

# Release Notes: Policy Enforcer Release 18.3R1

5 November 2018  
Revision R2

## 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 .....	4
Third-Party Wired and Wireless Access Network .....	6
Juniper Networks Contrail and AWS Specifications .....	7
Virtual Machine .....	7
Supported Browser Versions .....	8
Upgrade Support .....	8
Known Issues .....	8
Known Behavior .....	9
Resolved Issues .....	9
Finding More Information .....	10
Documentation Feedback .....	10
Requesting Technical Support .....	10
Self-Help Online Tools and Resources .....	11
Opening a Case with JTAC .....	11
Revision History .....	11

## 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).

## Release Notes for Policy Enforcer

---

- [New and Changed Features on page 2](#)
- [Product Compatibility on page 3](#)
- [Known Issues on page 8](#)
- [Known Behavior on page 9](#)
- [Resolved Issues on page 9](#)

## New and Changed Features

This section describes the new features and enhancements in Policy Enforcer Release 18.3R1:

- **Feed Sources page**—The threat feeds from Juniper Sky ATP and custom feeds are now consolidated on the Feed Sources page, available under [Configure>Threat Prevention>Feed Sources](#).
- **Third-party switch support**—Threat mitigation now supports Pulse Secure appliance in addition to supporting ForeScout CounterACT, HP Aruba ClearPass, and Cisco Identity Services Engine (ISE). The recommended Pulse Secure version is 9.0R3.
- **Update interval on Settings page**—You can now configure the update interval for each feed type on the Setting page, under [Configure>Threat Prevention>Feed Sources>Custom Feed>Settings](#). You can specify how often feeds must be updated in minutes. The default interval is for every 5 minutes.
- **Monitor option for the infected hosts**—The Monitor option is enabled for the infected host profiles along with the existing Block and Quarantine actions. For certain infected hosts, Policy Enforcer will log all the traffic to monitor it.

- **Enhancements to the Juniper Sky ATP Realms**—The following additional information is available for a Juniper Sky ATP Realm under Configure>Threat Prevention>Feed Sources>Sky ATP tab:
  - **Feed Status**—You can see the consolidated status of all the feeds of a Juniper Sky ATP realm. If the status of any one of the feeds is FAILED, then the consolidated status is shown as FAILED.
  - **Last Downloaded**—You can now view the date and time of the last downloaded feed. Hover over the field to see a detailed list.
  - **Token Expiry**—You can see the expiry date and time of a token generated at the Juniper Sky ATP side when a realm is registered. The token will be valid for 1 year. Once the token expires, the status is flipped to Expired. For 30 days prior to the expiry date, the Renew option is enabled to renew the token.
- **Device Feed Status details**—The detailed view of the download status of feeds from various feed sources is available under Monitor>Threat Prevention>Device Feed Status page. You can view the status of feeds for each device.
- **Infected host syslog support**—Policy Enforcer sends system logs for the following events to the remote system log server:
  - Infected host block
  - Infected host clear
  - Infected host quarantine
  - DDoS IP addition
  - DDoS IP deletion
  - Clear DDoS
- **Different time zone support**—You can now configure Policy Enforcer to different time zones based on your region.

## Product Compatibility

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, see the Security Director 18.3R1 release notes.

- [Supported Security Director Software Versions on page 4](#)
- [Supported Devices on page 4](#)
- [Third-Party Wired and Wireless Access Network on page 6](#)
- [Juniper Networks Contrail and AWS Specifications on page 7](#)
- [Virtual Machine on page 7](#)
- [Supported Browser Versions on page 8](#)
- [Upgrade Support on page 8](#)

## 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



**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, GeolP
SRX Series	SRX300, SRX320	Junos 15.1X49-D90 and later	C&C, GeolP
SRX Series	SRX340, SRX345, SRX550M	Junos 15.1X49-D60 and later	C&C, antimalware, infected hosts, GeolP
SRX Series	SRX1500	Junos 15.1X49-D60 and later	C&C, antimalware, infected hosts, GeolP
SRX Series	SRX5400, SRX5600, SRX5800	Junos 15.1X49-D62 and later	C&C, antimalware, infected hosts, GeolP
SRX Series	SRX4100, SRX4200	Junos 15.1X49-D65 and later	C&C, antimalware, infected hosts, GeolP
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



**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 5 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

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

Platform	Model	Junos OS Release	Supported Policy Enforcer Modes
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 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  <b>NOTE:</b> 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 6](#) 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.

**Table 6: Third-party Wired and Wireless Access Network (continued)**

Switch/Server	Notes
Forescout CounterACT	Must be running software version 7.0.0.  <b>NOTE:</b> To obtain an evaluation copy of CounterACT for use with Policy Enforcer, click <a href="#">here</a> .
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 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
vSRX	Junos OS 15.1X49-D120 and later	Microsegmentation and threat remediation with vSRX

Table 8 on page 7 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

### 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)
- 120-GB disk space

**Table 9: 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 10: 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 18.3R1 only from Policy Enforcer Release 18.2R1. However, Policy Enforcer 18.2R1 can be upgraded from 18.1R1 -> 18.2R1, 18.1R2 -> 18.2R1, or 18.1R1 -> 18.1R2 -> 18.2R1.

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 18.3R1.

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

- 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. [PR 1388771]

- 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. [PR 1390546]

- 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. [PR 1391925].



- If you select both threat remediation and next generation firewall as functions for the Contrail connector, vSRX in the Contrail service chain might not get enrolled with Juniper Sky ATP for threat remediation and malware scanning.

Workaround: Delete the connector instance and create the instance again or upload IP addresses through the custom infected host feeds. [PR 1357761]

- When the Infect Host blocking is through nonconnectors, All Host Status report might show that the infected host is yet to be blocked and report it as "pending". This might occur occasionally. However, the required VACL would be already pushed to the switches and the infected host would be blocked. [PR 1358109]
- Processes related to VMWare NSX could be restarting continuously.

Workaround: Use the following CLI commands to stop and restart the NSX micro services. [PR 1383863]

```
service nsxmico stop
service rabbitmq-server start
service nsxmico start
```

## 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.

## Resolved Issues

This section lists the issues fixed in Policy Enforcer Release 18.3R1.

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

- When the policy action changed from block to quarantine, the VACL association on the quarantine VLAN was applied on the output (egress) on the VLAN stanza instead of input. [PR 1376836]
- When the quarantined host moves from one VLAN to another VLAN as part of the VACL update, the "Then" part of the term action is missed. The actual intended traffic redirection does not occur. [PR 1375117]
- Quarantine fails if the EX Series switch has an existing block VACL configuration stanza. [PR 1373771]
- Quarantine fails for the second time for the same VLAN because of the presence of the ALLOW\_ALL\_OTHER\_HOST\_SDSN term. [PR 1361896]

## 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/>.

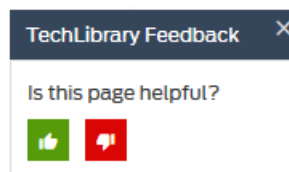
Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at <http://www.juniper.net/techpubs/content-applications/content-explorer/>.

## 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](mailto: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/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

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

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- 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://www.juniper.net/support/requesting-support.html>.

## Revision History

---

11 October, 2018—Revision 1—Policy Enforcer 18.3R1.

5 November, 2018—Revision 2—Policy Enforcer 18.3R1.

Copyright © 2018 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.