Release Notes: Policy Enforcer Release 18.1R2

26 September 2018
Revision 2

Contents

Introduction | 2

Release Notes for Policy Enforcer | 2

- New and Changed Features | 3
- Product Compatibility | 3
  - Supported Security Director Software Versions | 4
  - Supported Devices | 4
  - Third-Party Wired and Wireless Access Network | 7
  - Juniper Networks Contrail and AWS Specifications | 7
  - Virtual Machine | 8
  - Supported Browser Versions | 8
  - Upgrade Support | 8
- Known Issues | 9
- Known Behavior | 11
- Resolved Issues | 11

Finding More Information | 12

Documentation Feedback | 12

Requesting Technical Support | 13

- Self-Help Online Tools and Resources | 13
- Creating a Service Request with JTAC | 14

Revision History | 14

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 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).

Release Notes for Policy Enforcer

IN THIS SECTION

- New and Changed Features | **3**
- Product Compatibility | **3**
- Known Issues | **9**
- Known Behavior | **11**
- Resolved Issues | **11**

New and Changed Features

This section describes the new features and enhancements in Policy Enforcer Release 18.1R2:

- **Monitor pages for All Hosts and DDoS Feeds**—You can monitor the status of All Hosts and DDoS feeds under the Monitor > Threat Prevention section. To view the All Hosts Status and DDoS Feeds Status pages, you must have the Threat Management privileges or predefined roles enabled.
- **TTL Settings for Custom Feeds**—You can now specify the number of days for the custom feed to be active in the Time to Live (TTL) Settings page, under Configure > Threat Prevention > Custom Feeds. In the Sky ATP with SDSN, Clouds feed only, and No Sky ATP modes, you can configure the TTL settings for dynamic address, allowlist, blocklist, infected host, and DDoS feed types. In the Sky ATP mode, you can configure TTL settings for only dynamic address, allowlist, and blocklist feed types.
- **Proxy server support**—You can configure the proxy server details in Policy Enforcer and all calls to the internet made by Policy Enforcer are routed through the proxy server. Similarly, all calls from Security Director to SkyATP are routed through the proxy server, if the proxy server is configured in Junos Space.
- **Enhancements**—The following enhancements are made to the Sky ATP realm and adding enforcement point pages:
  - In the Add Enforcement Points page, you can choose which firewall device to consider as a perimeter firewall from the firewall devices (SRX and vSRX) list. Only the selected perimeter devices are enrolled to Sky ATP and receive the threat feeds. If you do not choose any firewall device as a perimeter firewall, all the listed firewall devices are enrolled to Sky ATP as perimeter firewalls by default.
  - The following new Sky ATP locations are added to create a Sky ATP realm: Asia Pacific and Canada.

    To know more about the geographic region, see here.

Product Compatibility

IN THIS SECTION

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

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, please see the Security Director 18.1R1 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 (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

Supported Devices

Table 2 on page 5 lists the SRX Series devices that support 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, 4 GB 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 18.1R2, 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	Sky ATP
EX Series	EX9200	Junos 15.1R6 and later	Sky ATP
EX Series	EX3400, EX2300	Junos 15.1R6 and later Junos 15.1X53-D57 and later	Sky ATP
QFX Series	QFX5100, QFX5200 vQFX	Junos 15.1R6 and later Junos 15.1X53-D60.4	Sky ATP

Table 4 on page 6 lists the supported MX Series routers that support the DDoS feed type.

Table 4: Supported MX Routers and Feed Types

Platform	Model	Junos OS Release	Supported Threat Feeds
MX Series	MX240, MX480, MX960 vMX	Junos 14.2R1 and later Junos 16.2R2.8	DDoS

Table 5 on page 6 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

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 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.

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 and AWS Specifications

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

Table 6: 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 7 on page 7 shows the required Policy Enforcer components for AWS.

Table 7: 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

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:

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

Table 8: 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 9: Supported Browser Versions

Browser	Version
Google Chrome	54.*x*
Internet Explorer	11 on Windows 7
Firefox	46 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 18.1R2 only from Policy Enforcer Release 18.1R1. However, Policy Enforcer 18.1R1 can be upgraded from 17.2R1 -> 18.1R1, 17.2R2 -> 18.1R1, or 17.2R1-> 17.2R2 -> 18.1R1.

NOTE: Ensure that the internet connectivity is available for Policy Enforcer. Without the internet connectivity, you cannot upgrade Policy Enforcer successfully.

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 18.1R2.

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

- After a connector-instance is created with only the NGFW option and if you edit the connector-instance to enable Threat Remediation also, the system does not initiate the enrollment of these enforcement points. The vSRX in the service chain of the cloud resource is not added to SkyATP realm for malware scanning.

  Workaround: Once you edit the connector and enable Threat Remediation along with NGFW, navigate to the SkyATP realm page and edit the realm to first remove the site that is associated to the connector-instance and save the changes. Once the system successfully saves the changes, edit the realm again and add back the site to the realm. This triggers the enrollment of the enforcement points in the connector-instance. [PR 1365715]

- On the Edit Connector page, if you want to view the Detailed View page for the second time for the same connector instance, click a different row and then click on the connector instance. Clicking the Detailed View page consecutively does not show any data.

- You cannot edit the generated metadata names, although the tag values are editable.

- Enrolling devices to Sky ATP through Policy Enforcer takes an average of four minutes to complete. Devices are enrolled serially, not in parallel. [PR 1222713]

- The first time you open the Monitoring pages, you receive the **error occurred while requesting the data** message. This also happens the first time you open the Top Compromised Host dashboard widget. As a workaround, click your browser's refresh icon to refresh the page and display the information. [PR 1239956]

- The Top Compromised Hosts widget on the dashboard does not list all the realms. As a workaround, drag and drop another top compromised host widget to the dashboard to display all realms. [PR 1262410]

- An infected host can be blocked by using a custom feed; however, there is no UI to indicate that the host is blocked. To unblock the infected host, remove its IP address from the custom feed. [PR 1292394]

- You can configure only one RADIUS server as a controller for a connector. [PR 1287908]

- When an SRX Series device is used as a Layer 3 gateway for a given host or subnet and a switch is part of the secure fabric, the block and unblock actions might fail when the Policy Enforcement Group (PEG) is created with the location group type. As a workaround, create the PEG with the IP/Subnet group type and associate that PEG to the threat prevention policy. [PR 1296535]

- Even when a device is unavailable (for example, when the device is down), the removal of the device or site from the realm might result in its disenrollment from the realm.
- You cannot delete the configuration for an SRX Series device when the threat prevention policy is associated with multiple PEGs. [PR 1309383]
- Resolving an infected host fails when there is no endpoint session available in the RADIUS server. [PR 1311081]
- The following minor UI issues are observed:
  - For connectors with IP subnets, sometimes the subnets cannot be moved to the list of available subnets.
  - When you modify a threat prevention policy, the GeoIP state changes from **updated** to **assign to groups**. The state should be maintained.
  - Deleting a realm displays an OK message with a red notification window. [PR 1310813]
- On the Create Secure Fabric and Edit Secure Fabric pages, when you search on selected devices and click OK, all devices that are added are deleted, except for the searched devices. Searching might disenroll some of the devices. Always clear the search selection and then click OK. [PR 1342960]
- The port information turns blank when the same host is re-infected and tracked by the Cisco ISE connector. [PR 1346167]
- The old sessions in ClearPass cannot be terminated and, therefore, the actual east-west traffic block cannot be active till those old sessions are reauthenitcated.

  Workaround: Regularly clear the old sessions in ClearPass. [PR 1317503]
- When a policy action is taken on devices on the AWS public cloud, the security groups applied to the end host are not updated on the Security Director > Threat Prevention > Monitoring page. [PR 1347164]
- You cannot delete the next-generation firewall policies when metadata provided only by Policy Enforcer is used as a source or destination address in the firewall policy rule. [PR 1344388]
- If you use an incorrect vSRX tag when creating AWS connector, the connector considers this as another EC2 instance and retains this entry in the connector or endpoint table. [PR 1348406]
- In Cloud only feed mode and Default mode, deleting a site would leave devices pointing to wrong feed source Id. Because of this when the mode is changed to higher modes, SDSN feed downloads may not work correctly.

  Workaround: If you are planning to change the SDSN threat type mode, delete devices that are in site first and then delete the site. [PR 1348376]
- In Threat Prevention Policy page, triggering a Rule analysis may throw an error message stating that an error has occurred while triggering the rule analysis. You must retry the rule analysis.

  Workaround:
  - Click **Update Required** or **View Analysis** after some time. These options successfully trigger the rule analysis.

  - If the problem still persists, in Configure >Firewall Policy >Policies, select a device and click **Publish & Update**. Once this is successful, click **Update Required** or **View Analysis** for the threat prevention policy. [PR 1331439].

- During the device enrollment to SkyATP, security devices might show the enrollment status as Failed along with Retry option.

  Workaround: Check the enrollment status of that particular device after 15 minutes by refreshing the page. If it still shows failed, use the retry option to enroll it. [PR 1350264]

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.
- 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.
- Policy Enforcer supports only the Default global domain in Junos Space Network Management Platform.

Resolved Issues

This section lists the issues fixed in Policy Enforcer Release 18.1R2.

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

- Policy Enforcer automatically discovers the vSRX devices for AWS;, however, the vSRX device is not shown in the available list in the secure fabric. On the Secure Fabric page, mouse over the site to see the corresponding device details. [PR 1342028]
- On the Create Connector page for AWS, it takes about 50 seconds to fetch 10 VPC records from AWS and during this time, if you change the region, it takes additional 50 seconds or more to fetch all the details. [PR 1346533]
- While creating a connector for Juniper Networks Contrail, you must provide infected host security group name in the Quarantine Security Group field. [PR 1349253]

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.

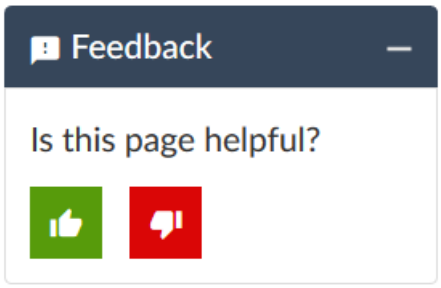
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

12 June, 2018—Revision 1—Policy Enforcer Release 18.1R2.

26 September 2018—Revision 2—Policy Enforcer Release 18.1R2.