Release Notes: Policy Enforcer Release 17.2R1

26 December 2017

Contents

Introduction | 2

Release Notes for Policy Enforcer | 2

- Product Compatibility | 2
  - Supported Security Director Software Versions | 3
  - Supported Devices | 3
  - Third-Party Wired and Wireless Access Network | 5
  - Virtual Machine | 6
  - Supported Browser Versions | 6
  - Upgrade Support | 7
- New and Changed Features | 7
- Known Issues | 8
- Known Behavior | 8
- Resolved Issues | 8

Finding More Information | 9

Documentation Feedback | 9

Requesting Technical Support | 10

- Self-Help Online Tools and Resources | 10
- Creating a Service Request with JTAC | 11

Revision History | 11

Introduction

Policy Enforcer orchestrates threat remediation workflows based on threat detection by Juniper Sky ATP solution or custom threat feeds and enforces these policies on Juniper's EX/QFX switches as well as 802.1x enabled third party wired and wireless switches. In addition, Policy Enforcer integrates with VMware NSX solution to deliver advanced Next Generation Firewall (NGFW) feature set using vSRX for VMware micro-segmentation deployments

Release Notes for Policy Enforcer

IN THIS SECTION

- Product Compatibility | 2
- New and Changed Features | 7
- Known Issues | 8
- Known Behavior | 8
- Resolved Issues | 8

Product Compatibility

IN THIS SECTION

- Supported Security Director Software Versions | 3
- Supported Devices | 3
- Third-Party Wired and Wireless Access Network | 5
- Virtual Machine | 6
- Supported Browser Versions | 6
- Upgrade Support | 7

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, please see the Security Director 17.2R1 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 3.

Table 1: Supported Security Director Software Versions

Policy Enforcer Software Version	Compatible with Security Director Software Version	Junos OS Release (Sky ATP Supported Devices)
16.1R1	16.1R1	Junos 15.1X49-D60 and above
16.2R1	16.1R1, 16.2R2	Junos 15.1X49-D80 and above
17.1R1	17.1R1	Junos 15.1X49-D80 and above
17.1R2	17.1R2	Junos 15.1X49-D80 and above
17.2R1	17.2R1	Junos 15.1X49-D110 and above

Supported Devices

The following table lists the Sky ATP supported SRX Series devices and their supported threat feeds.

> **NOTE:** Table 2 on page 3 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 3 for more information.

Table 2: Supported SRX Series Devices and Feed Types

Platform	Model	Junos OS Release	Supported Threat Feeds
vSRX	2 VCPUs, 4 GB RAM	Junos 15.1X49-D60 and above	CC, AntiMalware, Infected Hosts, Geo IP
SRX Series	SRX 300, SRX 320	Junos 15.1X49-D90 and above	CC, Geo IP
SRX Series	SRX 340, SRX 345, SRX 550m	Junos 15.1X49-D60 and above	CC, AntiMalware, Infected Hosts, Geo IP

Table 2: Supported SRX Series Devices and Feed Types *(continued)*

Platform	Model	Junos OS Release	Supported Threat Feeds
SRX Series	SRX 1500	Junos 15.1X49-D60 and above	CC, AntiMalware, Infected Hosts, Geo IP
SRX Series	SRX 5400, 5600, 5800	Junos 15.1X49-D62 and above	CC, AntiMalware, Infected Hosts, Geo IP
SRX Series	SRX 4100, SRX 4200	Junos 15.1X49-D65 and above	CC, AntiMalware, Infected Hosts, Geo IP
SRX Series	SRX3400, SRX3600	Junos 12.1X46-D25 and above	CC, Geo IP
SRX Series	SRX 1400	Junos 12.1X46-D25 and above	CC, Geo IP
SRX Series	SRX 550	Junos 12.1X46-D25 and above	CC, Geo IP
SRX Series	SRX 650	Junos 12.1X46-D25 and above	CC, Geo IP

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

In the Policy Enforcer Release 17.2R1, Policy Enforcer supports SRX Series devices running Junos OS Release 17.4R1.

The following table lists the supported EX Series ethernet switches 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, EX 2200, EX3200, EX3300, EX4300	Junos 15.1R6 and above	Sky ATP with PE
EX Series	EX9200	Junos 15.1R6 and above	Sky ATP with PE
EX Series	EX3400, EX 2300	Junos 15.1R6 and above	Sky ATP with PE

Table 3: Supported EX Series Ethernet Switches and QFX Series Switches *(continued)*

Platform	Model	Junos OS Release	Supported Policy Enforcer Modes
QFX Series	QFX5100, QFX 5200	Junos 15.1R6 and above	Sky ATP with PE

Table 4 on page 5 lists the MX routers supporting DDoS feed type.

Table 4: Supported MX Routers and Feed Types

Platform	Model	Junos OS Release	Supported Threat Feeds
MX Routers	MX240, MX480, MX960	Junos 14.2R1 and above	DDoS

Table 5 on page 5 shows the supported SDN and Cloud platforms.

Table 5: Supported SDN and Cloud Platforms

Component	Specification
VMware NSX for vSphere	6.3.1 or 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 or later

Third-Party Wired and Wireless Access Network

The following table lists the third-party support and required server.

Switch/Server	Notes
Third-party switch	Any switch model that adheres to Radius IETF attributes and support Radius Change of Authorization from ClearPass is supported by Policy Enforcer for threat remediation.
ClearPass Radius server	Must be running 6.6.0 software version.
Cisco ISE	Must be running 2.1 software version.

NOTE: Juniper Networks tested Cisco 2950 with 12.2(55)SE7 and Cisco WS-C3850-48P with 03.02.01.SE.

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

Virtual Machine

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

- 1 CPU
- 8-GB RAM
- 120-GB disk space

Table 6: 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 7: Supported Browser Versions

Browser	Version
Google Chrome	54.x
Internet Explorer	11 on Windows 7
Firefox	46 and above

Upgrade Support

Upgrading Policy Enforcer follows the same rules as for upgrading Security Director. You can upgrade only from the most previously released version. This includes the minor releases (R1, R2,and so on.) For example, Policy Enforcer 17.2R1 can be upgraded only from 17.1R1. The upgrade path to Policy Enforcer 17.2R1 is as follows: 16.1R1 -> 16.2R1 -> 17.1R1 -> 17.1R2 -> 17.2R1.

For more information on the Security Director upgrade path, see Upgrading Security Director.

New and Changed Features

This section describes the new features in Policy Enforcer Release 17.2R1.

- **Implementing threat policy on VMware NSX**—Juniper Sky ATP identifies the infected virtual machines(VMs) running on VMware NSX and tags these VMs as infected. This action is based on the malware file exchange from the infected VMs, on the command and control communication with known botnet sites on the internet or both.
- **Sky ATP feature support**—–The following Sky ATP features are supported:
  - IMAP e-mail support—You can use the Sky ATP Email Management page to configure e-mail management for IMAP. Enrolled SRX Series devices can transparently submit suspicious e-mails to Sky ATP for inspection and blocking. You can also take action on blocked e-mails, including releasing them and adding them to a blocklist.
  - X-Forwarded-For (XFF) header—XFF is a standard header added to packets by a proxy server that includes the real IP address of the client making the HTTP or HTTPS request. Therefore, if you add trusted proxy server IP addresses to a list in Sky ATP, by matching this list with the IP addresses in the HTTP header (or XFF) for requests sent from SRX Series devices, Sky ATP can determine the originating IP address.
  - Hash lookup—In the Create File Inspection Profile page, the Hash lookup only option is added to the File Categories section.
- **MX routers as enforcement points and DDoS profile support**—MX routers can be added as enforcement points to a Secure Fabric. Also, you can now include a DDoS profile when configuring the threat prevention policies and create a custom feed for DDoS.

  The following actions can be taken when DDoS is detected on the MX router:

  - Block—Block a DDoS attack.
  - Rate Limit Value—Limit the bandwidth on the flow route. You can express the rate limit value in Kbps, Mbps, or Gbps units.
  - Forward To—Configure the routing next hop to forward packets for scrubbing.

Known Issues

This section lists the known issues in Policy Enforcer Release 17.2R1.

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

- Sometime, Cisco ISE AA server does not enable the right SDSN Profile to block an infected host on a CoA accounting message from SDSN Policy Enforcer. The result is that the host gets reauthorized and assigned a new IP and will have access to the network. [PR 1327823]

  Workaround: Go to the Cisco ISE portal for that Infected host IP and manually enable the SDSN Profile and force a reauthorization of the host.

Known Behavior

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.

Resolved Issues

This section lists the issues fixed in Policy Enforcer Release 17.2R1.

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

- If a site is created with a CPPM connector, the site can be created only based on a location-based policy enforcement group. It cannot be created with an IP-based policy enforcement group. [PR 1288247]
- You can configure only one Radius server as a controller for a connector. [PR 1287908]

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: https://prsearch.juniper.net.

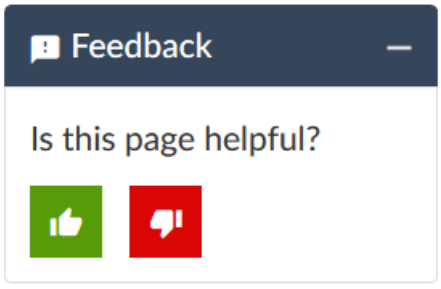
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

26 December, 2017—Revision 1—Junos Space Security Director Release 17.2R1.