

Release Notes: Policy Enforcer Release 21.1R1

20 January 2022
Revision 1

Contents	Introduction 2
	Release Notes for Policy Enforcer 2
	New and Changed Features 3
	Product Compatibility 3
	Supported Security Director Software Versions 3
	Supported Devices 4
	Third-Party Wired and Wireless Access Network 7
	Juniper Networks Contrail, Microsoft Azure, and AWS Specifications 7
	Virtual Machine 8
	Supported Browser Versions 8
	Upgrade Support 9
	Known Behavior 9
	Known Issues 10
	Resolved Issues 11
	Hot Patch Releases 12
	Installation Instructions 12
	Finding More Information 13
	Documentation Feedback 14
	Requesting Technical Support 14
	Self-Help Online Tools and Resources 15
	Creating a Service Request with JTAC 15
	Revision History 16

Introduction

Policy Enforcer orchestrates threat remediation workflows based on Juniper Networks Sky Advanced Threat Prevention (Sky ATP) solution, Command-and Control server (C&C server), and GeoIP identification feeds, in addition to other trusted custom feeds from customers. Policy Enforcer enforces security policies on Juniper Networks virtual and physical SRX Series firewalls, EX Series and QFX Series switches, MX Series routers, third-party switch and wireless networks, private cloud and SDN solutions such as Contrail and VMware NSX, as well as on public cloud deployments. On the MX Series router, only DDOS policy is pushed by Policy Enforcer/Security Director. The allowlist, blocklist, and CC policies must be manually configured. Policy Enforcer integrates with Juniper Networks Advanced Threat Prevention Appliance (JATP) to provide a continuous, multistage detection and analysis of Web, e-mail, and lateral spread traffic moving through the network.

Policy Enforcer integrates with the VMware NSX solution to deliver an advanced next-generation firewall feature set that uses vSRX for VMware microsegmentation deployments. Policy Enforcer enables pervasive security across the entire network using switches, routers, and security devices for on-premise scenarios leveraging SDN solutions such as Juniper Networks Contrail and VMware NSX to orchestrate networking functionality where needed, along with applications hosted in the public cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure.

Release Notes for Policy Enforcer

IN THIS SECTION

- [New and Changed Features | 3](#)
- [Product Compatibility | 3](#)
- [Known Behavior | 9](#)
- [Known Issues | 10](#)
- [Resolved Issues | 11](#)
- [Hot Patch Releases | 12](#)

New and Changed Features

This section describes the new features and enhancements to existing features in Policy Enforcer Release 21.1R1.

- **NSX-T Manager support for North-South traffic**—VMware NSX-T is the latest generation of VMware's network virtualization products. NSX-T is the successor to NSX-V. VMware NSX-T provides a framework to integrate the advanced security services as a North-South at Edge Gateway. vSRX runs as a service virtual machine and provides advanced services such as Layer 4 to Layer 7 services. To deploy the advanced security features of the vSRX Virtual Firewall in the VMware NSX-T environment, Junos Space Security Director, vSRX, and NSX-T Manager operate together as a solution to fully automate the provisioning and deployment of vSRX to protect applications and data from advanced cyberattacks.

Product Compatibility

IN THIS SECTION

- Supported Security Director Software Versions | 3
- Supported Devices | 4
- Third-Party Wired and Wireless Access Network | 7
- Juniper Networks Contrail, Microsoft Azure, and AWS Specifications | 7
- Virtual Machine | 8
- Supported Browser Versions | 8
- Upgrade Support | 9

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, see the Security Director 21.1R1 Release Notes.

Supported Security Director Software Versions

Policy Enforcer is supported only on specific Security Director software versions as shown in [Table 1 on page 4](#).

Table 1: Supported Security Director Software Versions

Policy Enforcer Software Version	Compatible with Security Director Software Version	Junos OS Release (Juniper Sky ATP Supported Devices)
21.1R1	21.1R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later

NOTE: The times zones set for Security Director and Policy Enforcer must be the same.

Supported Devices

Table 2 on page 4 lists the SRX Series devices that support Juniper Sky ATP and the threat feeds these devices support.

NOTE: Table 2 on page 4 lists the general Junos OS release support for each platform. However, each Policy Enforcer software version has specific requirements that take precedence. See Table 1 on page 4 for more information.

Table 2: Supported SRX Series Devices with Juniper Sky ATP and Feed Types

Platform	Model	Junos OS Release	Supported Threat Feeds
vSRX	2 vCPUs, 4GB RAM	Junos 15.1X49-D60 and later	C&C, antimalware, infected hosts, GeoIP
SRX Series	SRX300, SRX320	Junos 15.1X49-D90 and later	C&C, GeoIP
SRX Series	SRX340, SRX345, SRX550M	Junos 15.1X49-D60 and later	C&C, antimalware, infected hosts, GeoIP
SRX Series	SRX1500	Junos 15.1X49-D60 and later	C&C, antimalware, infected hosts, GeoIP
SRX Series	SRX5400, SRX5600, SRX5800	Junos 15.1X49-D62 and later	C&C, antimalware, infected hosts, GeoIP
SRX Series	SRX4100, SRX4200	Junos 15.1X49-D65 and later	C&C, antimalware, infected hosts, GeoIP

Table 2: Supported SRX Series Devices with Juniper Sky ATP and Feed Types (continued)

Platform	Model	Junos OS Release	Supported Threat Feeds
SRX Series	SRX4600	Junos 18.1R1 and later	C&C, antimalware, infected hosts, GeolP
SRX Series	SRX3400, SRX3600	Junos 12.1X46-D25 and later	C&C, GeolP
SRX Series	SRX1400	Junos 12.1X46-D25 and later	C&C, GeolP
SRX Series	SRX550	Junos 12.1X46-D25 and later	C&C, GeolP
SRX Series	SRX650	Junos 12.1X46-D25 and later	C&C, GeolP

Table 3 on page 5 describes the hardware and software components that are compatible with JATP.

Table 3: Supported Hardware and Software Versions Compatible with JATP

Platform	Hardware	Software Versions
vSRX		Junos 19.1R1.6 and above
SRX Series	SRX320, SRX300	Junos 19.1R1 and above
SRX Series	SRX4100, SRX4200, SRX4600	Junos 15.1X49-D65 and above for SRX4100 and SRX4200 Junos 18.1R1 and above for SRX4600
SRX Series	SRX340, SRX345, SRX550m	Junos 15.1X49-D60 and above
SRX Series	SRX5800, SRX5600, SRX5400	Junos 15.1X49-D50 and above
SRX Series	SRX1500	Junos 15.1X49-D33 and above

NOTE: The SMTP e-mail attachment scan feature is supported only on the SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices running Junos OS Release 15.1X49-D80 and later. vSRX does not support the SMTP e-mail attachment scan feature.

In Policy Enforcer Release 18.3R1, Policy Enforcer supports SRX Series devices running Junos OS Release 17.3R1 and later.

Table 4 on page 6 lists the supported EX Series and QFX Series switches.

Table 4: Supported EX Series Ethernet Switches and QFX Series Switches

Platform	Model	Junos OS Release
EX Series	EX4200, EX2200, EX3200, EX3300, EX4300	Junos 15.1R6 and later
EX Series	EX9200	Junos 15.1R6 and later
EX Series	EX3400, EX2300	Junos 15.1R6 and later Junos 15.1X53-D57 and later
QFX Series	QFX5100, QFX5200	Junos 15.1R6 and later
	vQFX	Junos 15.1X53-D60.4

Table 5 on page 6 lists the supported MX Series routers that support the DDoS and C&C feed types.

Table 5: Supported MX Routers and Feed Types

Platform	Model	Junos OS Release	Supported Feed Types
MX Series	MX240, MX480, MX960	Junos 14.2R1 and later	DDoS
	MX240, MX480, MX960	Junos 18.4R1 and later	C&C <i>(Mark MX Series router as perimeter device in secure fabric)</i> The C&C feed is global and is overridden if C&C custom feed is set on Policy Enforcer.
	vMX	Junos 16.2R2.8	-

Table 6 on page 6 shows the supported SDN and cloud platforms.

Table 6: Supported SDN and Cloud Platforms

Component	Specification
VMware NSX for vSphere	6.3.1 and later NOTE: For sites that are running vSphere 6.5, vSphere 6.5a is the minimum supported version with NSX for vSphere 6.3.0.
VMware NSX Manager	6.3.1 and later

Third-Party Wired and Wireless Access Network

Table 7 on page 7 lists the third-party support and required server.

Table 7: Third-party Wired and Wireless Access Network

Switch/Server	Notes
Third-party switch	Any switch model that adheres to RADIUS IETF attributes and supports RADIUS Change of Authorization from ClearPass is supported by Policy Enforcer for threat remediation.
ClearPass RADIUS server	Must be running software version 6.6.0.
Cisco ISE	Must be running software version 2.1 or 2.2.
Forescout CounterACT	Must be running software version 7.0.0. NOTE: To obtain an evaluation copy of CounterACT for use with Policy Enforcer, click here .
Pulse Secure	Must be running software version 9.0R3.

If you use Juniper Networks EX4300 Ethernet switch to integrate with the third-party switches, the EX4300 must be running Junos OS Release 15.1R6 or later.

Juniper Networks Contrail, Microsoft Azure, and AWS Specifications

Table 8 on page 7 shows the required components for Juniper Networks Contrail.

Table 8: Juniper Networks Contrail Components

Model	Software Version	Supported Policy Enforcer Mode
Juniper Networks Contrail	5.0	Microsegmentation and threat remediation with vSRX
vSRX	Junos OS 15.1X49-D120 and later	Microsegmentation and threat remediation with vSRX

Table 9 on page 8 shows the required Policy Enforcer components for AWS.

Table 9: AWS Support Components

Model	Software Version	Supported Policy Enforcer Mode
vSRX	Junos OS 15.1X49-D100.6 and later	vSRX policy based on workload discovery
	Junos OS 19.2R1 and later	AWS with JATP

To get started with Microsoft Azure, see [Getting Started with Microsoft Azure](#).

[Table 10 on page 8](#) shows the required Policy Enforcer components for Microsoft Azure.

Table 10: Microsoft Azure Support Components

Model	Software Version	Supported Policy Enforcer Mode
vSRX	Junos OS 15.1X49-D110.4 and later	vSRX policy based on workload discovery

Virtual Machine

Policy Enforcer is delivered as an OVA or a KVM package to be deployed inside your VMware ESX or QEMU/KVM network with the following configuration:

- 2 CPU
- 8-GB RAM (16 GB recommended)

You must increase the RAM to 16-GB if you configure more than 256 custom dynamic addresses, allowlist, or blocklist.

- 120-GB disk space

Table 11: Supported Virtual Machine Versions

Virtual Machine	Version
VMware	VMware ESX server version 4.0 or later or a VMware ESXi server version 4.0 or later
QEMU/KVM	CentOS Release 6.8 or later

Supported Browser Versions

Security Director and Policy Enforcer are best viewed on the following browsers.

Table 12: Supported Browser Versions

Browser	Version
Google Chrome	75.x
Internet Explorer	11 on Windows 7
Firefox	67.0 and later

Upgrade Support

Upgrading Policy Enforcer follows the same rules as for upgrading Security Director. You can upgrade only from the previously released version. This includes the minor releases. For example, you can upgrade to Policy Enforcer Release 21.1R1 only from Policy Enforcer Release 20.1R1. However, Policy Enforcer 20.1R1 can be upgraded from 19.1R1 -> 19.1R2 -> 19.2R1->19.3R1-> 19.4R1-> 20.1R1 or 18.1R2 -> 18.2R1 -> 18.3R1 -> 18.4R1 -> 19.1R1 -> 19.1R2 -> 19.2R1 -> 19.3R1 -> 19.4R1 -> 20.1R1 -> 20.3R1 ->21.1R1.

For complete upgrade instructions, see [Upgrading Your Policy Enforcer Software](#).

For more information about the Security Director upgrade path, see [Upgrading Security Director](#).

Known Behavior

This section lists the known behavior in Policy Enforcer Release 21.1R1.

- You can associate a tenant with only one VRF instance.
- A realm can have all the sites either with tenants or without tenants.
- Tenants and VRF-based feeds are supported only on MX Series devices.
- To take action on the feeds from Policy Enforcer, you must configure policies on the MX Series device through the CLI and not from Security Director.
- To upload certificates for Policy Enforcer, to be used in certificate-based authentication mode of Junos Space, Junos Space must be in password authentication mode to complete the Policy Enforcer settings workflow. The mode can be switched to certificate-based authentication after the Policy Enforcer settings are completed.
- Policy Enforcer supports only the default global domain in Junos Space Network Management.
- When you are creating a connector for third-party devices, it is mandatory to add at least one IP subnet to a connector. You cannot complete the configuration without adding a subnet.

- If you replace a device as part of RMA and if that device is already in secure fabric, you must remove the device from secure fabric and add it again. Otherwise, feeds are not downloaded to the replaced device.
- JATP zone creation or assignment cannot be done in the General Setup Wizard.
- Ensure that the time difference between the JATP and the SRX Series devices is less than 20 seconds to avoid the enrollment failure.
- When the vSRX device is disenrolled with JATP and enrolled again, you might see the device shown twice in the Feed Sources page in Security Director.
- When the feed source is JATP, you must change the Infected host state in the JATP portal. There are no Dashboard widgets to show the JATP related threats or Infected hosts in Security Director.
- During the JATP enrollment, it may state that Juniper Sky ATP license is not present. You can ignore this warning.
- For SRX Series devices in a chassis cluster, both primary and secondary chassis cluster nodes need to be discovered in Security director before adding them to secure fabric. If only one chassis cluster node is discovered and added to secure fabric, the feed download does not work after failover to secondary node.

Known Issues

This section lists the known issues in Policy Enforcer Release 21.1R1.

For the most complete and latest information about resolved Policy Enforcer defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

- You may not be allowed to edit the ClearPass connector password on the Policy Enforcer Connector page.

Workaround: Delete the connector and add it again with the right credentials. [PR1464446](#)

- Sites associated with tenants (Multi-tenant sites) are shown while creating policy enforcement group. This is applicable for guided setup also. UC-334
- You will be unable to add enforcement points to site after changing the mode when the certificate based authentication is enabled. UC-368

After changing the Policy Enforcer mode in Policy Enforcer settings page, go to **Junos Space Network Management Platform > Users > pe_user** and manually upload the client certificate.

OR

Go to Junos Space Network Management Platform and change the mode to Password Authentication and perform Policy Enforcer settings again.

- When you download feeds to a device after the realm is deleted and added again in Policy Enforcer, an internal server error is identified.

Workaround:

On Junos OS CLI on the SRX Series device, execute the command **request services security-intelligence download**. [PR1586287](#)

- Error shown while adding Policy Enforcer in cloud feed-only mode. [PR1585381](#)
- After restoring the 21.1R1 Junos Space Network Management Platform, Security Director, and Policy Enforcer database backup from one Junos Space Network Management Platform, Security Director, and Policy Enforcer server to another 21.1R1 Junos Space Network Management Platform, Security Director, and Policy Enforcer server, you cannot add Policy Enforcer.

Workaround:

1. Go to the Junos Space Network Management Platform CLI.
2. Execute the following MySQL command to take the backup of the triggers:

```
mysqldump -u<username> -p<password> --triggers --add-drop-trigger --no-create-info --no-data --no-create-db --skip-opt build_db > <filename>
```

Sample command: `mysqldump -ujboss -pMMtmPD6EBfmYsNW46kGxbWGpXiNWW6l0 --triggers --add-drop-trigger --no-create-info --no-data --no-create-db --skip-opt build_db > /tmp/triggers.sql`

3. Open the SQL file that we got from the above command and take the hostname from the DEFINER.
4. Replace the old hostname with 'jmp-CLUSTER' using the **sed** command as below:

```
sed -i 's/<old hostname>/jmp-CLUSTER/g' <filename>
```

Sample command: `sed -i 's/space-000c29d74288/jmp-CLUSTER/g' /tmp/triggers.sql`

5. Delete the line with **SET @@GLOBAL.GTID_PURGED='sample ids';** in /tmp/triggers.sql file.
6. Restore the triggers to MySQL using the following command:

```
mysql -ujboss -p<password> build_db < <filename>
```

Sample command: `mysql -ujboss -pMMtmPD6EBfmYsNW46kGxbWGpXiNWW6l0 build_db < /tmp/triggers.sql`

[PR1588186](#)

Resolved Issues

This section lists the issues fixed in Policy Enforcer Release 21.1R1.

For the most complete and latest information about resolved Policy Enforcer defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

- The custom feeds downloaded from the remote server through HTTPS do not work. [PR1576467](#)
- Policy Enforcer does not allow you to create custom feeds with a URL or domain. You can create only IP-based custom feeds. [PR1522841](#)
- The country codes available in the Security Director GeoIP feed do not match the Junos OS CLI on an SRX Series device GeoIP. [PR1582766](#)
- An issue with GeoIP country code for Serbia and Montenegro. [PR1569964](#)
- In the Security Director UI, the finish button for **Add Sky ATP Realm/Modify Sky ATP Realm** does not work in Configure > Threat Prevention > Feed Sources from Firefox 83.0 onward. [PR1564456](#)

Hot Patch Releases

IN THIS SECTION

- [Installation Instructions](#) | 12

This section describes the new features and installation procedure in Policy Enforcer Release 21.1R1 hot patch v1.

NOTE: Security vulnerabilities are addressed in the Policy Enforcer Release 21.1R1 hot patch v1.

Installation Instructions

During hot patch installation, the script performs the following operations:

- Stops controller, feed-collector and feed-provider services of Policy Enforcer.
- Backs up existing configuration files and libraries.
- Updates the Red Hat Package Manager (RPM) file for Policy Enforcer.
- Restarts the controller, feed-collector and feed-provider.

NOTE: You must install the hot patch on Policy Enforcer Release 21.1R1-1196 or on any previously installed hot patch. The hot patch installer backs up all the files which are modified or replaced during hot patch installation.

Perform the following steps in the CLI:

1. Download the Policy Enforcer 21.1R1 Patch `Policy_Enforcer-21.1R1-XX-PE-Upgrade.rpm` from the [download site](#).

Here, XX is the hot patch version.

2. Copy the `Policy_Enforcer-21.1R1-XX-PE-Upgrade.rpm` file to the `/tmp` location.

3. Verify the checksum of the hot patch for data integrity:

`md5sum Policy_Enforcer-21.1R1-XX-PE-Upgrade.rpm.`

4. Install the rpm using the command:

`rpm -Uvh Policy_Enforcer-21.1R1-XX-PE-Upgrade.rpm`

NOTE: We recommend that you install the latest available hot-patch version, which is the cumulative patch.

Finding More Information

For the latest, most complete information about known and resolved issues with Junos Space Network Management Platform and Junos Space Management Applications, see the Juniper Networks Problem Report Search application at: <http://prsearch.juniper.net>.

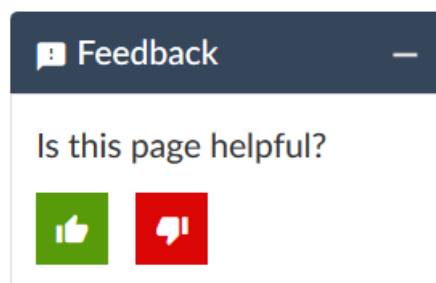
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: <http://pathfinder.juniper.net/feature-explorer/>.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: <http://www.juniper.net/techpubs/content-applications/content-explorer/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes:
<https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool:
<https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see
<https://support.juniper.net/support/requesting-support/>.

Revision History

20 January, 2022—Revision 2—Policy Enforcer Release 21.1R1.

14 April, 2021—Revision 1—Policy Enforcer Release 21.1R1.

Copyright © 2022 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.