

Release Notes: Policy Enforcer Release 18.4R1

20 December 2018
Revision R1

Contents	Introduction 2
	Release Notes for Policy Enforcer 2
	New and Changed Features 2
	Product Compatibility 3
	Supported Security Director Software Versions 4
	Supported Devices 5
	Third-Party Wired and Wireless Access Network 7
	Juniper Networks Contrail, Microsoft Azure, and AWS Specifications 7
	Virtual Machine 8
	Supported Browser Versions 9
	Upgrade Support 9
	Known Issues 9
	Known Behavior 10
	Finding More Information 11
	Documentation Feedback 11
	Requesting Technical Support 12
	Self-Help Online Tools and Resources 12
	Creating a Service Request with JTAC 13
	Revision History 13

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 GeolP 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.

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 | 2](#)
- [Product Compatibility | 3](#)
- [Known Issues | 9](#)
- [Known Behavior | 10](#)

New and Changed Features

This section describes the new features and enhancements in Policy Enforcer Release 18.4R1:

- **Policy enforcement for public cloud with Microsoft Azure**—Policy Enforcer integrates with Microsoft Azure for workload discovery, allowing enterprises to configure a dynamic workload metadata-based policy that is always kept up-to-date without requiring security administrators to manually update the VM inventory in Security Director. In addition, Policy Enforcer updates Microsoft Azure Security Groups for the virtual machines identified as infected with malware or command and control activity, mitigating lateral threats inside the network.
- **Support of IPv6 feeds**—Policy Enforcer extends supports for IPv6 addresses for Command and Control (C&C), Allowlist and Blocklist Juniper Sky ATP feeds. With this enhancement, users can leverage both IPv4 and IPv6 based rich set of curated threat feeds from Juniper Sky ATP to proactively remediate threat in their environment. The custom feed and infected host do not support IPv6 feeds.
- **MX Series routers as perimeter devices**—In addition to SRX firewalls, Policy Enforcer now allows MX Series routers to be defined as perimeter devices within secure fabric, to support environments that deploy MX Series routers at the network edge. Policy Enforcer adds the ability to push C&C and GeolP feeds to these MX Series devices allowing users to protect their network by proactively blocking outbound C&C communication.
- **Support of 256 DAGs per SRX Series device**—Policy Enforcer supports 256 dynamic address groups (DAGs) per SRX Series device running Junos OS Release 15.1X49-D160 and later. This provides users with greater flexibility and scale in using DAGs to define their firewall policy.

NOTE: The maximum number of dynamic address groups supported by Policy Enforcer is 1000 with 16-GB RAM and 4 CPUs.

Product Compatibility

IN THIS SECTION

- [Supported Security Director Software Versions | 4](#)
- [Supported Devices | 5](#)
- [Third-Party Wired and Wireless Access Network | 7](#)
- [Juniper Networks Contrail, Microsoft Azure, and AWS Specifications | 7](#)
- [Virtual Machine | 8](#)
- [Supported Browser Versions | 9](#)
- [Upgrade Support | 9](#)

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, see the Security Director 18.4R1 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)
16.1R1	16.1R1	Junos 15.1X49-D60 and later
16.2R1	16.1R1, 16.2R2	Junos 15.1X49-D80 and later
17.1R1	17.1R1	Junos 15.1X49-D80 and later
17.1R2	17.1R2	Junos 15.1X49-D80 and later
17.2R1	17.2R1	Junos 15.1X49-D110 and later
17.2R2	17.2R2	Junos 15.1X49-D110 or Junos 17.3R1 and later
18.1R1	18.1R1	Junos 15.1X49-D110 or Junos 17.3R1 and later
18.1R2	18.1R2	Junos 15.1X49-D110 or Junos 17.3R1 and later
18.2R1	18.2R1	Junos 15.1X49-D110 or Junos 17.3R1 and later
18.3R1	18.3R1	Junos 15.1X49-D110 or Junos 17.3R1 and later
18.4R1	18.4R1	Junos 15.1X49-D110 or Junos 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 5 lists the SRX Series devices that support Juniper Sky ATP and the threat feeds these devices support.

NOTE: Table 2 on page 5 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 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
SRX Series	SRX4600	Junos 18.1R1 and later	C&C, antimalware, infected hosts, GeoIP
SRX Series	SRX3400, SRX3600	Junos 12.1X46-D25 and later	C&C, GeoIP
SRX Series	SRX1400	Junos 12.1X46-D25 and later	C&C, GeoIP
SRX Series	SRX550	Junos 12.1X46-D25 and later	C&C, GeoIP
SRX Series	SRX650	Junos 12.1X46-D25 and later	C&C, GeoIP

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

Table 3: Supported EX Series Ethernet Switches and QFX Series Switches

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

Table 4 on page 6 lists the supported MX Series routers that support the DDoS and C&C feed types.

Table 4: Supported MX Routers and Feed Types

Platform	Model	Junos OS Release	Supported Threat Feeds
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>
	vMX	Junos 16.2R2.8	-

Table 5 on page 7 shows the supported SDN and cloud platforms.

Table 5: 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 6 on page 7 lists the third-party support and required server.

Table 6: 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 7 on page 7 shows the required components for Juniper Networks Contrail.

Table 7: Juniper Networks Contrail Components

Model	Software Version	Supported Policy Enforcer Mode
Juniper Networks Contrail	5.0	Microsegmentation and threat remediation with vSRX

Table 7: Juniper Networks Contrail Components (continued)

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

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

Table 8: 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

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

[Table 9 on page 8](#) shows the required Policy Enforcer components for Microsoft Azure.

Table 9: 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 10: 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 11: Supported Browser Versions

Browser	Version
Google Chrome	54.x
Internet Explorer	11 on Windows 7
Firefox	55 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 18.4R1 only from Policy Enforcer Release 18.3R1. However, Policy Enforcer 18.3R1 can be upgraded from 18.2R1 -> 18.3R1, 18.1R2 -> 18.2R1 -> 18.3R1.

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

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

Known Issues

This section lists the known issues in Policy Enforcer Release 18.4R1.

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

- If you select both threat remediation and next gen firewall as functions for a Contrail connector for a specific project, sometimes the vSRX in the service chain might not be enrolled in Juniper Sky ATP for threat remediation and malware scanning.

Workaround: Delete the connector instance and recreate or upload the IP addresses through the custom infected host feeds. [PR1357761](#)

- After a connector instance is created with only the next generation firewall option, if you edit the connector instance to add threat remediation option, the system does not initiate the enrollment of these enforcement points. That is, vSRX in the service chain of the cloud resource is not enrolled in Juniper Sky ATP realm for malware scanning.

Workaround: After editing the connector workflow to add threat remediation along with the next generation firewall option, go to the Juniper Sky ATP realm page and edit the realm to remove the site associated to the connector instance and save the changes. Once Policy Enforcer successfully saves the change, edit the realm again and add the site back to the realm. This triggers the enrollment of the enforcement points in the connector instance. [PR1365715](#)

- If there are infected hosts either blocked or quarantined in the system before the Policy Enforcer mode is updated to Cloud Only Mode and after updating to Cloud Only Mode, all the infected hosts cannot be cleared from the system or user interface (UI).

Workaround: Clear all the infected hosts before updating the mode to Cloud Only mode, where Juniper Sky ATP realm is required. [PR1388771](#)

- If you delete a custom feed from the system that had infected hosts in the monitor state, host entries are not cleared from the system.

Workaround: Clear the infected hosts' IP addresses in the monitor state before deleting the custom feed. [PR1390546](#)

- Some of the UI requests fail because the Policy Enforcer controller service processing UI API calls go through a shutdown sequence. The shutdown could be initiated forcefully or because of a service failure condition.

Workaround: Initiate requests from the UI once again and when the service is up and running, UI requests are processed successfully. [PR1391925](#)

- For Microsoft Azure connector, the metadata-based firewall policies do not get updated to a device as expected. [PR1403820](#)
- When multiple dynamic address groups are created and provided to more than one realm, it takes more than the expected time for SRX Series device to receive that feed. [PR1405462](#)
- When the workloads in AWS are shutdown, for any newly added connectors such as AWS or Microsoft Azure, vSRX do not receive the dynamic feeds. It is observed that Policy Enforcer tries to update the dynamic feeds frequently instead of updating once. [PR1408014](#)

Known Behavior

- 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.

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>.

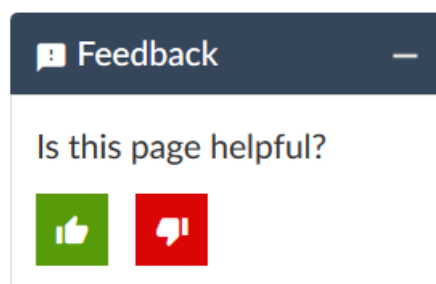
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: <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 December, 2018—Revision 1—Policy Enforcer Release 18.4R1.

Copyright © 2020 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.