Release Notes: Policy Enforcer Release 19.4R1

29 January 2020
Revision 1

Contents

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. 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

Product Compatibility

IN THIS SECTION

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, see the Security Director 19.4R1 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 3.

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)
19.4R1	19.4R1	Junos 15.1X49-D120 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 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 3 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
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

Table 3 on page 4 describes the hardware and software components that are compatible with JATP.

Table 3: Supported Hardware and Software Versions Compatible with JATP

Platform	Hardware Requirements	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

Table 3: Supported Hardware and Software Versions Compatible with JATP *(continued)*

Platform	Hardware Requirements	Software Versions
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.

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 vQFX	Junos 15.1R6 and later Junos 15.1X53-D60.4

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 Juniper Sky ATP Threat Feeds
MX Series	MX240, MX480, MX960	Junos 14.2R1 and later	DDoS
	MX240, MX480, MX960	Junos 18.4R1 and later	C&C *(Mark MX Series router as perimeter device in secure fabric)*
	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 6 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.

Table 7: Third-party Wired and Wireless Access Network *(continued)*

Switch/Server	Notes
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 7 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 Junos OS 19.2R1 and later	vSRX policy based on workload discovery AWS with JATP

To get started with Microsoft Azure, see Getting Started with Microsoft Azure.

Table 10 on page 7 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 19.4R1 only from Policy Enforcer Release 19.3R1. However, Policy Enforcer 19.3R1 can be upgraded from 18.4R1 -> 19.1R1 -> 19.1R2 -> 19.2R1->19.3R1 or 18.1R2 -> 18.2R1 -> 18.3R1 -> 18.4R1 -> 19.1R1 -> 19.1R2 -> 19.2R1 -> 19.3R1.

> **NOTE:** When you upgrade your system from Policy Enforcer Release 19.3R1 to Policy Enforcer Release 19.4R1, you must restart the Policy Enforcer virtual machine using the **reboot** command.

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

- 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 needs 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 19.4R1.

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

- When a host is marked as infected host by Juniper Sky ATP, you cannot resolve the host from the Security Director monitoring page. You can only see the current status. If you try to take any action on the infected host, error occurs.

  Workaround: Use the Juniper Sky ATP portal to take actions on the infected host. PR1458969

Resolved Issues

This section lists the issues fixed in Policy Enforcer Release 19.4R1.

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

- Unable to export Juniper Sky ATP hosts list from Security Director user interface. PR1461157
- The addition of SRX Series Chassis Cluster to a secure fabric site fails for the first time. Workaround: To successfully add the cluster SRX Series to a secure fabric site at the first instance, Junos Space must first discover both the cluster nodes. PR1477825

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.
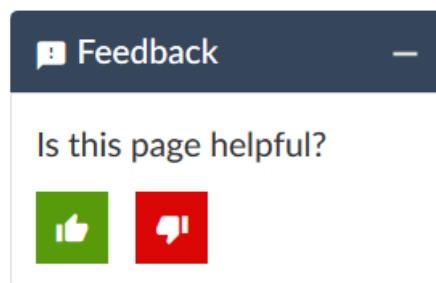
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: 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, 2020—Revision 1—Policy Enforcer Release 19.4R1.