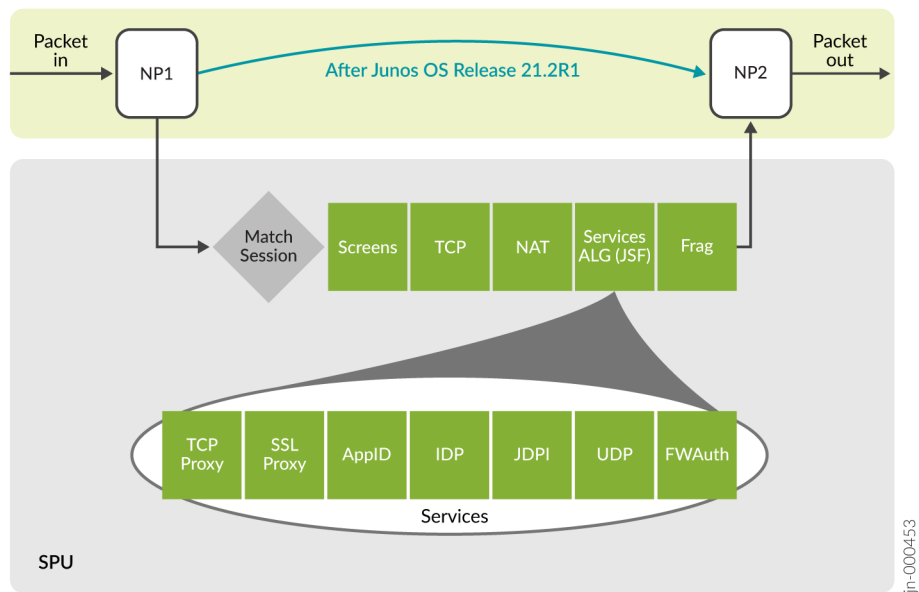
### Benefits

1.5 to 20 times performance improvement for next-generation firewall features without any additional configuration or hardware investment.

**Introduced in** Junos OS Release 20.4R1 and Junos OS Release 21.1R1 (validation checks).

**Want to know more?** See [show security flow session plugins](#).

## Express Path +



### What's This Feature About?

Provides automatic offloading of all eligible flows to the data-plane ASICs for line-rate forwarding without any additional configuration. Use Express Path+ to deliver full inspection services to all flows, regardless of size, as required across the network so you no longer need to choose between performance and security.

### Benefits

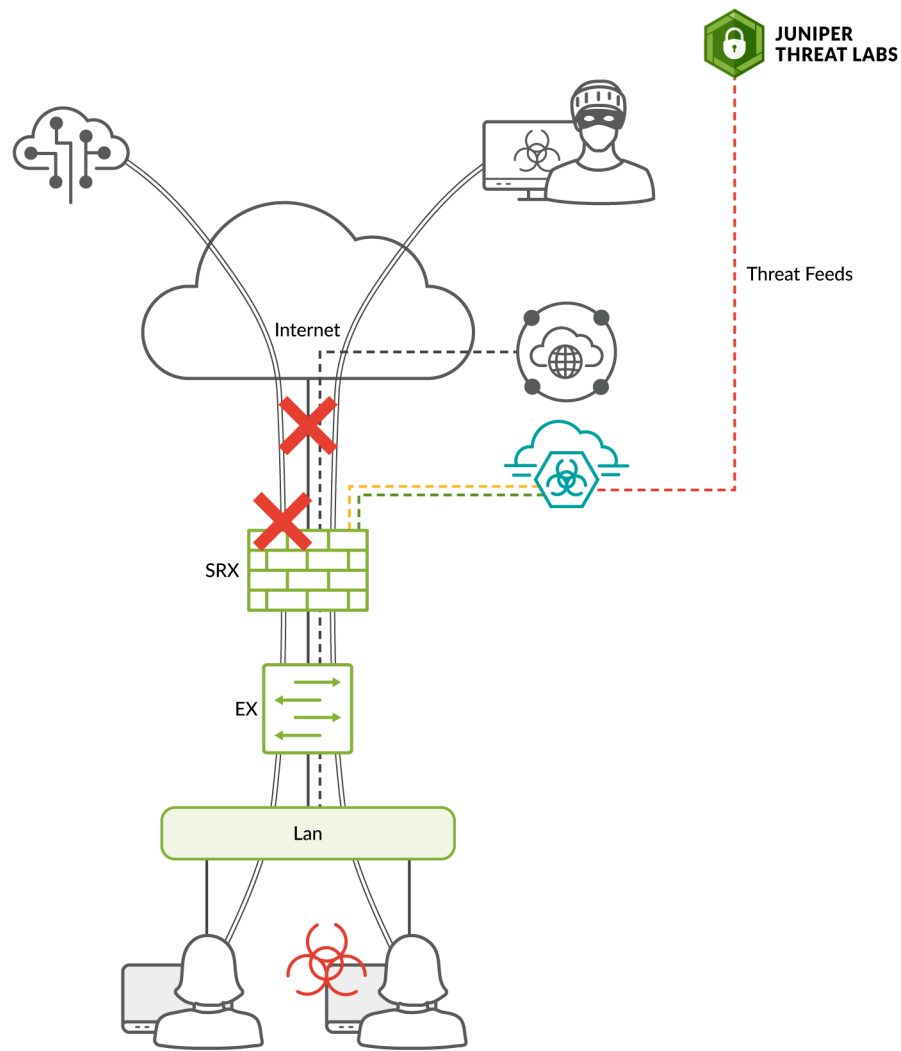
- Provides free, unparalleled next-generation firewall performance, without any additional configuration or hardware investments.
- Significantly improves UDP and TCP throughput, single-flow, and chassis-level performance while

**Introduced in** Junos OS Release 20.4R1.

Junos OS Release 20.4R1 supports manually defining what traffic to accelerate on a per policy configuration. Junos OS Release 21.2R1 adds the full automated and intelligent offload capabilities.

**Want to know more?** See [Automated Express Path](#).

## DNS Security



jn-000454

### What's This Feature About?

Protects against exploitation of critical DNS traffic in the network that can lead to misuse and compromises through filtering or sinkholing DNS requests from disallowed domains. This feature can be used with Domain Generation Algorithm (DGA) and DNS tunnel detection from ATP Cloud to identify and prevent compromised hosts from exploiting DNS traffic.

### Benefits:

- Prevents access to illegitimate domains and prevents infected hosts from contacting malicious servers by exploiting DNS. This includes protections against malicious activities such as:
  - DNS tunnels for obfuscation
  - Evasion techniques
  - Command and control (C&C) communication

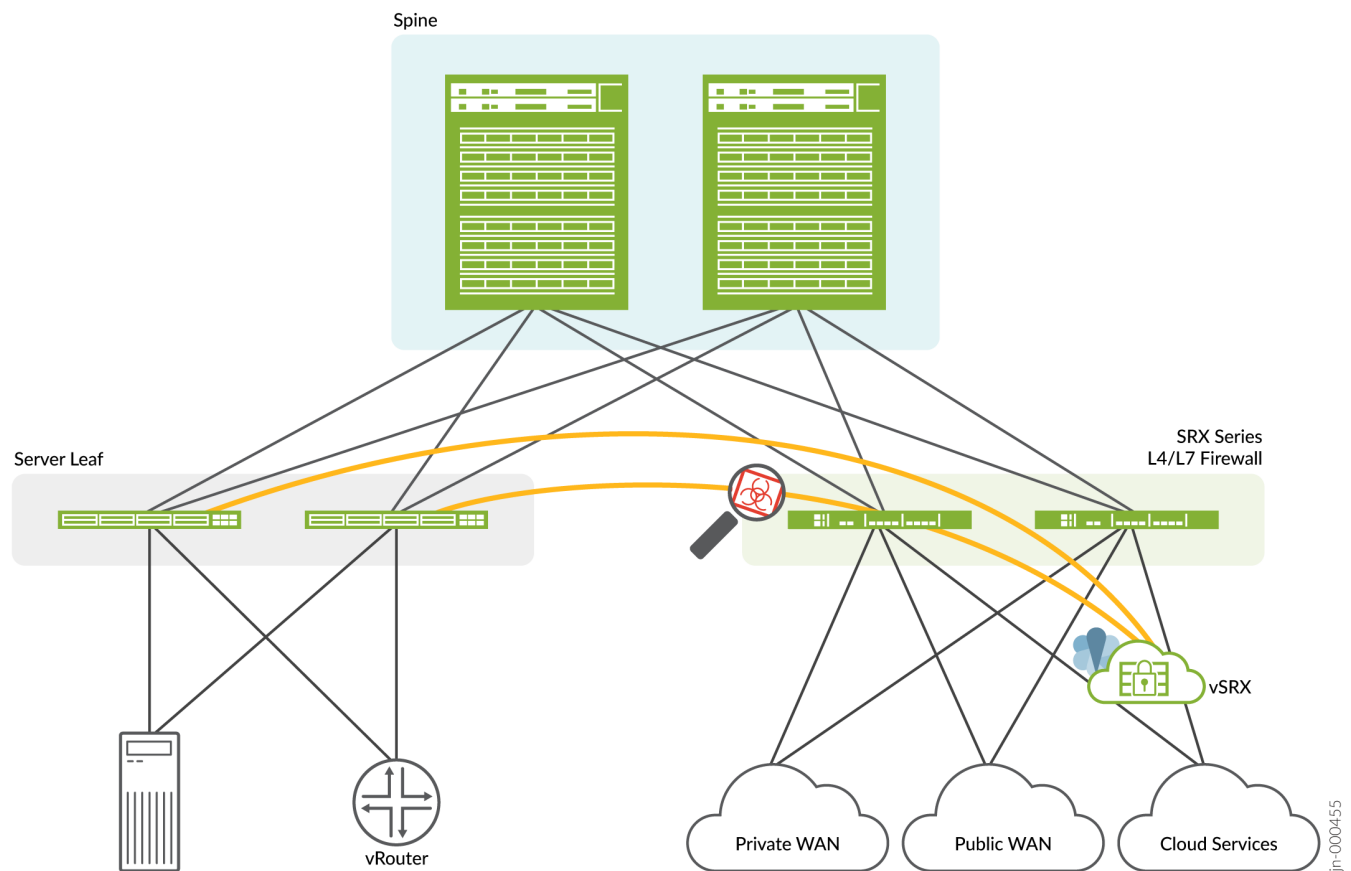


- Exfiltration of protected data
- Along with stopping malicious usage, this feature prevents applications that misuse DNS traffic to get around security mechanisms in place. The full set of features helps provide an overall improvement to your security posture by examining often trusted DNS traffic more closely.

**Introduced in:** Junos OS Release 20.4 (DNS filtering and sinkhole capabilities for the SRX Series) and Junos OS Release 21.2 (Additional functionality by ATP Cloud and the SRX Series for DGA detection and misuse of DNS tunneling detection).

**Want to know more?** See [DNS Sinkhole](#), [DNS DGA Detection Overview](#) and [DNS Tunnel Detection Overview](#).

## VXLAN Tunnel Inspection



### What's This Feature About?

Performs enhanced VXLAN tunnel inspection for encapsulated traffic by applying application-level security services such as application identification, IDP, content security, and Juniper Advanced Threat Prevention (ATP) to tunnel traffic. This feature provides better visibility of east-west traffic within a datacenters and public cloud environments.

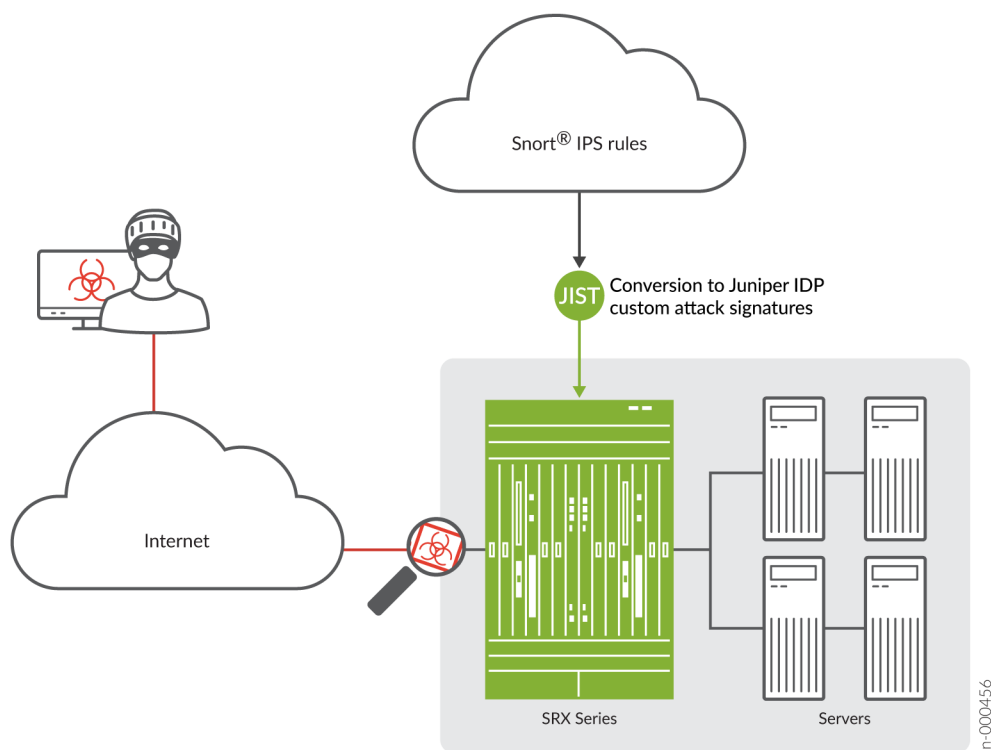
### Benefits

Supports collapsed architectures using industry-leading inspection services for secure flexible data center infrastructure and offers Layer 7 security services to inspect and to protect application workloads, users, and devices.

**Introduced in** Junos OS Release Junos OS Release 21.1R1.

**Want to know more?** See [Tunnel Inspection for EVPN-VXLAN by SRX Series Devices](#).

## Improved Usability, Reporting, and Interoperability for IDP



### What's This Feature About?

Captures packets before, during, and after an intrusion detection and transmits capture information to a host device (or to Security Director) for further analysis. Juniper Integration of Snort Tool (JIST) helps you convert Snort rules (v2 and v3) to Juniper IDP signatures.

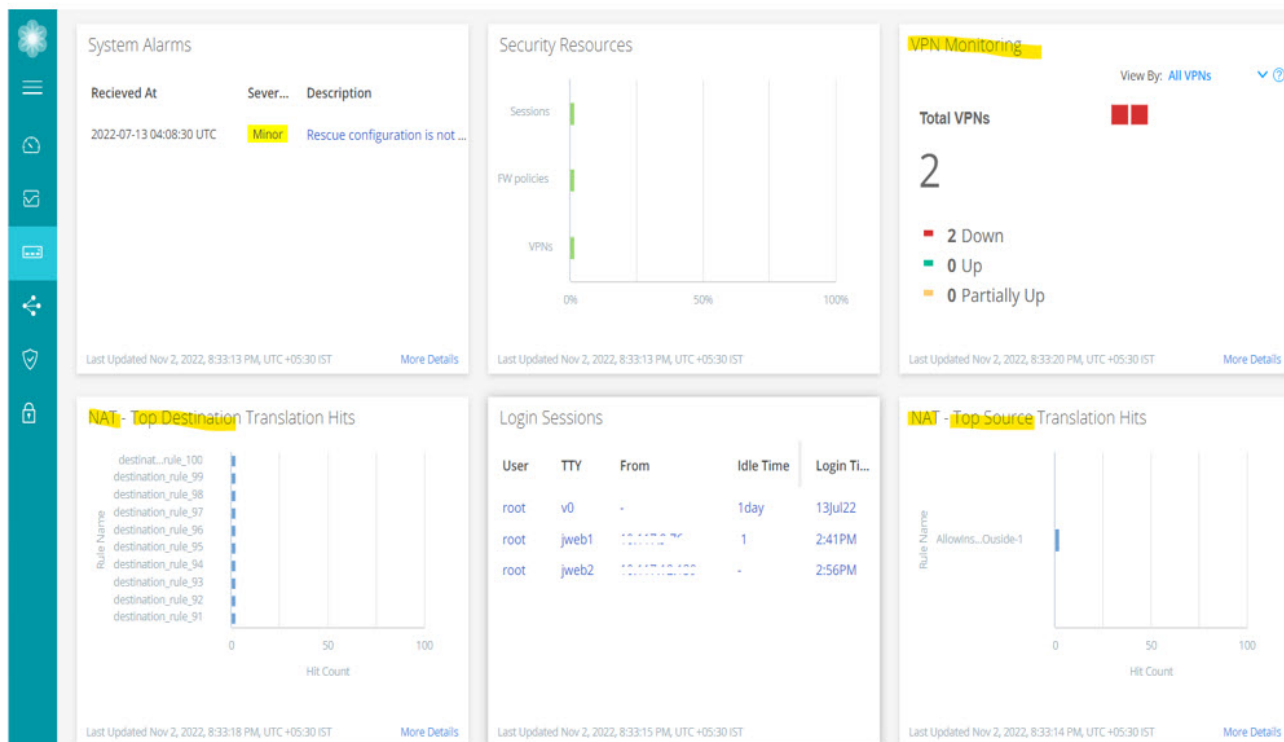
### Benefits

Improved usability and reporting with new PCAP analysis tool that can help you determine the purpose and extent of an attack, as well as conduct a postmortem to determine efficacy of triggered signatures. Snort signatures detect malicious activity using open-source intelligence that can be used in addition to Juniper IDP capabilities, providing better interoperability between tool sets across the network.

**Introduced in** Junos OS Release 20.4R1 for the PCAP analysis tool and Junos OS Release 21.1 the Juniper Integration of Snort Tool (JIST).

Want to know more? See [IDP utility to read PCAP and generate protocol](#) and [Understanding Snort IPS Signatures](#).

## Enhanced Security Reporting and IPsec Monitoring in J-Web



### What's This Feature About?

Provides updates to J-Web that enhanced security reporting with updates to the Threat Map, NAT top destination translations, source of threats for C&C and malware downloads, incidents by severity, and count of IPsec VPN IKE peers. Also includes refreshed Monitor and IPsec VPN pages with updates to interfaces and DHCP sever bindings, IPsec security associations (SAs), remote access reporting, and more.

### Benefits

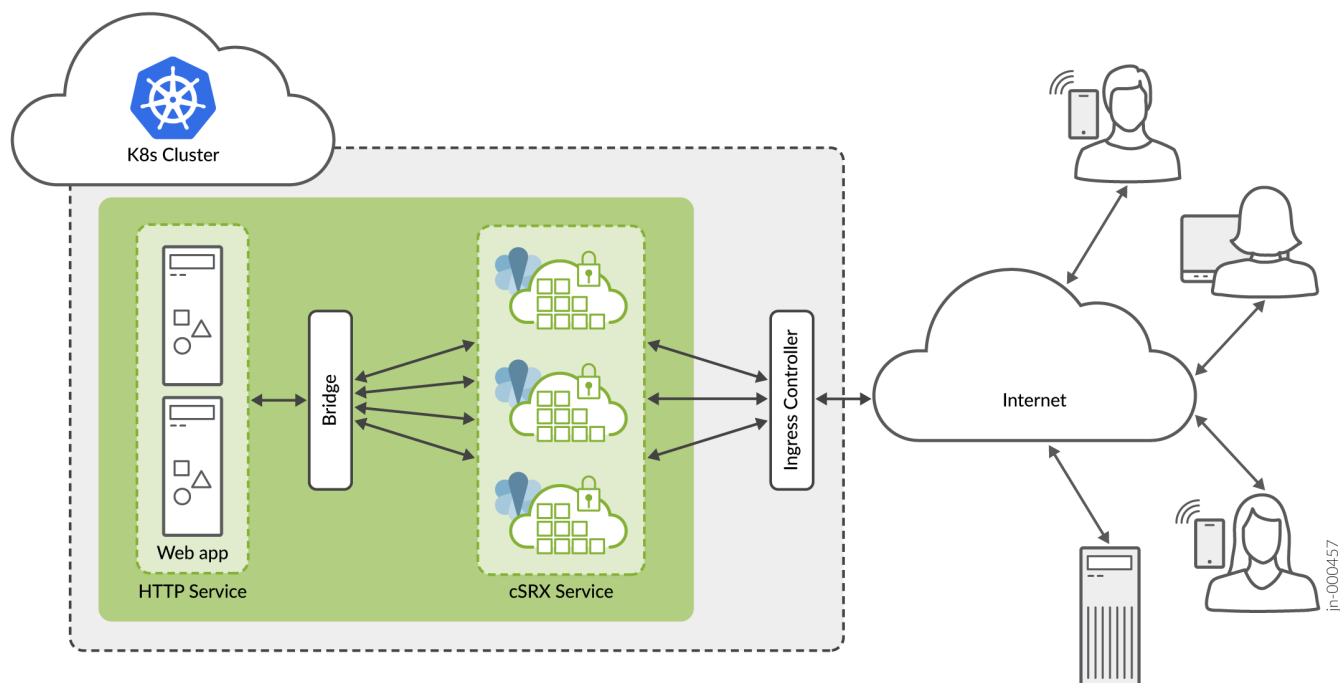
Enhanced visibility that helps you easily understand the threats on your network and the risk they pose. Overall better user experience with improved VPN monitoring and troubleshooting capabilities to diagnose and remediate VPN issues faster.

Provides better user experience with improved VPN monitoring and troubleshooting capabilities.

**Introduced in:** Junos OS Release 21.2R1.

Want to know more? See [Monitor IPsec VPN](#).

## cSRX Container Firewall Support on AWS



### What's This Feature About?

Deploy cSRX Container Firewall in AWS Cloud using Amazon Elastic Kubernetes Service (EKS), which is a fully managed Kubernetes service. You can use cSRX Container Firewall in Amazon EKS to set up automated service provisioning and orchestration for distributed and multitenant traffic security with centralized management through Security Director.

### Benefits

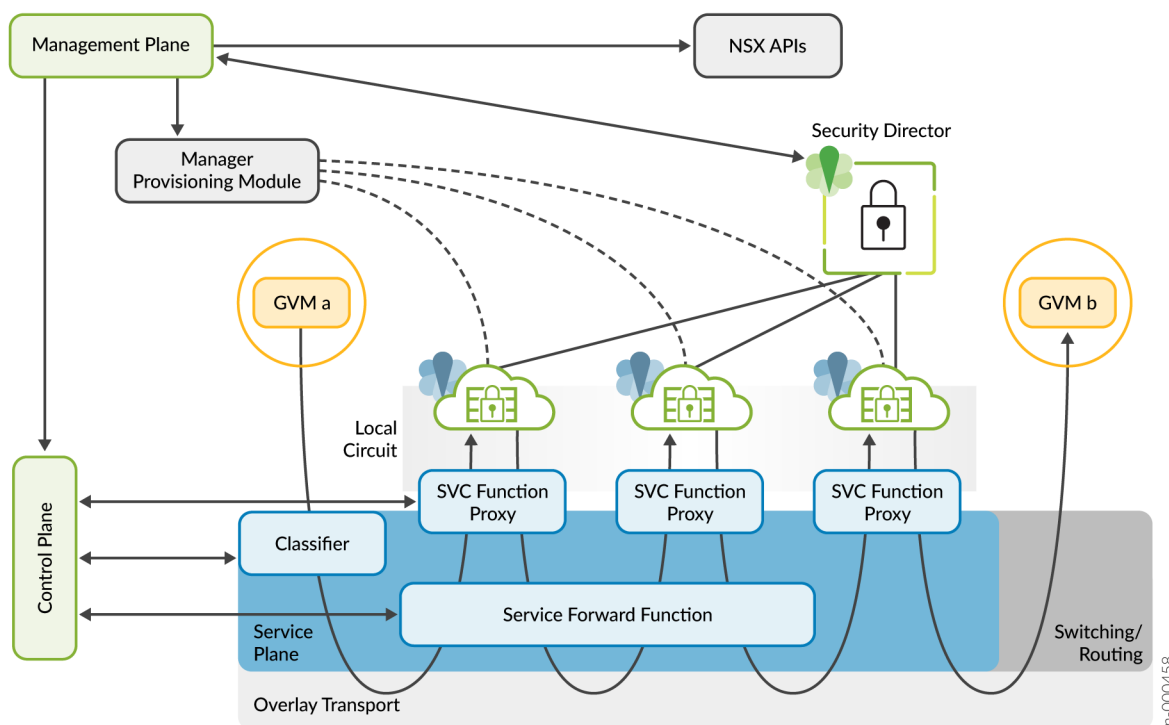
This feature helps to protect Amazon Web Services (AWS) workloads from external threats incoming from the Internet (north-south) with dynamic scale-up and scale-down of the cSRX Container Firewall, so security scales as your applications do. It also provides zero trust network access between applications' traffic (east-west) can be enforced through the cSRX Container Firewall for applications running in an overlay network in EKS.

Now deployments support dynamic scale-up and scale-down of cSRX Container Firewall based on predefined limits and the Horizontal Pod Autoscaler in Kubernetes. Also, centralized policy management for all applications as well as visibility between public cloud and private cloud environments is made easier through Security Director.

**Introduced in** Junos OS Release 21.2R1.

**Want to know more?** See [Understanding cSRX Deployment in AWS using Elastic Kubernetes Service \(EKS\)](#) and [How to Enhance Protection of AWS Workloads with the Juniper cSRX Container Firewall in Amazon EKS](#).

## NSX-T Integration with Security Director and vSRX Virtual Firewall for Service Chaining



### What's this?

Brings together vSRX Virtual Firewall and Security Director at the NSX Edge Gateway to protect and monitor both north-south and east-west network traffic. The solution provides best-in-class advanced threat protection with industry leading security efficacy and performance leveraging the vSRX Virtual Firewall for data center and cloud environments using NSX-T. Also provides simplified and automated security operations through orchestrating the solution through Security Director.

### Benefits

Offers true hybrid mesh security with a single policy set for both physical and virtual security devices from edge to cloud. Zero-trust network access with microsegmentation to protect against lateral threats at scale through the use of service chaining.

**Introduced in** Junos OS Release 21.2R1.

**Want to know more?** See [Understanding Juniper Connected Security for VMware NSX-T Integration](#).

## Upgrade Path for Junos OS Release 21.2R3

### SUMMARY

Read this topic to determine the upgrade path for Junos OS releases for your Juniper Networks SRX Series Firewall, vSRX Virtual Firewall Virtual Firewall, and cSRX Container Firewall Container Firewall.

### IN THIS SECTION

- [Upgrade Path for Your SRX Series Firewalls | 14](#)
- [Downgrading Junos OS | 16](#)

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

[Table 1 on page 14](#) shows the Junos OS release to which you can consider upgrading your SRX Series Firewalls and vSRX Virtual Firewall and cSRX Container Firewall instances.

**Table 1: Junos OS Release for SRX Series**

Devices	Junos OS Release
SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800	21.2R3
vSRX Virtual Firewall and cSRX Container Firewall	21.2R3

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 the following Knowledge Base articles.

- [Junos Software Versions - Suggested Releases to Consider and Evaluate](#)
- [Junos Upgrade Paths for SRX Platforms](#)

## Upgrade Path for Your SRX Series Firewalls

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

### Direct Upgrade

We support direct upgrade for selected Junos OS releases. [Table 2 on page 15](#) lists the direct upgrade paths supported for SRX Series Firewalls.

**Table 2: Direct Upgrade Paths for Junos OS Release**

Current Junos OS Release	Direct Upgrade Releases
15.1X49	19.4R3 Service release
18.4R3 or 18.4R3 Service release	19.4R3 or 19.4R3 Service release
19.4R3	20.4R3
20.4R3	21.2R3

### Interim Upgrade Path for Junos OS Releases 19.4R3 and 21.2R3

Use [Table 3 on page 15](#) and [Table 4 on page 16](#) 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 21.2R3

Junos OS Release	Target Junos OS (First Hop)	Target Junos OS (Second Hop)	Target Junos OS (Third Hop)
15.1X49	19.4R3	20.4R3	21.2R3
19.4R3	20.4R3	21.2R3	—
20.1	20.4	21.2R3	—
20.2	21.2R3	—	—
20.3	21.2R3	—	—
20.4	21.2R3	—	—
21.1	21.2R3	—	—
21.2	21.2R3	—	—

**Examples of Direct and Interim Upgrades:****To Upgrade from Junos OS Release**

15.1X49-D170 to 19.4R3

19.4

20.4

17.3 to 19.4R3

18.2 to 21.2

19.4 to 21.2

**Use This Path**

15.1X49-D170 → 19.4R3 (direct upgrade)

19.4R3 → 20.4R3 (direct upgrade)

20.4R3 → 21.2R3 (direct upgrade)

17.4R3 → 18.2 R3 → 18.4R3 → 19.4R3 (interim upgrade)

18.2R3 → 18.4R3 → 19.4R3 → 20.4R3 → 21.2R3 (interim upgrade)

19.4R3 → 20.4R3 → 21.2R3 (interim upgrade)

## Downgrading Junos OS

We support downgrades to up to three Junos OS releases at a time. You can downgrade to the Junos OS release that immediately precedes the current Junos OS release or to three Junos OS releases before the current release. For example, you can downgrade directly from Junos OS Release 20.2R1 to Junos OS Release 19.4R3. If you want to downgrade from Release 20.2R1 to Release 18.4R1, you must first downgrade to Release 19.3R1 and then to Release 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 21.2R3" on page 17](#).



# How to Upgrade to Junos OS Release 21.2R3

## SUMMARY

In this topic, you'll learn how to upgrade Junos OS software to Release 21.2R3 on your Juniper Networks® SRX Series Firewall device. You'll also learn about the upgrade options available for your Juniper Networks® vSRX Virtual Firewall Virtual Firewall.

## IN THIS SECTION

- [Best Practices for Upgrading Junos OS | 17](#)
- [Perform Preinstallation Steps | 18](#)
- [Upgrade Directly on Your Standalone Security Device \(CLI\) | 19](#)
- [Upgrade Directly on Your Security Devices in a Chassis Cluster \(CLI\) | 24](#)
- [Upgrade Junos OS Using USB Flash Drive or J-Web | 25](#)
- [Upgrade Considerations for vSRX Virtual Firewall VM | 26](#)
- [Upgrade Considerations for Your cSRX Container Firewall Container Firewall | 26](#)
- [Upgrade Junos OS on SRX Series Firewalls Managed by Junos Space | 27](#)
- [Upgrade Junos OS on SRX Series Firewalls Managed by Juniper Security Director Cloud | 30](#)
- [Upgrade Junos OS on SRX Series Firewalls Managed by Juniper Sky™ Enterprise | 30](#)
- [After You Upgrade to Junos OS Release 21.2R3 | 31](#)

## Best Practices for Upgrading Junos OS

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

- Read the Release Notes for [Junos OS Release 21.2R3](#).
- Connect your laptop/computer to the SRX Series firewall through the console port if you are upgrading software using CLI (recommended).
- 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 that both nodes are online and have the same version of Junos OS if you have 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.

## Perform Preinstallation Steps

Ensure that you complete the following tasks before you perform the upgrade.

1. 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]
```

2. 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 that storage is available on the CompactFlash card and the hard disk.

3. Save the active configuration and license keys. You can create a file containing configuration or license key and save it using one of the following methods.

- Save it on external server (FTP, HTTP, or SCP) or your laptop (recommended). The following example shows saving active configuration on an external device using SCP.

```
user@host> show configuration | save
scp://username@host<:port>/url-path password $abc123;
```

- Save it on the local device. The following example shows saving active configuration on the device.

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

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

Similarly save license keys using the `user@host> request system license save filename` command and copy it to external device or store it locally.

4. Optionally, create copies of the software running on your device using the system snapshot feature. Having a snapshot of software helps you recover to a known, stable environment in case something goes wrong with the upgrade. See [Backing Up an Installation Using Snapshots](#).
5. Ensure that there are no uncommitted changes.
6. Remove the NTP configuration that has more than one source address.

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

7. Remove chassis cluster fabric interface disable or enable configuration in case you have configured that option.

Example:

```
user@host# delete interfaces fab0 fabric-options member-interfaces interface-name enable/disable
```

8. Check if your configuration includes the following Junos default applications and remove them.
  - GPRS tunneling protocol (GTP) applications: `Junos-gprs-gtp-c-tcp`, `Junos-gprs-gtp-c-tcp`, `Junos-gprs-gtp-u-tcp`
  - SSL-based dynamic-applications: `Junos:HTTPS`, `Junos:IMAPS`, `Junos:POP3S`, `Junos:SMTPS`

## Upgrade Directly on Your Standalone Security Device (CLI)

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

- Juniper Networks SRX300 Firewall
- Junos OS Release 20.4R3
- Available flash memory of 512 MB

To upgrade from Junos OS Release 20.4R3 to Junos OS Release 21.2R3:

1. Navigate to the Juniper Networks [Support](#) page for the SRX300 and select **Junos** as the OS and **21.2** as the version, as shown in [Figure 1 on page 20](#).

**Figure 1: Download Junos OS Software**

Select:	OS	Junos	VERSION	21.2	Expand All +
X Install Package 3 File(s)					
Description		Release	File Date	Downloads	
SRX300-Series		21.2R3	29 Mar 2022	tgz (395.91MB) <a href="#">Checksums</a>	
SRX300-Series		21.2R2	16 Nov 2021	tgz (395.66MB) <a href="#">Checksums</a>	
SRX300-Series		21.2R1	29 Jun 2021	tgz (395.52MB) <a href="#">Checksums</a>	

2. Click **tgz (395.91 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 on the page. Use one of the options to download the Junos OS image file:

- **To download the image directly on your security device, use the following URL:** You can download the software image directly on your security device. According to the instructions on the screen, copy the URL provided in the box. The URL string is copied to the clipboard. Use file copy command on your security device to download the image.

Example: To download the image directly on your security device, run the following command on your security device. .

```
user@host> file copy "https://cdn.juniper.net/software/junos/21.2R3/junos-srxsme-21.2R3.8.tgz?
SM_USER=user1&__gda__=1668673424_186d7e0a4d79868b8969441980071208" /var/tmp/junos-srxsme-21.2R3.8.tgz
```

Your security device downloads the image to the **/var/tmp/image-name** location. The image name in this example is *junos-srxsme-21.2R3.8.tgz*.

- **To download the image on your local host (local system such as laptop):** You can copy the software image from your local system to the security device using SCP or SFTP options.

Example : To use SCP to copy software image to your security device, run the following commands on your security device.

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

```

user@host%
user@host% cd /var/tmp
user@host% scp userabc@hostname:/path/junos-srxsme-21.2R3.8.tgz

```

In this procedure, we'll download the image directly on to the security device.

## 5. Verify MD5 checksums on a Junos installation 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
eedebg_bin_file
install/
junos-srxsme-21.2R3.8.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-srxsme-21.2R3.8.tgz
```

```
MD5 (/var/tmp/junos-srxsme-21.2R3.8.tgz) = 9ecf2a049d8f1da96305decccf94208d
```

### c. Go back to software download page and click the **Checksums** option for SRX300. Compare the MD5 checksum value displayed on the screen with MD5 hash output value you obtained from the CLI command output.

Figure 2: MD5 Checksum Value

Select: OS Junos VERSION 21.2 [Expand All](#) +

✕ Install Package 3 File(s)

Description	Release	File Date	Downloads
SRX300-Series	21.2R3	29 Mar 2022	<a href="#">tgz (395.91MB)</a> <a href="#">Checksums</a>
SRX300-Series	21.2R2	16 Nov 2021	<a href="#">tgz (395.66MB)</a> <a href="#">Checksums</a>

**Checksums** ✕

MD5 : 9ecf2a049d8f1da96305decccf94208d

SHA1 : 4b0f032d830a5905940ca658ab584a45720090e8

SHA256 : 1ef777147e281ea447c328a5a792b50f70d7128e5e3e200b792739970752d579

SHA512 : 0474d5ccbdbd1dcf939cfc0eda1ab582c83b7b65d5a1569228b25658fa088ffb20ff522c27d2  
 84dde507ad162ff6a62392a18e0bf8bf9409daafb8b2628b3183

- 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-srxsme-21.2R3.8.tgz
```

```
Checking compatibility with configuration
Initializing...
cp: /var/etc/extensions.allow: No such file or directory
cp: /var/db/certs/common/local/*: No such file or directory
cp: /var/db/certs/common/key-pair/*: No such file or directory
cp: /var/db/certs/common/certification-authority/*: No such file or directory
Verified manifest signed by PackageProductionECP256_2021 method ECDSA256+SHA256
Using /var/tmp/junos-srxsme-21.2R3.8.tgz
Checking junos requirements on /
Available space: 592690 require: 457024
Saving boot file package in /var/sw/pkg/junos-boot-srxsme-21.2R3.8.tgz
```

```
Verified manifest signed by PackageProductionECP256_2022 method ECDSA256+SHA256
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
```

**NOTE:**

request system software validate

**7. Install the image.**

```
user@host> request system software add /var/tmp/junos-srxsme-21.2R3.8.tgz no-copy
```

```
NOTICE: Validating configuration against /var/tmp/junos-srxmr-x86-64-21.2R3.8.tgz. NOTICE: Validating
configuration against junos-srxsme-21.2R3.8.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
Formatting alternate root (/dev/da0s1a)...
/dev/da0s1a: 588.2MB (1204616 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 147.06MB, 9412 blks, 18944 inodes.
super-block backups (for fsck -b #) at:
    32, 301216, 602400, 903584
saving package file in /var/sw/pkg ...
Checking compatibility with configuration
Initializing...
cp: /var/etc/extensions.allow: No such file or directory
cp: /var/db/certs/common/local/*: No such file or directory
cp: /var/db/certs/common/key-pair/*: No such file or directory
cp: /var/db/certs/common/certification-authority/*: No such file or directory
Verified manifest signed by PackageProductionECP256_2021 method ECDSA256+SHA256
Using junos-21.2R3.8 from /altroot/cf/packages/install-tmp/junos-21.2R3.8
Copying package ...
Verified manifest signed by PackageProductionECP256_2022 method ECDSA256+SHA256
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/altroot/cf/packages/install-tmp/junos-21.2R3.8' ...
Verified junos-boot-srxsme-21.2R3.8.tgz signed by PackageProductionECP256_2022 method ECDSA256+SHA256
Verified junos-srxsme-21.2R3.8-domestic signed by PackageProductionECP256_2022 method ECDSA256+SHA256
Verified manifest signed by PackageProductionECP256_2022 method ECDSA256+SHA256
JUNOS 21.2R3.8 will become active at next reboot
WARNING: A reboot is required to load this software correctly
WARNING:      Use the 'request system reboot' command
WARNING:      when software installation is complete
Saving state for rollback ...
```

## About Software Validation Options

Note the following when you upgrade Junos OS from the release 21.2 or earlier to the release 21.2 or later:

- SRX1500 device, SRX4000 line of devices, SRX5000 line of devices with RE3, and vSRX Virtual Firewall instances do not support software validation due to FreeBSD upgrade.
- Use the `no-validate` option in the `request system software upgrade` or the `request system software in-service-upgrade` commands.
- Use the `no-compatibility-check` option with the `request system software in-service-upgrade` command instead of `no-validate` option.

Check the Knowledge Base article [Need to use "no-validate" option](#) for more details.

**NOTE:** If you are upgrading an SRX5000-line firewall with RE3, you must use the "request vmhost software add" command.

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

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

- Juniper Networks SRX4200 Firewall devices in a chassis cluster setup
- Junos OS Release 20.4R3
- 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 chassis cluster fabric interface enable or disable configuration in case you have configured that option.

Example:

```
user@host# delete interfaces fab0 fabric-options member-interfaces interface-name enable/
disable
```

1. Download and validate the Junos OS Release 21.2R3 image. See Step 1 through Step 6 provided in "[Upgrade Directly on Your Standalone Security Device \(CLI\)](#)" on page 19 for details.
2. Install the Junos OS image on node 0.

```
{primary:node0}
```

```
user@host> request system software add /var/tmp/junos-srxmr-x86-64-21.2R3.8.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-x86-64-21.2R3.8.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 by using the `show version` command.

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

### IN THIS SECTION

- [USB Flash Drive | 25](#)
- [J-Web | 26](#)

## USB Flash Drive

You can use a USB flash drive to upgrade Junos OS images or recover an SRX Series Firewall after boot media corruption in cases where you don't have console access to an SRX Series Firewall. 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 Firewall in a few steps using J-Web. For more information, see [Install Software Packages](#).

## Upgrade Considerations for vSRX Virtual Firewall VM

If you consider upgrading Junos OS on your vSRX Virtual Firewall VM, note the following:

- We recommend that you deploy a new vSRX Virtual Firewall VM instead of performing a Junos OS upgrade. The new VM enables you to move from vSRX Virtual Firewall to the newer and more enhanced vSRX Virtual Firewall 3.0 version.
- Moving to the vSRX Virtual Firewall 3.0 software architecture offers many benefits including introduction to new services, delivering customized services, and scaling security services based on dynamic needs. Junos OS Release 18.4R1 and later releases support vSRX Virtual Firewall 3.0.
- See the KB article [Overview of the Available Virtual SRX Models, vSRX and vSRX 3.0](#) for more details on vSRX Virtual Firewall 3.0 support and "[Migrate to vSRX3.0](#)" on [page 69](#) for instructions on migrating to vSRX Virtual Firewall 3.0.

## Upgrade Considerations for Your cSRX Container Firewall Container Firewall

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

To upgrade cSRX Container Firewall, you must download the cSRX Container Firewall software image from the Juniper Networks website on your Docker environment and launch the new cSRX Container Firewall instance. For more information, see the following links:

- [Requirements for Deploying cSRX on a Bare-Metal Linux Server](#)
- [Installing cSRX in a Bare-Metal Linux Server](#)
- [Requirements for Deploying cSRX on Kubernetes](#)
- [cSRX Installation on Kubernetes](#)

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/Red Hat—<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/>

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

## Upgrade Junos OS on SRX Series Firewalls Managed by Junos Space

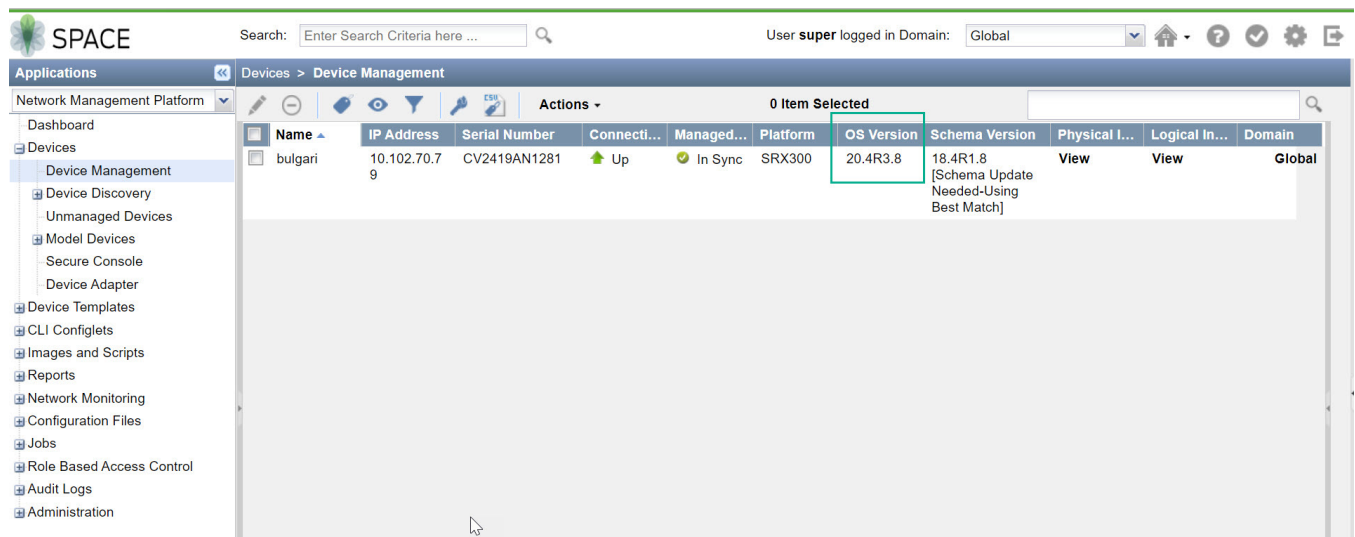
### SUMMARY

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.

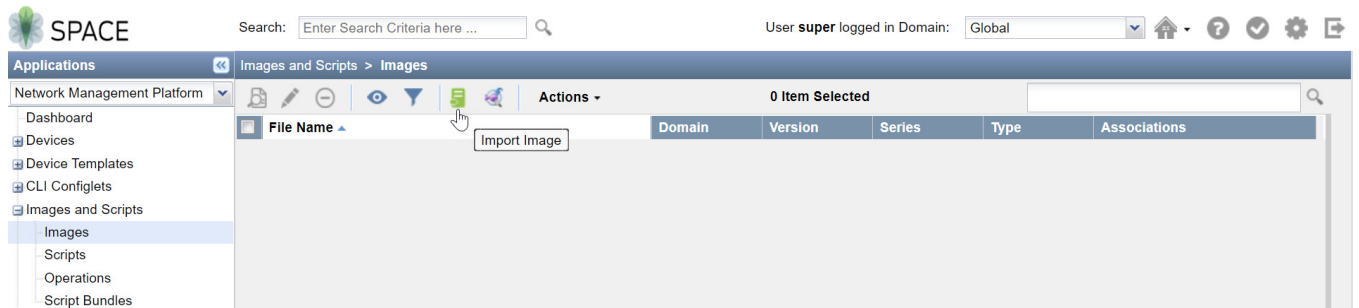
We'll use the following hardware and software combination in this example:

- Juniper Networks SRX300 Firewall managed by Security Director
- Junos OS Release 15.1X49-D170

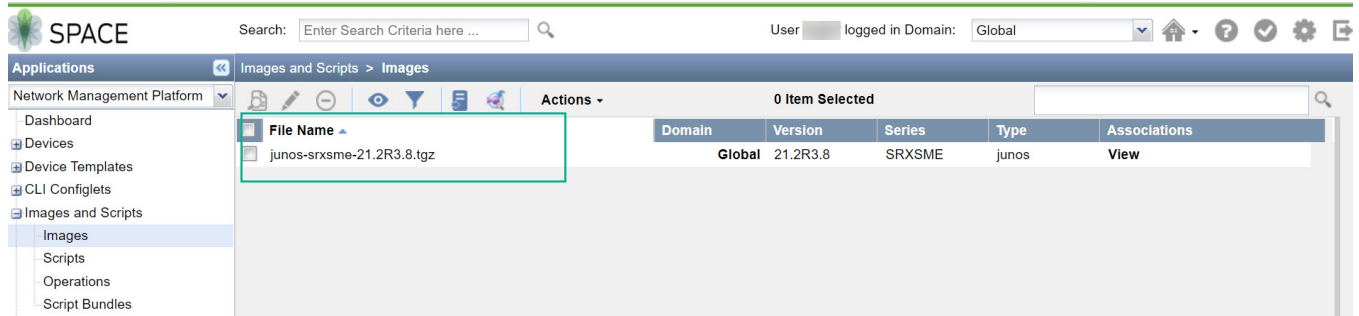
1. On the Network Management Platform GUI, select **Devices > Device Management**. The Device Management page appears.



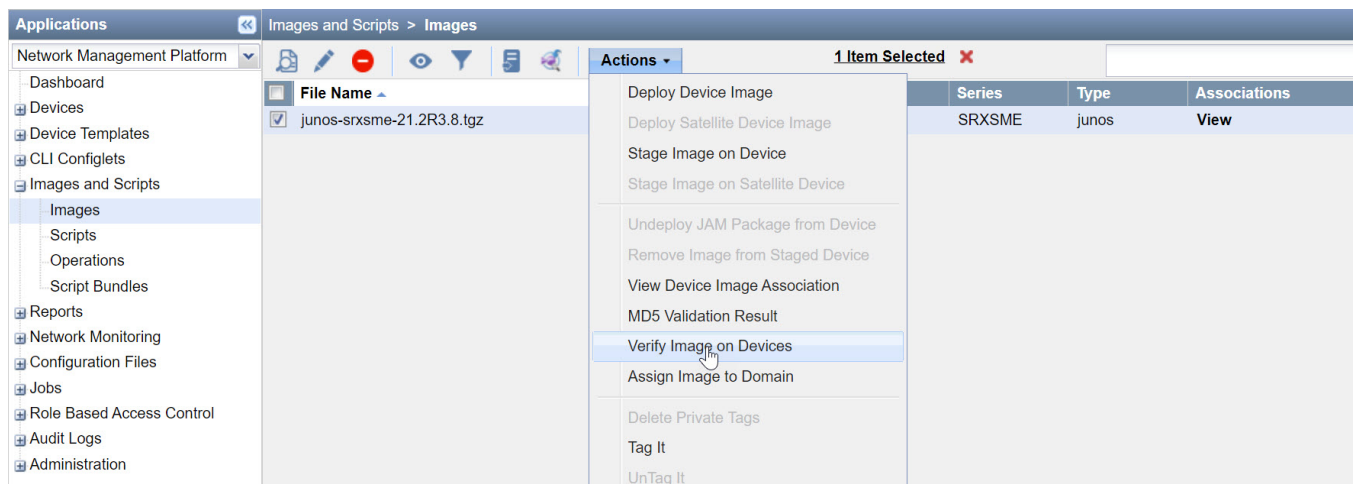
2. Check the operating system (OS) version running on the device.
3. Navigate to the Juniper Networks [Support](#) page and download Junos OS Release 21.2R3 and save the file to your computer. See "[Upgrade Directly on Your Security Device \(CLI\)](#)" on page 19 for instructions.
4. Go to **Images and Scripts** and select **Images**. Click the **Import Image** icon to upload the image file to Junos Space Platform.



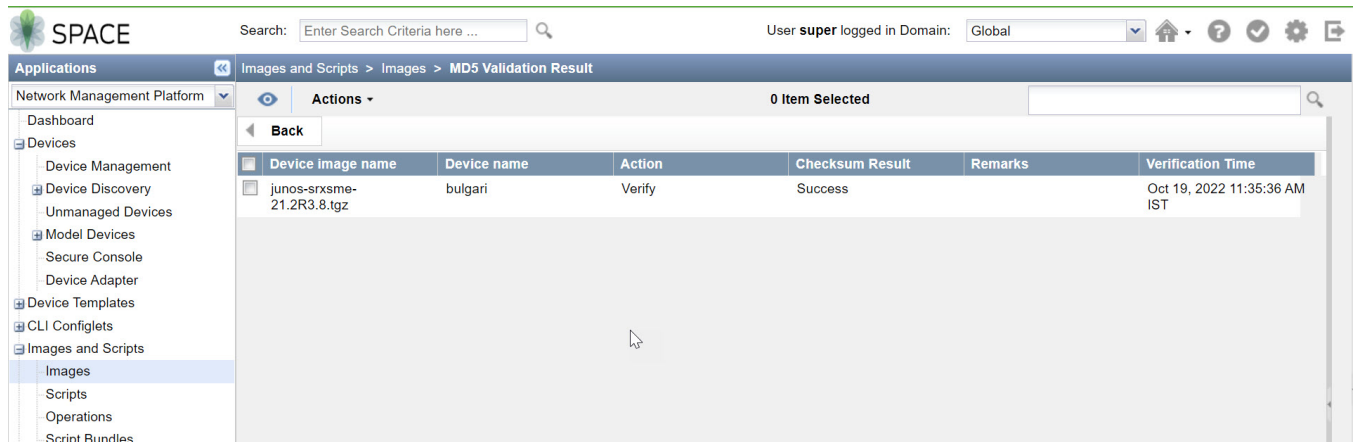
After the uploading of the image completes, the Images page displays the uploaded image under **File Name**.



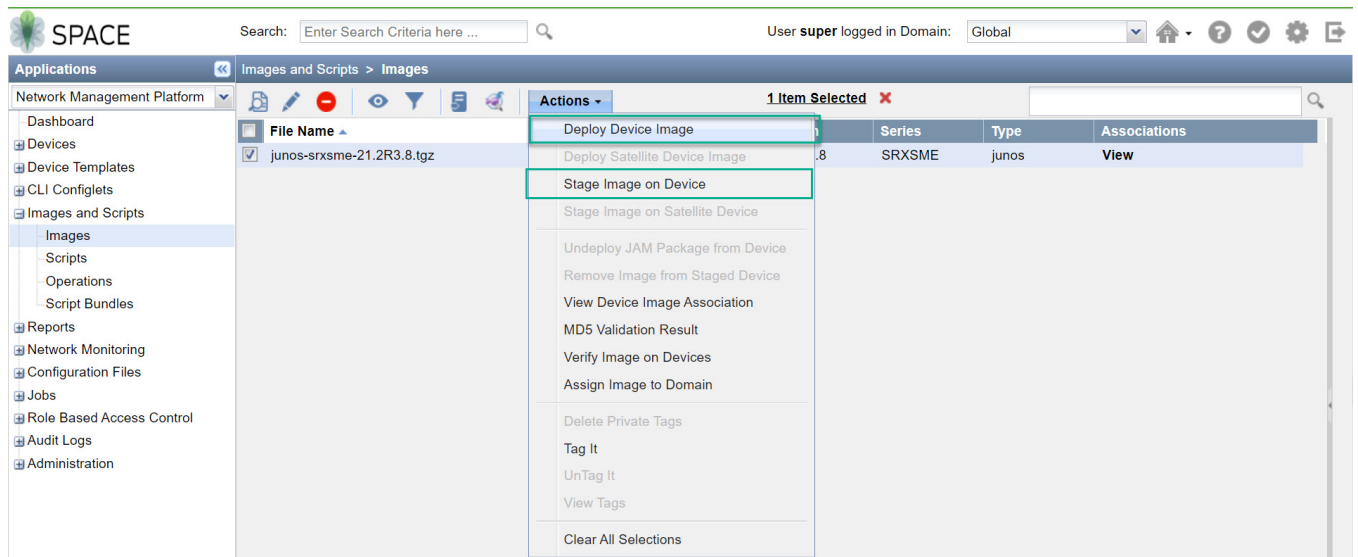
- Validate the image by selecting the **Actions > Verify Image on Device** option.



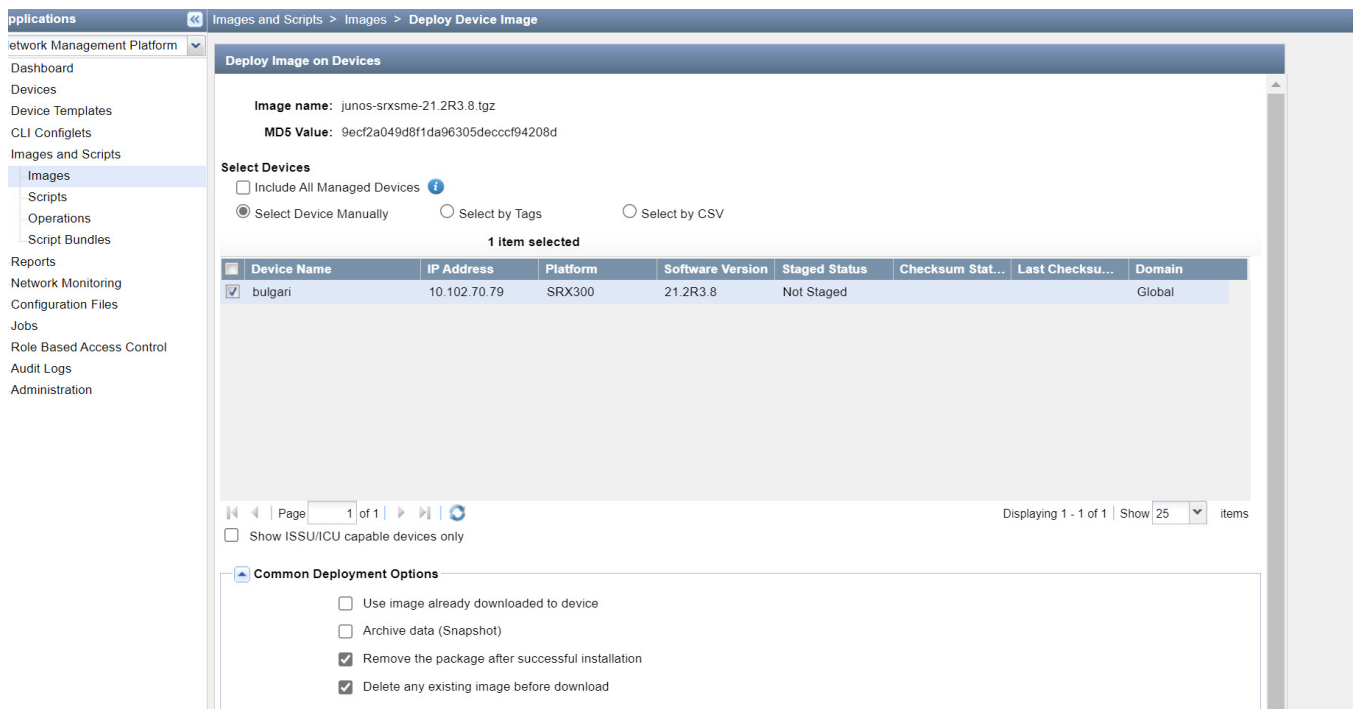
- Check the validation results by navigating to the **Images and Scripts > Images > MD5 Validation Result** page.



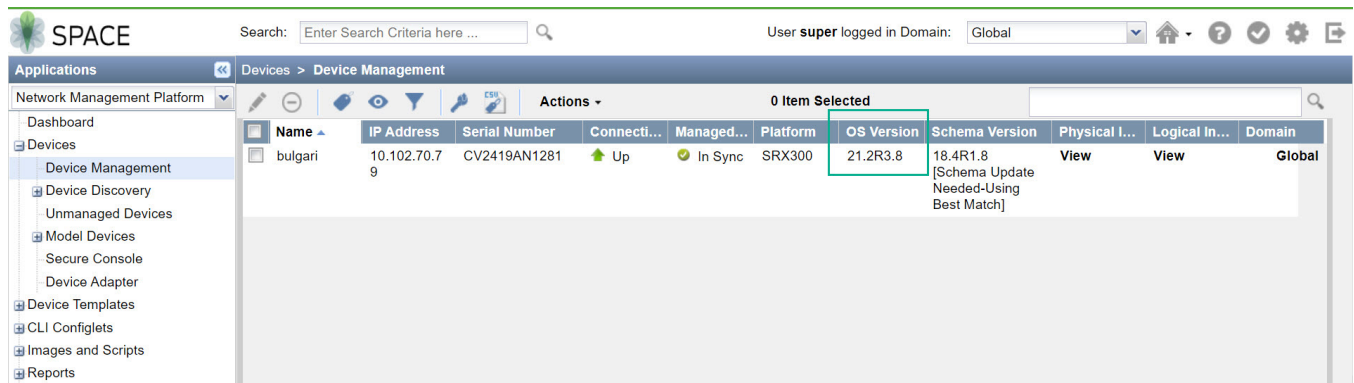
- Select the uploaded Junos OS image and choose the **Deploy Image** option from **Actions** menu. Alternatively, you can choose to stage the deployment at a later time by selecting the **Stage Image on Device** option.



8. On the **Deploy Image on Devices** page, select the device that you want to upgrade and specify the **Remove the package after successful installation** and **Delete any existing image before download** options.



9. Click **Deploy** to start installation. After the upgrade completes, you can check the software version on your device by navigating to the **Devices > Device Management** page. Here, the OS version now displays Junos OS Release 21.2R3.



10. Reboot the device after a successful installation.

## Upgrade Junos OS on SRX Series Firewalls Managed by Juniper Security Director Cloud

You can use Juniper Security Director Cloud to manage the software images running on SRX Series (both standalone and chassis clusters) and vSRX Virtual Firewall. Juniper Security Director Cloud helps you to manage (add, stage, deploy, and delete) the entire lifecycle of images of all managed network devices.

To perform the Junos OS upgrade on devices managed by security director cloud, go to **SRX > Device Management > Software images**.

- [Add an Image](#)
- [Stage an Image.](#)
- [Deploy an Image.](#)
- [Delete Images.](#)

When you need to upgrade or downgrade the image running on a device, you can add software images of devices, stage and deploy the required image on the device by using Juniper Security Director Cloud.

For more information, see [About the Images Page](#) of [Juniper Security Director Cloud User Guide](#).

## Upgrade Junos OS on SRX Series Firewalls 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 by using only a browser.

To perform the Junos OS upgrade on devices managed by Juniper Sky Enterprise:

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

Juniper 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 21.2R3

### IN THIS SECTION

- [Licensing Requirements](#) | 31

Perform the following steps after you upgrade to Junos OS Release 19.4R3 or to Junos OS Release 21.2R3.

- Copy the device configuration files back to the device. We recommend that you retain the configuration unless you are deploying a new vSRX Virtual Firewall VM.
- Download and install the latest intrusion detection and prevention (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 Release 15.1X49 to Junos OS 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 that passes through the device. You do this by configuring a GTP profile on all security policies that may carry GTP traffic. See [Example: Enabling GTP Inspection in Policies](#).
- Decide when you'd like to migrate to unified policies. See ["Start Using Unified Policies Post Upgrade" on page 82](#).

## Licensing Requirements

Starting in Junos OS Release 21.1R1, we've transitioned to the Flex Software Subscription Licensing Model for SRX Series Firewalls and vSRX Virtual Firewall. Junos OS Releases before Release 21.1 use licenses from a legacy Licensing Management System (LMS).

If you have legacy license keys and if you apply them when you upgrade to Junos OS Release 21.1, Release 21.2R3, or later releases, the license expires after a grace period of 30 days. You must purchase a new license using the Juniper Agile Licensing (JAL) portal. See [Flex Software License for SRX Series Devices](#) for details.

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.

## What's Next

Now that you've 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 82](#). Otherwise, learn about new features and enhancements that you can start using with your Junos OS. See ["Explore New Features Post Upgrade to Junos OS Release 19.4R3" on page 64](#).

## Explore New Features After Upgrading to Junos OS Release 21.2R3

### SUMMARY

Read this topic to know about the additional features available on your security device after you upgrade Junos OS. Access the links provided in this topic to start using the features quickly and easily.

### IN THIS SECTION

- [Simplified Configuration | 32](#)
- [Improved Security | 33](#)
- [Software-Defined WAN \(SD-WAN\) Enhancements | 35](#)
- [Enhanced Reporting | 36](#)
- [Virtual Firewall and Container Firewall Features | 38](#)

## Simplified Configuration

Feature	If You Want to	Go to
Listing of micro-applications (Junos OS Release 20.3)	Manage the applications at a sub-function level with the application identification feature.	<a href="#">Application Identification Support for Micro-Applications</a>
Application signature rollback (Junos OS Release 20.3)	Roll back the current version of the application signature pack to the previous version.	<a href="#">Application Signature Package Rollback</a>
Intrusion Detection and Prevention (IDP) packet capture analysis tool (Junos OS Release 20.4)	Display IDP context, hits, and associated data details for traffic that is generated by the packet capture feeder	<a href="#">IDP Utility for PCAP</a>
Tracing and debugging of packets (Junos OS Release 20.4)	Trace packet footprints captured in a sequential time order	<a href="#">traceoptions (Security Flow)</a>
Resource management enhancement (Junos OS Release 20.4)	Control whether to drop or to create a new session with Layer 7 services if the resource is busy	<a href="#">security-service</a>
Captive portal on Wi-Fi modules (Junos OS Release 20.4)	Use captive portal for integrated guest access management on the Wi-Fi Mini-PIM card	<a href="#">Wi-Fi Mini-Physical Interface Module Overview</a>



*(Continued)*

Feature	If You Want to	Go to
Custom response page for captive portal/block pages (Junos OS Release 20.4)	Configure a custom response page for a URL that is configured with the block or quarantine actions in the Web filtering profile	<a href="#">custom-page</a>
Juniper Extension Toolkit (JET) support for 64-bit applications (Junos OS Release 20.4)	Compile 64-bit applications for use with the AMD64 or ARM64 64-bit processor architecture	<a href="#">Develop On-Device JET Applications</a>
Application signature and package enhancements (Junos OS Release 21.1)	Use the enhanced application signature package that includes a group of newly added signatures under the junos:all-new-apps group	<a href="#">Grouping Newly Added Application Signatures</a>
Client information configuration in Juniper Identity Management Service (JIMS) (Junos OS Release 21.1)	Configure the specific interface, source IP address, or routing instance that your security device must use for connecting to a JIMS server	<a href="#">Configuring the Connection to an SRX Series Device</a>
Improved software upgrade process (Junos OS Release 21.1)	View the status of the software package installation or uninstallation. command.	request system software status
Preboot Execution Environment (PXE) boot support (Junos OS Release 21.2)	Use the PXE boot method to prepare an environment to boot devices by using a network interface that is independent of available data storage devices or installed operating systems	<a href="#">Upgrading the Personality of a Device by Using a PXE Boot Server</a>

## Improved Security

Feature	If You Want to	Go To
Tunneled application with unified policy (Junos OS Release 20.4)	Manage a specific tunneling application by using a unified policy	<a href="#">Tunnelling Applications Support</a>
Unified policy support for zonal and global policies (Junos OS Release 20.4)	Configure unified policies at the zone level or at the global level	<a href="#">Global Security Policies</a>

*(Continued)*

Feature	If You Want to	Go To
PowerMode IPsec (PMI) support for the SRX5000 line of devices and the SRX4600 (Junos OS Release 20.4)	Avail IPsec performance improvements on your security device	<a href="#">Improving IPsec Performance with PowerMode IPsec</a>
Transport Layer Security (TLS) profiles in Dynamic Address Feed servers (Junos OS Release 20.3)	Secure the communication channel between a Juniper Networks® SRX Series Firewall and a feed server using a TLS profile	<a href="#">tls-profile</a>
Dynamic address group (DAG) rescan option (Junos OS Release 20.4)	Efficiently apply policies by utilizing the session rescan option in DAGs. The system rescans the sessions, including the existing sessions, to ensure that the traffic matches the updated policy	<a href="#">session-scan</a>
Wildcard enhancement for URL pattern matching (Junos OS Release 20.4)	Configure better and user-friendly URL pattern matching in the Web filtering function by using new pattern matching rules for the domain name and URL path	<a href="#">url-pattern</a>
Terminal Access Point (TAP) mode support for pass-through GRE and IP-IP tunneling (Junos OS Release 20.4)	Perform pass-through authentication of IP-IP and GRE tunnel traffic when your device is in TAP mode	<a href="#">Understanding TAP Mode Support for Security Flow Sessions</a>
Server Name Indication (SNI) dynamic app selection for SSL proxy (Junos OS Release 20.4)	Avail enhanced SSL proxy profile selection mechanism that utilizes SNI TLS extensions to identify dynamic applications	<a href="#">SNI-Based Dynamic Application Information for SSL Proxy Profile</a>
Juniper Identity Management Service (JIMS) support for logical domains (Junos OS Release 20.4)	Configure enhanced firewall user authentication by including the logical system and tenant system names as a differentiators when using JIMS as the authentication source	<a href="#">Understanding Integrated User Firewall support in a Logical System</a>
Enhancements to packet capture of unknown applications (Junos OS Release 21.1)	Store the packet capture of unknown applications' details per session, where the packet capture (.pcap) file includes the session ID in the filename	<a href="#">Packet Capture of Unknown Application Traffic Overview</a>

*(Continued)*

Feature	If You Want to	Go To
Tunnel inspection for EVPN-VXLAN pass-through traffic (Junos OS Release 20.4)	Perform tunnel inspection for VXLAN-encapsulated traffic by applying Layer 4 or Layer 7 security services to the tunnel traffic passing through your security device	<a href="#">Tunnel Inspection for EVPN-VXLAN by SRX Series Devices</a>
Full TLS 1.3 support for Secure Sockets Layer (SSL) proxy (Junos OS Release 21.2)	Use SSL proxy with TLS protocol version 1.3, which provides improved security and better performance	<a href="#">SSL Proxy</a>

## Software-Defined WAN (SD-WAN) Enhancements

Feature	If You Want to	Go to
Wi-Fi support in dual customer premises equipment (CPE) deployments (Junos OS Release 20.3)	Provide a backup WAN connection by including Wi-Fi Mini-PIM configuration details in a chassis cluster configuration	<a href="#">Wi-Fi Mini-Physical Interface Module Overview</a>
Application quality of experience (AppQoE) support for Software as a Service (SaaS) applications (Junos OS Release 20.4)	Configure AppQoE for SaaS applications	<a href="#">AppQoE Support for SaaS Applications</a>
Application quality of service (AppQoS) support for J-Web (Junos OS Release 20.3)	Configure AppQoS in J-Web to prioritize and meter application traffic to provide better service for business-critical or high-priority application traffic	<a href="#">About the Application QoS Page</a>
PMI and generic routing encapsulation (GRE) acceleration (Junos OS Release 21.1)	Avail the PMI and GRE acceleration solutions to improve the SD-WAN performance	<a href="#">gre-performance-acceleration (Security Flow)</a>
Service-level agreement (SLA) link preference enhancement (Junos OS Release 21.2)	Set an SLA link preference for security device interfaces that allows application traffic to switch from a lower-priority link to a higher-priority link that meets the SLA requirements	<a href="#">Understanding Link-Type Affinity for the Preferred Link</a>

*(Continued)*

Feature	If You Want to	Go to
Application-based multipath routing (AMR) improvements (Junos OS Release 21.2)	Configure AMR with additional features including association of AMR rules and SLA rules with advanced policy-based routing (APBR) rule in an APBR profile	<a href="#">Application-Based Multipath Routing</a>
Multicast support in SD-WAN deployments (Junos OS Release 21.2)	Use multicast traffic on SRX Series Firewalls in SD-WAN deployments for bandwidth preservation and efficient traffic flows	<a href="#">Virtual Routing and Forwarding Instances in SD-WAN Deployments</a>
Application-based load balancing for APBR (Junos OS Release 21.2)	Achieve load balancing by moving the application traffic in multiple WAN links using user-defined link selection criteria. Load balancing improves the application traffic performance for APBR and AppQoS.	<a href="#">Advanced Policy-Based Routing</a>
GRE acceleration enhancement (Junos OS Release 21.2)	Use the existing PMI and GRE acceleration for non-SD-WAN deployments to improve GRE and MPLS-over-GRE performance	<a href="#">gre-performance-acceleration</a>

## Enhanced Reporting

Feature	If You Want to	Go to
Enhanced J-Web monitoring options. (Junos OS Release 20.4)	<ul style="list-style-type: none"> <li>Experience the newly reorganized Monitor tab for interfaces, reports, statistics, logs, and maps and charts</li> <li>Use the new Traffic Map page to visualize inbound and outbound traffic between geographic regions</li> </ul>	<a href="#">Monitor Interfaces</a> and <a href="#">Monitor Traffic Map</a>
Enhanced Setup Wizard (Junos OS Release 20.4)	Use the improved J-Web Setup Wizard settings for better experience when you perform various configuration tasks	<a href="#">Start J-Web</a>

*(Continued)*

Feature	If You Want to	Go to
Support for captive portal in J-Web (Junos OS Release 20.4)	Configure captive portal for creating a rule for security policies, adding a logical interface, or uploading a logo for firewall authentication	<a href="#">Add a Rule</a> , <a href="#">Add a Logical Interface</a> , and <a href="#">About the Authentication Settings Page</a> .
In-service software upgrade (ISSU) status command (Junos OS Release 20.4)	Display ISSU status during upgrade using the request system software in-service-upgrade command with the status option.	<a href="#">request system software in-service-upgrade</a>
Enhanced remote-access VPN support (Junos OS Release 20.3)	Use Juniper Secure Connect, a client-based SSL-VPN application, that allows you to securely connect and access protected resources on your network	<a href="#">Juniper Secure Connect Administrator Guide</a> , <a href="#">Juniper Secure Connect User Guide</a>
JTI support for Packet Forwarding Engine and Routing Engine (Junos OS Release 20.3)	Stream telemetry statistics to an outside collector through Packet Forwarding Engine sensors and pseudo-interface statistics through Routing Engine sensors	<a href="#">Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface)</a>
Enhanced monitoring and troubleshooting of the flow session (Junos OS Release 21.1)	Easily monitor the flow session by using additional filters in the show security flow session command, which generates the specified output in a list format	<a href="#">show security flow session</a> and <a href="#">show security flow session pretty</a>
Advanced Threat Prevention (ATP) enhancements to alerts, alarms, and fallback options (Junos OS Release 21.1)	Use newly introduced alerts, alarms, and fallback options for failure conditions when you enroll SRX Series Firewalls in Juniper ATP Cloud	<a href="#">advanced-anti-malware policy</a>
Improved logging and customizable log profiles for optimal log storage and archival (Junos OS Release 21.1)	Configure the security log profile per policy and define the format for fields selection and fields order for the log file	<a href="#">profile (security)</a>
Hit-count display for dynamic applications and URL categories in a security policy (Junos OS Release 21.2)	Use the enhanced show security policies hit-count command to view the usage details of the dynamic applications and URL categories	<a href="#">show security policies hit-count</a>

*(Continued)*

Feature	If You Want to	Go to
J-Web enhanced security reporting and IPsec monitoring (Junos OS Release 21.2)	Use the enhanced J-Web page for monitoring <ul style="list-style-type: none"> <li>• Interfaces and DHCP server bindings</li> <li>• IKE and IPsec VPN security associations (SAs) and statistics</li> <li>• Remote URLs for Juniper Secure Connect</li> </ul>	<a href="#">Monitor IPsec VPN</a>

## Virtual Firewall and Container Firewall Features

Feature	If You Want To	Go To
TAP mode support (Junos OS Release 20.3)	Use TAP mode for IDP, content security (formerly Content Security), and user firewall (UserFW) to generate security log information and display information such as threats detected, application usage, and user details for the incoming traffic	<a href="#">TAP Mode Support Overview</a>
Amazon Web Services (AWS) GuardDuty with Juniper Networks® vSRX Virtual Firewall Virtual Firewall and Juniper® Advanced Threat Prevention (ATP) Cloud (Junos OS Release 20.3)	Configure security threat feeds from AWS GuardDuty to the vSRX Virtual Firewall firewall in the AWS environment	<a href="#">Integrate AWS GuardDuty with vSRX Firewalls</a>
Enhanced Service mode (ESM) support (Junos OS Release 20.3)	Enable vSRX Virtual Firewall 3.0 to support a maximum of 128,000 sessions for Layer 7 services with increased service memory, thereby reducing the number of Layer 4 sessions by 50%.	<a href="#">forwarding-process</a>
Scaling vSRX Virtual Firewall 3.0 using Microsoft Azure Load Balancer and Virtual Machine Scale Sets (Junos OS Release 20.3)	Automatically increase or decrease internal and outbound traffic on vSRX Virtual Firewall using Azure Load Balancer and Microsoft Azure Virtual Machine Scale Sets	<a href="#">vSRX 3.0 Scaling for Internal and Outbound Traffic Using Azure Load Balancer and Virtual Machine Scale Sets</a>

*(Continued)*

Feature	If You Want To	Go To
Scale-out and scale-in elastic firewall support for Juniper Networks® cSRX Container Firewall Container Firewall in Kubernetes (Junos OS Release 20.3)	Deploy cSRX Container Firewall as a Kubernetes service or pod to scale out and scale in cSRX Container Firewall in a cluster that provides an elastic firewall service to application containers	<a href="#">cSRX Installation using Kubernetes</a>
vSRX Virtual Firewall 3.0 support in Oracle Cloud Infrastructure (OCI) (Junos OS Release 20.4)	Deploy vSRX Virtual Firewall 3.0 in OCI with the <i>bring your own license</i> (BYOL) licensing model	<a href="#">vSRX Deployment Guide for Private and Public Cloud Platforms</a>
SR-IOV 10GbE high availability (HA) support (Junos OS Release 20.4)	Set up SR-IOV 10GbE HA deployment on vSRX Virtual Firewall 3.0 instances to: <ul style="list-style-type: none"> <li>• Access the hardware directly from a virtual machines environment.</li> <li>• Share the PCIe devices to optimize performance and capacity.</li> </ul>	<a href="#">Configuring SR-IOV 10-Gigabit High Availability on vSRX 3.0</a>
LiquidIO DPDK driver (Junos OS Release 20.4)	Use the LiquidIO II smart NICs with vSRX Virtual Firewall 3.0 instances to employ the virtual function of SR-IOV.	<a href="#">Requirements for vSRX on KVM</a>
AWS Key Management Service (KMS) integration (Junos OS Release 20.4)	Use AWS KMS to safeguard the private keys used by the public key infrastructure (PKI) and Internet Key Exchange process (IKED).	<a href="#">Deploying vSRX 3.0 for Securing Data using AWS KMS</a>
Centralized licensing (Junos OS Release 21.1)	Install and manage licenses for hardware and software features using the Juniper Agile Licensing model. This licensing model provides simplified and centralized license administration and deployment	<a href="#">Juniper Agile Licensing Guide</a>
Phone-home client (PHC) (Junos OS Release 21.1)	Use the PHC to enable the device or virtual machine (VM) instance to securely obtain bootstrapping data, such as a configuration or software image, with no user intervention	<a href="#">Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client</a>
Increased VPN tunnel scale (Junos OS Release 21.1)	Configure IPsec VPN features with vSRX Virtual Firewall 3.0 for increased tunnel scale	<a href="#">IPsec VPN Feature Support on SRX5000 Line of Devices with SRX5K-SPC3 and vSRX Instances with New Package</a>

## What's Next

You can now get started with configuring new features on your security device. See complete documentation at [TechLibrary](#). For additional references, see "[Appendix: Resources](#)" on page 88.

# Upgrade to 19.4R3

### IN THIS SECTION

- [Key Features Post Junos OS 19.4R3 Upgrade | 40](#)
- [Know the Upgrade Path for Junos OS Release 19.4R3 and 20.2R3 | 46](#)
- [How to Upgrade to Junos OS Release 19.4R3 and 20.2R3 | 51](#)
- [Explore New Features Post Upgrade to Junos OS Release 19.4R3 | 64](#)

## Key Features Post Junos OS 19.4R3 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.

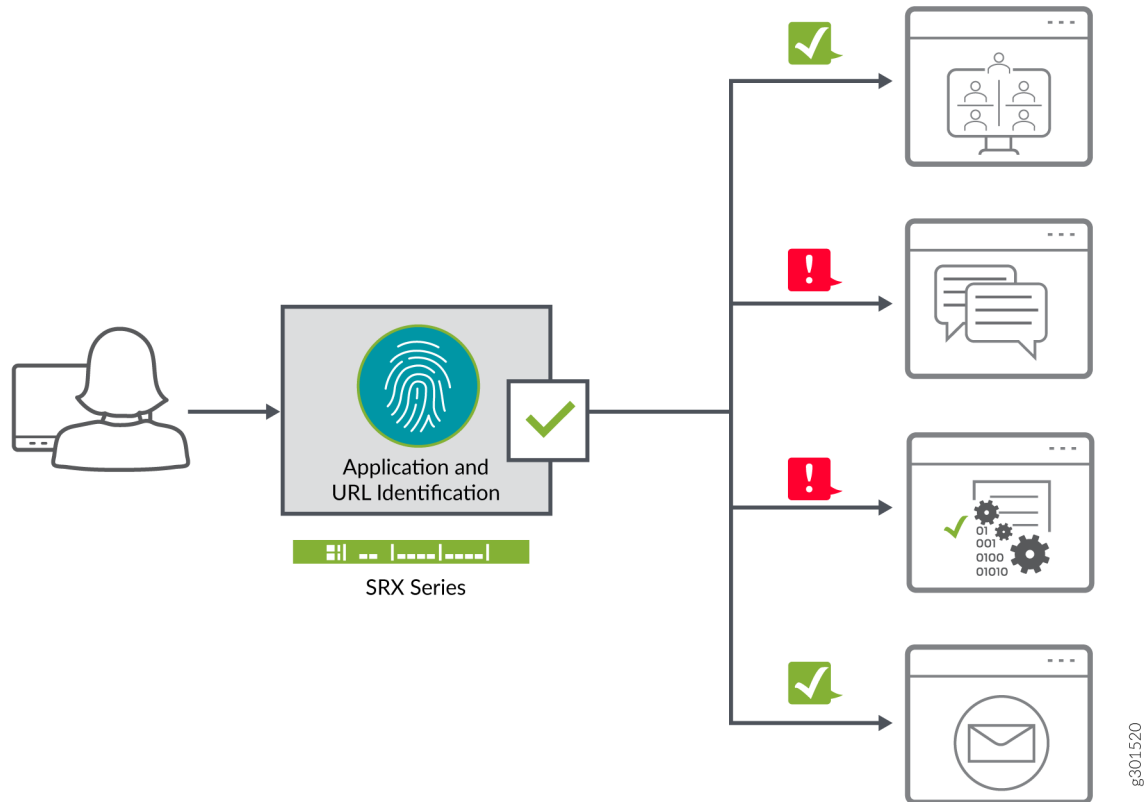
### IN THIS SECTION

- [Unified Policy | 41](#)
- [SD-WAN | 42](#)
- [Encrypted Traffic Insights | 43](#)
- [Adaptive Threat Profiling | 44](#)
- [Packet Capture for Unknown Applications | 45](#)
- [J-Web Getting Started Panel | 46](#)

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



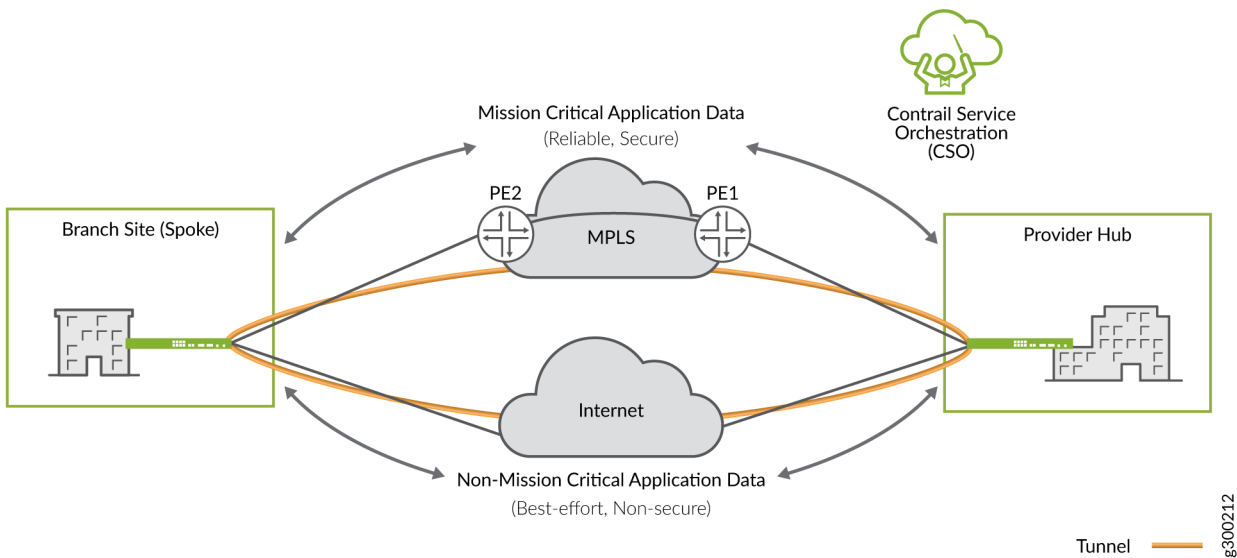
**What's this?** For the ease of use and adaptive policy management, you can now configure your security policies with dynamic applications and URLs as match conditions to react to changes in your network traffic over time.

**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



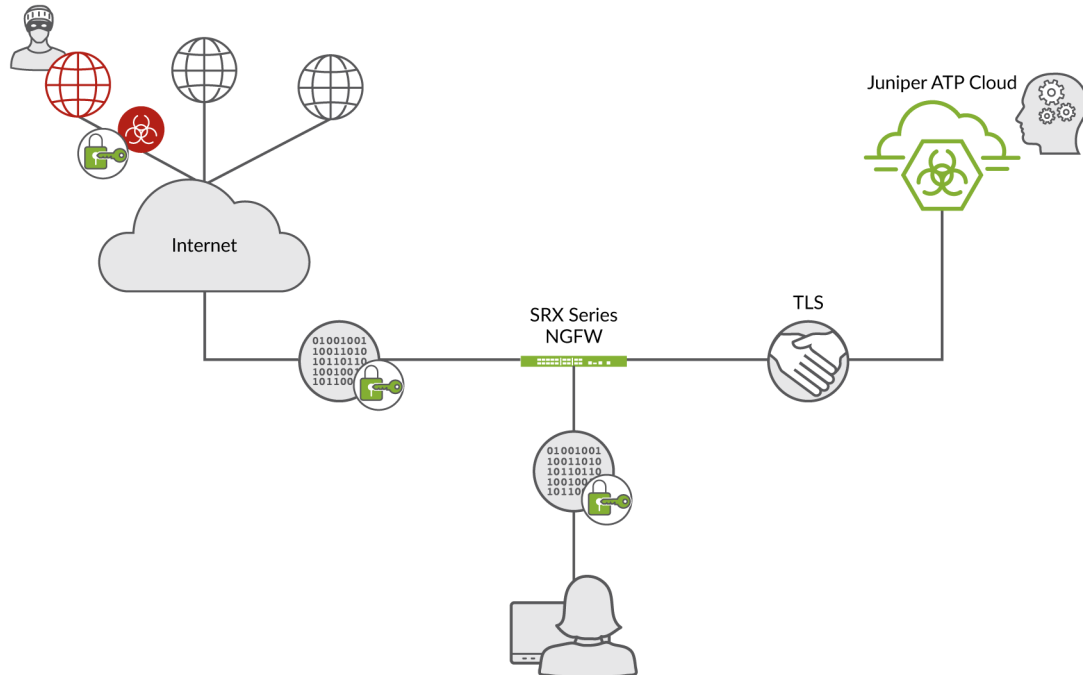
**What's this?** An SD-WAN implementation offers a flexible and automated way to route traffic from site to site. You can route traffic over different WAN links and assign higher priority to business-critical applications with advanced policy-based routing (APBR) and application quality of experience (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

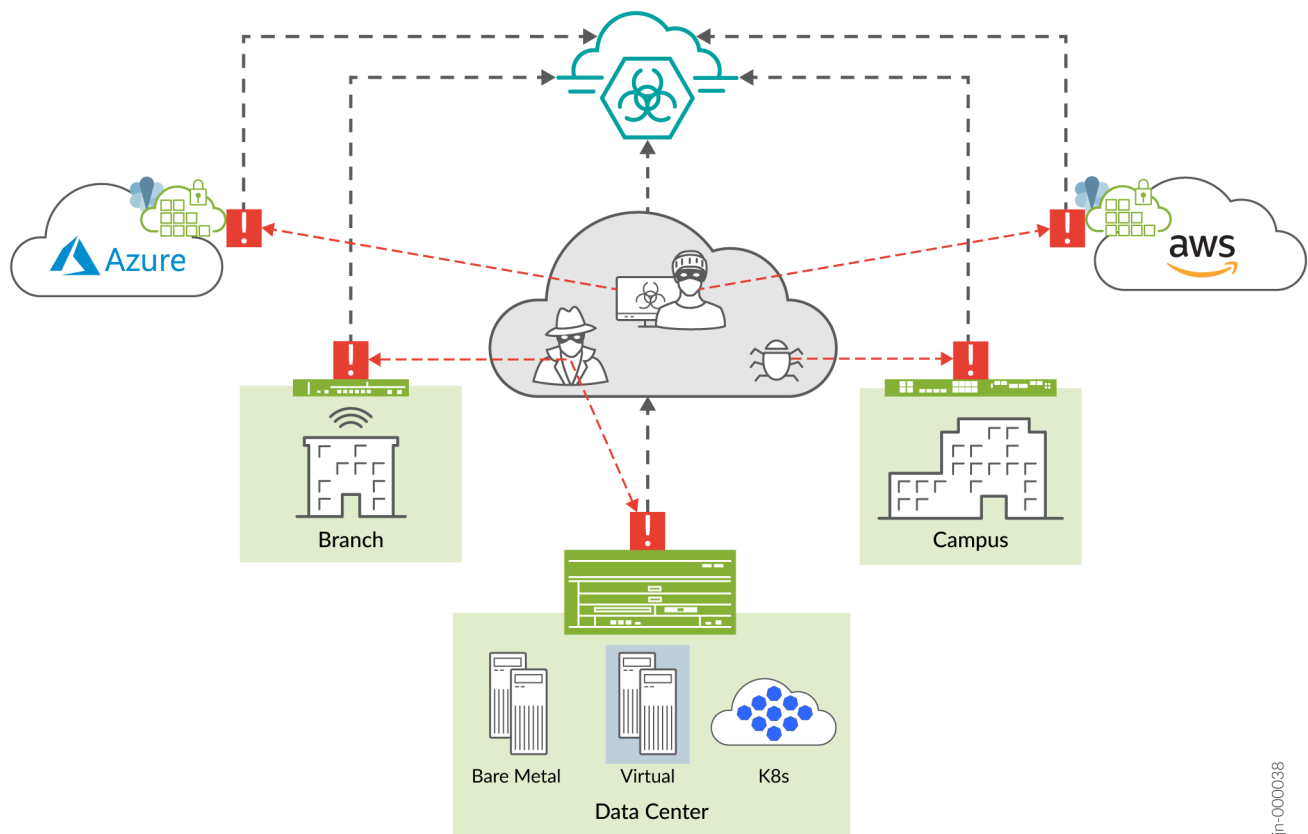
**What's this?** Encrypted Traffic Insights uses machine learning to analyze and detect malicious threats that are hidden in encrypted traffic without the need for decryption.

**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



jn-000038

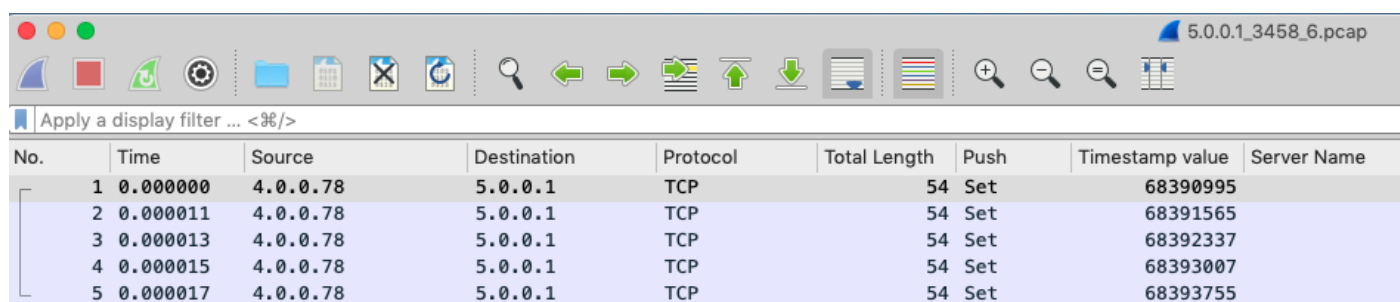
**What's this?** Adaptive Threat Profiling uses various detection capabilities of SRX Series Firewalls to create security intelligence feeds based on real-time events in your network. With this feature, you can detect threat actors targeting your network, look for potential problems or suspicious activity, 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](#).

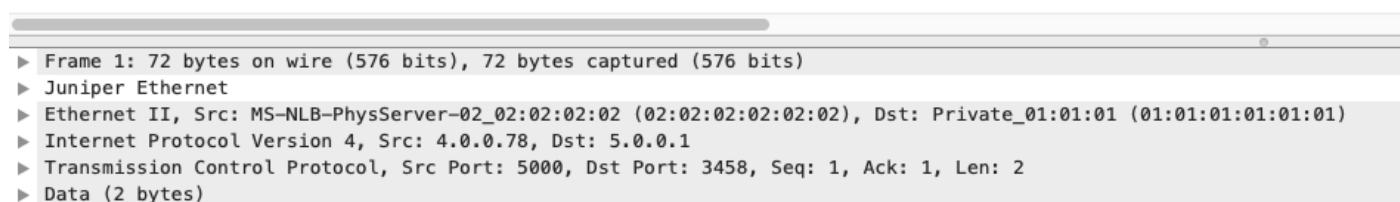
## Packet Capture for Unknown Applications



5.0.0.1\_3458\_6.pcap

Apply a display filter ... <96/>

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)

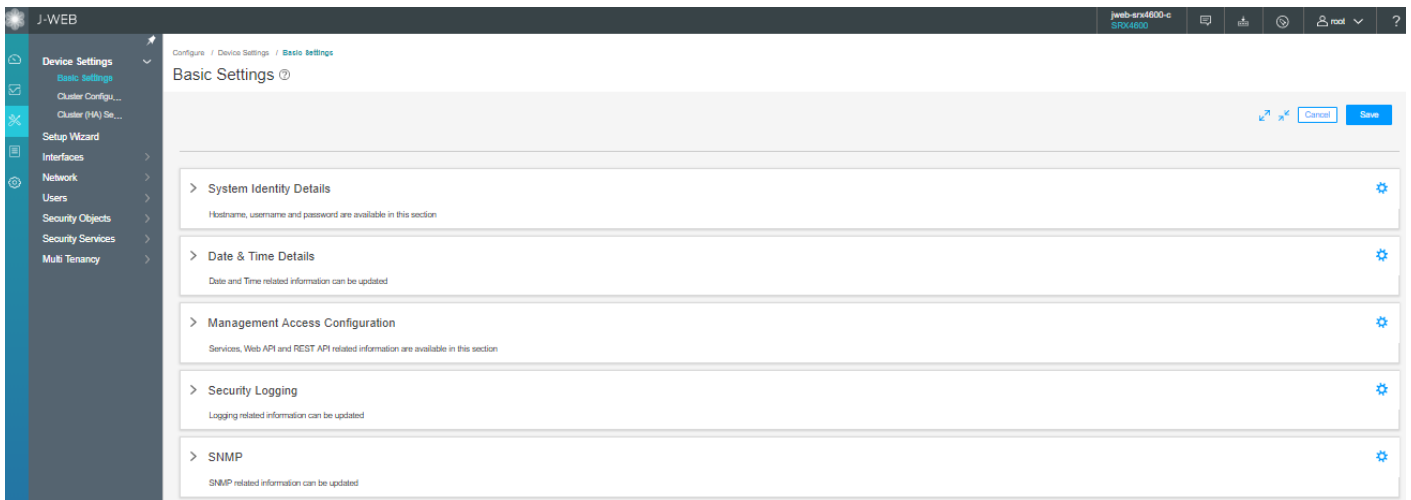
**What's this?** Custom applications are an unavoidable part of almost every enterprise network and can be difficult to identify and control. You can automatically capture packets from unknown applications and use the packet captures to gain additional insights to about your network, analyze it for potential 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 Firewall 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 Firewall 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 Firewall 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 Release 19.4R3 and 20.2R3](#)" on page 46.

## Know the Upgrade Path for Junos OS Release 19.4R3 and 20.2R3

### SUMMARY

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

### IN THIS SECTION

- [Upgrade Path for Your SRX Series | 47](#)
- [Upgrade Path for vSRX Virtual Firewall | 50](#)

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 Virtual Firewall and SRX380) as stated in [Table 5 on page 47](#).

**Table 5: 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 Virtual Firewall, and cSRX Container Firewall	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 Firewalls.

[Table 6 on page 47](#) lists the direct upgrade paths supported for SRX Series Firewalls.

**Table 6: 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 6: 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 7 on page 48](#) and [Table 8 on page 49](#) list the interim upgrade paths supported for SRX Series Firewalls.

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

**Table 7: 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 8: 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 Virtual Firewall, and cSRX Container Firewall)
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 Virtual Firewall

Junos OS Release 18.4R1 supports a new software architecture called vSRX Virtual Firewall 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 9 on page 50](#) to know about the direct upgrade path supported for your Junos OS on vSRX Virtual Firewall instances.

**Table 9: Upgrade Path for vSRX Virtual Firewall**

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 Virtual Firewall from Junos OS Release 15.1X49 Releases to 19.3 and higher releases.

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

We recommend that you deploy a new vSRX Virtual Firewall VM instead of performing a Junos OS upgrade. Upgrading to the latest VM enables you to move from vSRX Virtual Firewall to the newer and enhanced vSRX Virtual Firewall 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 51](#).

### RELATED DOCUMENTATION

[Upgrade Path for Junos OS Release 21.2R3](#) | 14

# 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 Virtual Firewall VM.

## IN THIS SECTION

- [Best Practices for Upgrading Junos OS | 51](#)
- [Follow Pre-Installation Steps | 52](#)
- [Upgrade Directly on Your Security Device \(CLI\) | 53](#)
- [Upgrade Directly on Your Security Devices in a Chassis Cluster \(CLI\) | 57](#)
- [Upgrade Junos OS Using a USB Flash Drive or J-Web | 58](#)
- [Upgrade Your vSRX Virtual Firewall VM | 58](#)
- [Upgrade Your cSRX Container Firewall Software Image | 59](#)
- [Upgrade Junos OS on SRX Series Firewalls Managed by Junos Space | 60](#)
- [Upgrade Junos OS on SRX Series Firewalls Managed by Juniper Sky™ Enterprise | 63](#)
- [After You Upgrade to Junos OS Release 19.4R3 or 20.2R3 | 63](#)

## 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 3 on page 54](#).

Figure 3: Download Junos OS Software

Download Results for: SRX4200 | X

---

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	<a href="#">tgz (1197.37MB)</a> <a href="#">Checksums</a>
SRX4100 and SRX4200	19.4R3-S1	12 Dec 2020	<a href="#">tgz (1197.08MB)</a> <a href="#">Checksums</a>

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/junosr/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-vsr-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	<a href="#">tgz (1197.37MB)</a> <a href="#">Checksums</a>
SRX4100 and SRX4200	19.4R3-S1	12 Dec 2020	<a href="#">tgz (1197.08MB)</a> <a href="#">Checksums</a>

## 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 Virtual Firewall 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 53](#) 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 | 58](#)
- [J-Web | 58](#)

## USB Flash Drive

You can use a USB flash drive to upgrade Junos OS images or recover an SRX Series Firewall after boot media corruption in cases where there is no console access to an SRX Series Firewall. 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 Firewall in a few steps using J-Web. For more information, see [Install Software Packages](#).

## Upgrade Your vSRX Virtual Firewall VM

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

- We recommend that you deploy a new vSRX Virtual Firewall VM instead of performing a Junos OS upgrade. The new VM enables you to move from vSRX Virtual Firewall to the newer and more enhanced vSRX Virtual Firewall 3.0 version.
- Moving to the vSRX Virtual Firewall 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 Virtual Firewall 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 Virtual Firewall 3.0 support.

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

## Upgrade Your cSRX Container Firewall Software Image

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

To install cSRX Container Firewall 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 Firewall 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/>

4. Download the cSRX Container Firewall 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 Container Firewall on a server with Ubuntu OS, see [Day One: Building Containers with cSRX](#).

## Upgrade Junos OS on SRX Series Firewalls Managed by Junos Space

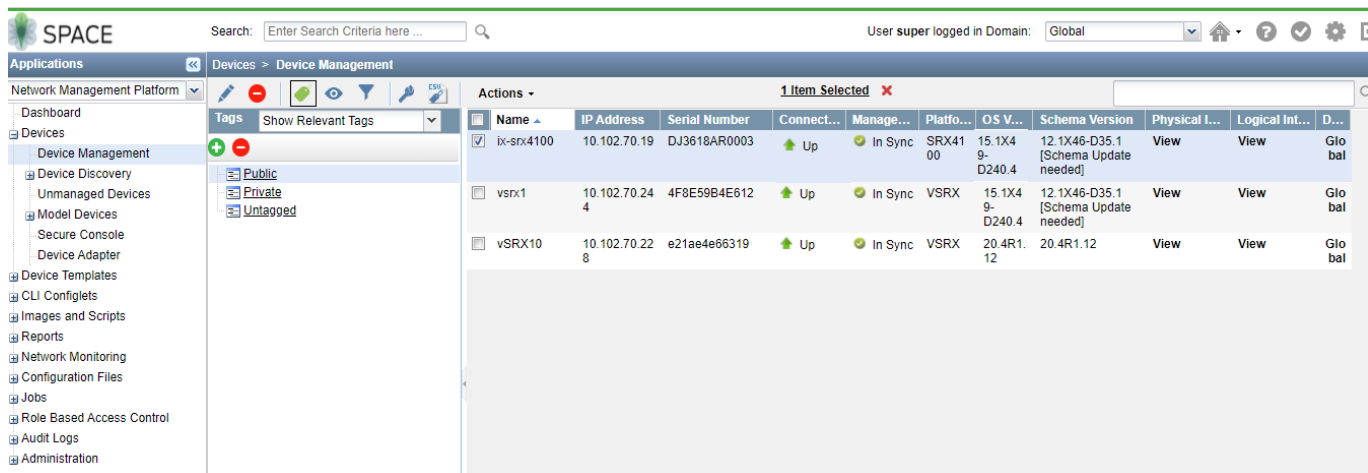
### SUMMARY

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.

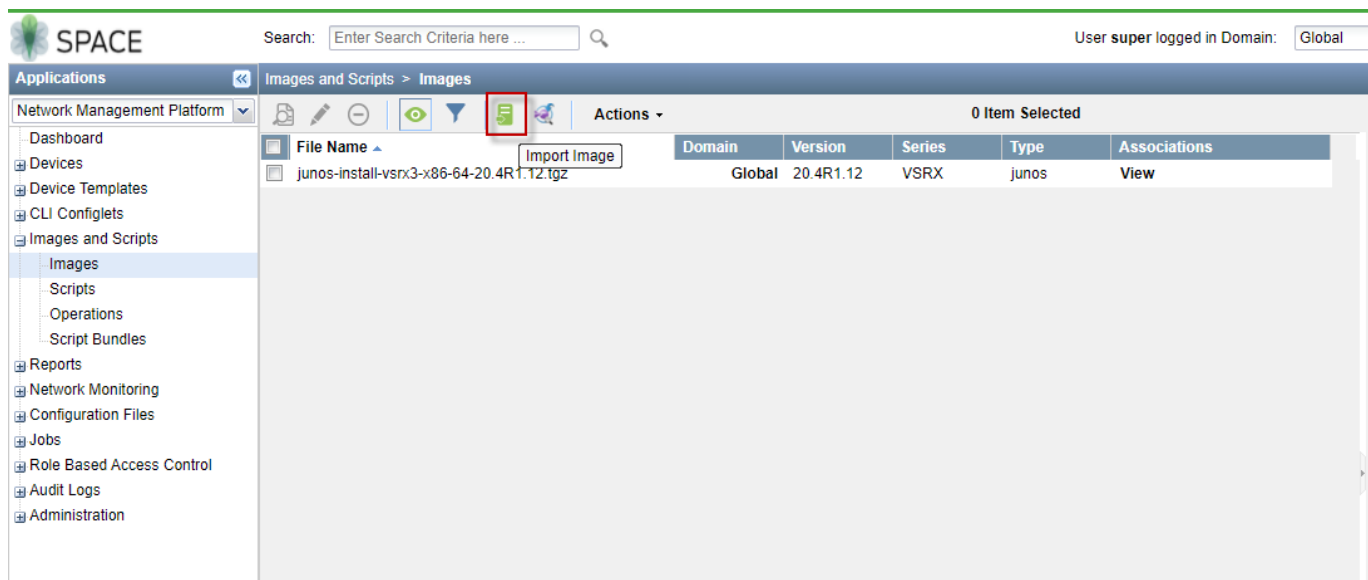
We'll use the following hardware and software combination in this example:

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

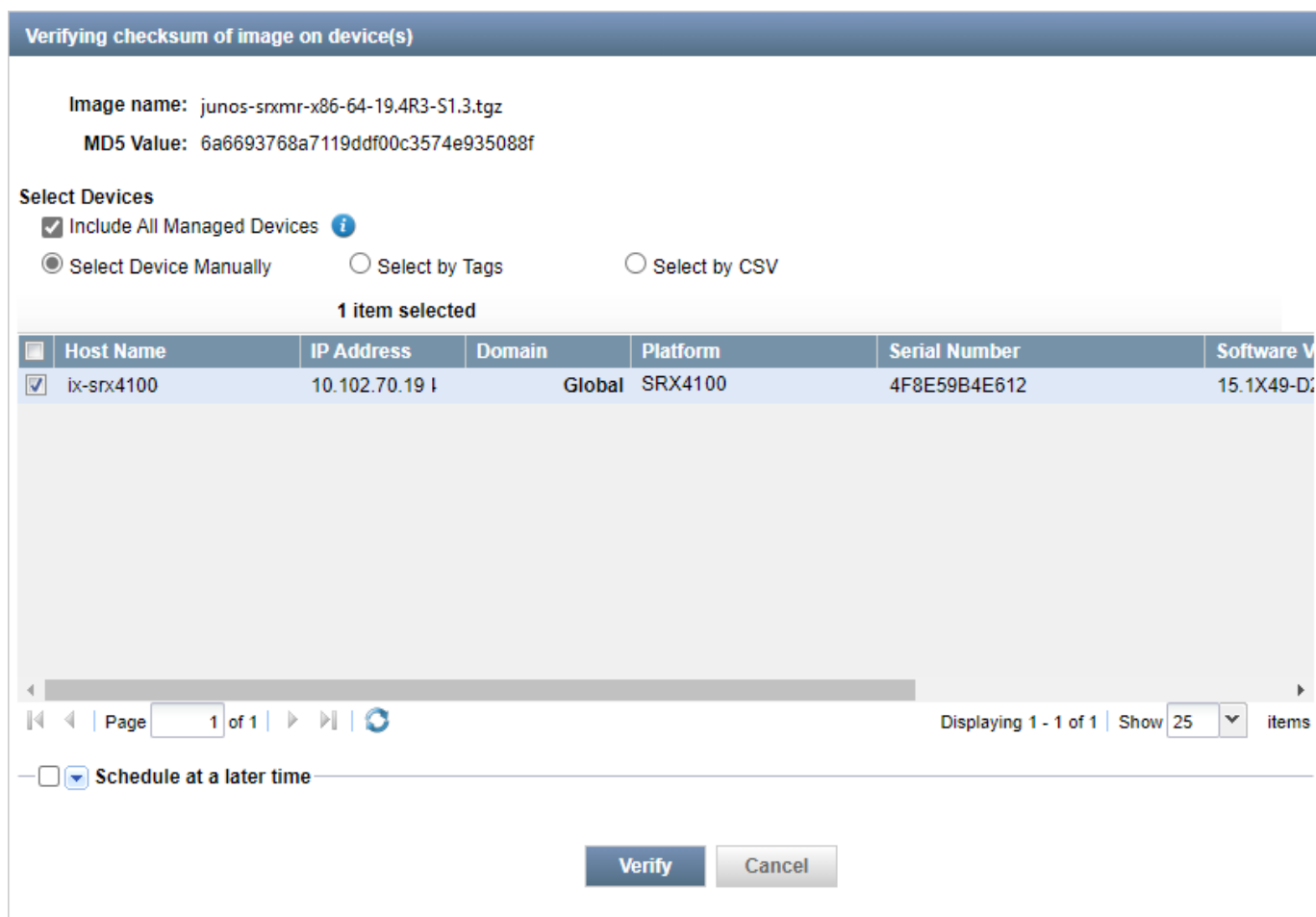
1. On the Network Management Platform GUI, select **Devices > Device Management**. The Device Management page is displayed.



2. Check the OS version running on the device.
3. 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 53 for instructions.
4. 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.

**Applications** << **Images and Scripts > Images**

Network Management Platform

**Actions**

- Deploy Device Image
- Deploy Satellite Device Image
- Stage Image on Device
- Stage Image on Satellite Device
- Undeploy JAM Package from Device
- Remove Image from Staged Device
- View Device Image Association
- MD5 Validation Result
- Verify Image on Devices
- Assign Image to Domain
- Delete Private Tags
- Tag It
- UnTag It
- View Tags
- Clear All Selections

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 Firewalls 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](#) | 64

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 Virtual Firewall 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 82](#).

## Licensing Requirements

Starting in January 2020, we've transitioned to the Flex Software Subscription Licensing Model for SRX Series and vSRX Virtual Firewall. 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 82](#). Otherwise, learn about new features and enhancements that you can start using with your Junos OS. See ["Explore New Features Post Upgrade to Junos OS Release 19.4R3" on page 64](#).

## Explore New Features Post Upgrade to Junos OS Release 19.4R3

### 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 | 65](#)
- [Improved Security | 66](#)
- [SD-WAN Enhancements | 67](#)
- [Enhanced Reporting | 67](#)
- [Virtual and Container Firewall Features | 68](#)



## 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.	<a href="#">Management Interface in a Non-Default Instance</a>
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.	<a href="#">Guidelines for gRPC and gNMI Sensors</a>
HA mode wizard (Junos OS Release 19.2R1)	Use HA wizards to set up chassis cluster in a few steps using J-Web.	<a href="#">HA Mode Wizards</a>
Juniper Agile Licensing (Junos OS Release 19.2R1)	Use Juniper Agile Licensing, a simplified and centralized license administration and deployment for your SRX Series.	<a href="#">Juniper Agile Licensing Guide</a> <a href="#">Software Feature Licenses for SRX Series Devices</a>
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.	<a href="#">Understanding Multiple IDP Policies for Unified Policies</a>
Packet captures from operational mode (Junos OS Release 19.3R1)	Execute the packet capture from the operational mode without committing the configurations.	<a href="#">Packet Capture from Operational Mode</a>
Simplified VPN Configuration in J-Web (Junos OS Release 20.2R1)	Configure IPsec VPN in a few steps using J-Web.	<a href="#">About the IPsec VPN Page</a>
SSL certificate management enhancements (Junos OS Release 19.2R1)	Easily manage the device certificates required for SSL.	<a href="#">Managing Device Certificates</a>
SSL proxy troubleshooting commands (Junos OS Release 19.3R1)	Easily monitor SSL-related issues by using an extensive set of operational commands.	<a href="#">Operational Commands to Troubleshoot SSL Sessions</a>

*(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.	<a href="#">Tenant Systems Overview</a>
Unified policies (Junos OS Release 18.2R1)	Get greater control and extensibility to manage dynamic applications traffic within the security policy.	<a href="#">Unified Security Policies</a>

## 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.	<a href="#">Adaptive Threat Profiling</a>
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.	<a href="#">Express Path</a>
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.	<a href="#">PMI Flow Based CoS functions for GTP-U</a>
IDP sensor enhancements and intelligent inspection (Junos OS Release 19.2R1)	Use IDP sensor settings and IDP intelligent inspection to optimize system resource usage.	<a href="#">IDP Sensor Configuration</a>
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.	<a href="#">IDP Signature Language Enhancements</a>
PowerMode IPsec (PMI) enhancements (Junos OS Release 19.1R1)	Enjoy the enhanced IPsec performance improvements using PMI.	<a href="#">Improving IPsec Performance with PowerMode IPsec</a>

*(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.	<a href="#">Express Path</a>
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.	<a href="#">SSL Performance Enhancements</a>
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	<a href="#">Understanding User Principal Name as User Identity in SRX Series Devices</a>

## 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 Content Security using the APBR rule.	<a href="#">Bypassing Application Services in an APBR Rule</a>
AppQoE enhancements (Junos OS Release 20.2R1)	Configure AppQoE for multihoming with active-active deployment.	<a href="#">Application Quality of Experience</a>

## 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.	<a href="#">About the Dynamic Applications Page</a>
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.	<a href="#">Monitoring the Dashboard</a>
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.	<a href="#">show services application-identification entries</a>

## Virtual and Container Firewall Features

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

(Continued)

Feature	If You Want to	Go to
cSRX Container Firewall support (Junos OS Release 18.1R1)	Protect your containerized environments with advanced security services, including content security, intrusion prevention system (IPS), AppSecure, and Content Security .	<a href="#">Building Containers with cSRX</a>

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 88.

# Migrate to vSRX3.0

SUMMARY

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

IN THIS SECTION

- [Overview | 70](#)
- [Migrate to vSRX3.0 | 76](#)
- [What's Next? | 81](#)

In Junos OS Release 18.4R1, we've introduced a new software architecture vSRX3.0 for vSRX Virtual Firewall virtual firewalls. We recommend that you migrate to vSRX3.0 for your vSRX Virtual Firewall 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 Virtual Firewall architectures:

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

## Overview

### IN THIS SECTION

- [Introduction to vSRX3.0 | 70](#)
- [License Requirements for vSRX3.0 | 75](#)

## 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.

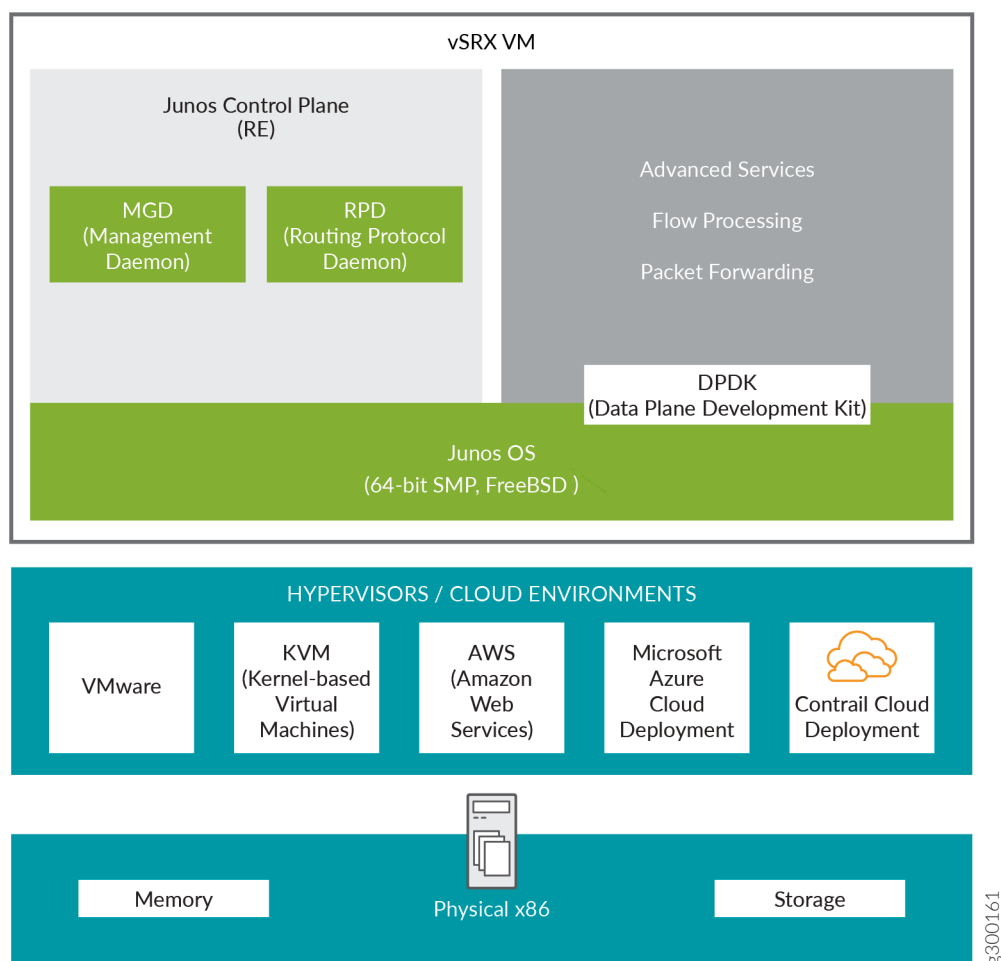
### Benefits

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 configuration required for enabling promiscuous mode on the management port and cluster control links
- Simplified and seamless deployments across different host environments

[Figure 4 on page 71](#) shows vSRX Virtual Firewall architecture.

Figure 4: vSRX3.0 Architecture



## Supported Junos OS Releases

Table 10 on page 71 provides a list of supported Junos OS releases for vSRX2.0 and vSRX3.0.

Table 10: Junos OS Release Support for vSRX2.0 and vSRX3.0

vSRX Virtual Firewall Architectures	Supported Junos OS Releases
vSRX2.0	15.1X49, 17.3 and later up to and including 22.4. Junos OS Release 22.4 is the last version available for vSRX2.0. We recommend using vSRX Virtual Firewall 3.0 going forward.
vSRX3.0	18.4 and later

## Feature Support in vSRX2.0 and vSRX3.0

Table 11 on page 72 and Table 12 on page 74 lists features supported in vSRX2.0 and vSRX3.0.

**Table 11: 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
<b>Supported Hypervisors</b>		
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)
Multicore scaling support on Microsoft Hyper-V	No	Yes (Junos OS Release 19.1R1 onwards)
Nutanix	Yes	Yes (Junos OS Release 19.1R1 onwards)
Contrail Networking 3.x	Yes	Yes



Table 11: 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)
<b>Other Features</b>		
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)
<b>System Requirements</b>		
Hardware acceleration/enabled VMX CPU flag in the hypervisor	Yes	No
Disk space	16 GB	18 GB

Table 12: 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 Virtual Firewall. 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 5 on page 75 summarizes license requirements for different upgrade scenarios.

Figure 5: License Requirements for vSRX3.0

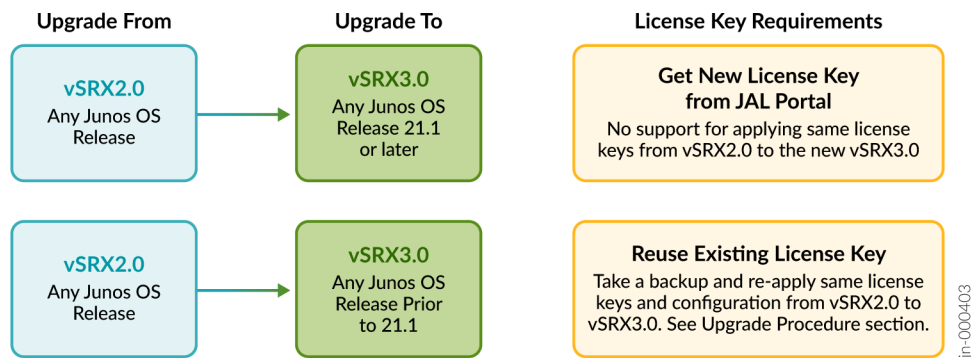


Table 13: License Requirements for vSRX3.0

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 ( <a href="https://license.juniper.net/licensemanage/">https://license.juniper.net/licensemanage/</a> ).  See <a href="#">Release Notes: Junos OS Release 21.1R1</a> , <a href="#">Flex Software License for vSRX</a> , and <a href="#">Licensing Guide</a> for details. Ensure you specify the correct numbers of vCPUs in the license request.

Table 13: 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"> <li>• Take backup of license key and configuration file.</li> <li>• Install a new VM.</li> <li>• Reapply the license key and configuration file.</li> </ul> <p>See <a href="#">"Migration Procedure"</a> on page 78 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 Virtual Firewall image upgrades in the future.

## Migrate to vSRX3.0

### IN THIS SECTION

- [Check vSRX Virtual Firewall Version | 76](#)
- [Pre-Migration Checklist | 77](#)
- [Migration Procedure | 78](#)
- [Post-Migration Tasks | 79](#)

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

## Check vSRX Virtual Firewall Version

Check if your vSRX Virtual Firewall 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 Virtual Firewall instance.

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

The sample output indicates that your vSRX Virtual Firewall 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 5 on page 75](#). 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 Virtual Firewall 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 6 on page 79](#).

Figure 6: 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	<a href="#">vhd (1452.39MB)</a> <a href="#">Checksums</a>
vSRX KVM Appliance	21.2R3	29 Mar 2022	<a href="#">qcow2 (731.88MB)</a>

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 Virtual Firewall 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 Virtual Firewall 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 Virtual Firewall 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 5 on page 75](#)) on the newly launched vSRX Virtual Firewall 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 bwbm13 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.

## Changes in Application Layer Gateways (ALG) Default Behavior

In vSRX2.0, the following ALGs were disabled by default; however, when you migrate to vSRX3.0, these ALGs are enabled by default:

- H323
- MGCP
- RTSP



- SCCP
- SIP

If you've not enabled these ALGs in your vSRX2.0 configuration, you might want to disable them in the vSRX3.0 configuration to keep the same ALG behavior.

To disable an ALG:

```
[edit]
set security alg <alg-name> disable
```

Use the `show security alg status` command to confirm which ALGs are enabled/disabled.

Example:

```
user@host> show security alg status
DNS      : Enabled
FTP      : Enabled
H323     : Disabled
MGCP     : Disabled
MSRPC    : Enabled
PPTP     : Enabled
RSH      : Disabled
RTSP     : Disabled
SCCP     : Disabled
SIP      : Disabled
SQL      : Disabled
SUNRPC   : Enabled
TALK     : Enabled
TFTP     : Enabled
IKE-ESP  : Disabled
TWAMP    : Disabled
```

## 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 Firewalls Managed by Security Director | 82](#)
- [Unified Policies on SRX Series Firewalls | 84](#)

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 Content Security 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 Firewalls 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 7 on page 83](#) shows the option available in Security Director that you can use to convert a security policy to a unified policy.

Figure 7: Security Director: Convert to Unified Policies

The screenshot shows the 'Standard Policies' configuration page in the Security Director. The left sidebar lists various policy types, including 'Firewall Policy' which is expanded to show 'Standard Policies'. The main area displays a table of policies. A context menu is open for the policy 'vSRX\_FW\_132', and the 'Convert To Unified Policy' option is highlighted in red.

Seq.	Name	Rules	Devices	Publish State	Li
<b>POLICIES APPLIED BEFORE 'DEVICE SPECIFIC POLICIES' (1 policy)</b>					
1	All Devices Policy Pre	Add Rule	3	Not Published	St
<b>DEVICE SPECIFIC POLICIES (3 policies)</b>					
	sriini-vsrx-17020.1r1	1	sriini-vsrx-17020.1r1	Re-Publish Required	Ti
<input checked="" type="checkbox"/>	vSRX_FW_132		vSRX_FW_132	Re-Publish Required	Fr
	tme-srx4600-01_2			Not Published	W
<b>POLICIES APPLIED AFTER 'DEVICE SPECIFIC POLICIES' (1 policy)</b>					
2	All Devices Policy Post		3	Not Published	St

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 'Unified Policies' configuration page in the Security Director. The left sidebar lists various policy types, including 'Firewall Policy' which is expanded to show 'Unified Policies'. The main area displays the 'policy-2 / Rules' section, showing a table of rules.

Seq.	Rule Name	Src. Zone	Dest. Zone	Action	Advanced Security	URL Category
<b>ZONE (2 Rules)</b>						
1	rule-allow-known-traffic	trust	untrust	Permit	-	-
2	check-known-http-traffic	trust	untrust	Permit	UTM wf-policy IPS P...recommended	Facebook Commenting Facebook Events
<b>GLOBAL (1 Rule)</b>						
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.

Configure / IPS Policy / Policies

Global

## IPS-Policy-Main / Rules

Edited few seconds ago

Save Discard Publish Update More Create

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 Content Security policy, navigate to **Configure>UTM Policy** page.

Configure / UTM Policy / Policies

Global

## UTM Policies

1 selected

More + Edit Delete Search Filter

Name	Antispam	Antivirus	Content Filtering	Web Filtering
default-utm-policy		-	-	
je-wf-policy		-	-	wf-enhanced-default
sophos-av-policy		HTTP: sophos-av-... +5	-	
sophos-je-av-wf-policy		HTTP: sophos-av-... +5	-	wf-enhanced-default
UTM-Policy-Main	as-defaults	HTTP: sophos-av-def... FTP Upload: sophos-... FTP Download: soph... IMAP: sophos-av-def...	HTTP: CF-Profile FTP Upload: CF-Profile FTP Download: CF-P... IMAP: CF-Profile	wf-local-default
wf-policy		-	-	wf-cpa-default

8 items

## Unified Policies on SRX Series Firewalls

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"> <li>Configure rules and rule sets at the set security application-firewall hierarchy level.</li> <li>Apply application firewall functionality           <pre>set security policies from-zone &lt;zone&gt; to-zone &lt;zone&gt; policy &lt;policy&gt; then permit application-services application-firewall rule-set.</pre> </li> </ul>	<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 &lt;zone&gt; to-zone &lt;zone&gt; policy &lt;policy&gt; match dynamic-application &lt;application-name&gt;</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"> <li>Specify an active IDP policy:   <pre>set security idp active-policy &lt;IDP policy name&gt;</pre> </li> <li>Apply IDP policy in the security policy:   <pre>set security policies from-zone &lt;zone&gt; to-zone &lt;zone&gt; policy &lt;policy&gt; then permit application-services idp</pre> </li> </ul>	<p>Specify multiple IDP policies per firewall rule:</p> <pre>set security policies from-zone &lt;zone&gt; to-zone &lt;zone&gt; policy &lt;policy-1&gt; then permit application-services &lt;IDP-policy-name-1&gt;</pre> <pre>set security policies from-zone &lt;zone&gt; to-zone &lt;zone&gt; policy &lt;policy-2&gt; then permit application-services &lt;IDP-policy-name-2&gt;</pre> <pre>set security idp default-policy &lt;IDP-policy name&gt;</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
```

## Content Security

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

**Example:** The following samples show the difference in Content Security 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 to Junos OS Release 19.4R3](#)" on page 64.

# Appendix: Resources

## SUMMARY

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

## IN THIS SECTION

- [Additional References | 88](#)

## 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	<a href="#">Feature Explorer</a>
Suggested Junos OS Release for the device	<a href="#">Junos Software Versions - Suggested Releases to Consider and Evaluate</a>
Managing insufficient space on device during an upgrade	<a href="#">Verifying Available Disk Space on SRX Series Devices</a>
Firmware Upgrade PoE	<a href="#">Understanding OS Upgrade versus Firmware Upgrade</a>
How to upgrade from Junos X version to Junos Y version?	<a href="#">"Know your Upgrade Paths" on page 46</a>
How to handle if primary partition becomes corrupt?	<a href="#">How to Copy OS from Primary Partition to Secondary Partition if the Primary Partition is Corrupt</a>
System outage during upgrade	<a href="#">Upgrading a Chassis Cluster Using In-Service Software Upgrade</a> <a href="#">How to Upgrade an SRX Cluster with Minimal Down Time</a> <a href="#">ISSU/ICU upgrade limitations on SRX firewalls</a>
Licensing Information on SRX Series Firewalls	<a href="#">Flex Software License for SRX Series Devices</a>
Configure advanced security features on SRX Series Firewalls	<a href="#">Get Up and Running with Advanced Security Services</a>



*(Continued)*

If Your Query Is About	See
Hardening a Junos device and understanding the rationale for, and possible impact of, doing so.	<i>Hardening Junos Devices</i> at <a href="#">Day One Books</a>
Get started with configuring security features.	<a href="#">Day One+</a>

## What's Next

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