

# Policy Enforcer Release Notes

Security Director 16.1  
December 2016  
Revision 1

## Contents

Policy Enforcer Release Notes . . . . .	2
Introduction . . . . .	2
Product Compatibility . . . . .	2
Known Behavior . . . . .	3
Known Issues . . . . .	3
Documentation Feedback . . . . .	4
Requesting Technical Support . . . . .	4
Self-Help Online Tools and Resources . . . . .	5
Opening a Case with JTAC . . . . .	5
Revision History . . . . .	5

## Policy Enforcer Release Notes

---

- [Introduction](#)
- [Product Compatibility](#)
- [Known Behavior](#)
- [Known Issues](#)

### Introduction

Juniper's Software-Defined Secure Network (SDSN) platform leverages the entire network, not just perimeter firewalls, as a threat detection and security enforcement domain. Policy Enforcer provides the ability to orchestrate policies created by Juniper's Sky Advanced Threat Prevention cloud-based malware detection solution and distributes them to EX Series switches, as well as to Juniper virtual and physical SRX Series firewalls.

### Product Compatibility

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

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

The following table lists the supported EX Series ethernet switches and QFX Series switches.

Platform	Model	Junos OS version	Supported Policy Enforcer Modes
EX Series	EX4200, EX 2200, EX3200, EX3300	Junos 15.1R1.5 and above	Sky ATP with PE
EX Series	EX4300, EX9200	Junos 14.1X53-D30 and above	Sky ATP with PE
EX Series	EX3400, EX 2300	Junos 15.1X53-D50 and above	Sky ATP with PE
QFX Series	QFX5100, QFX 5200	Junos 14.1X53-D40 and above	Sky ATP with PE

Security Director and Policy Enforcer are best viewed on the following browsers.

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

For Security Director requirements, please see the Security Director 16.1R1 release notes.

## Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Policy Enforcer for Security Director 16.1R1.

- SRX High Availability is not supported in this release of Policy Enforcer.

## Known Issues

This section lists the known issues in hardware and software for Policy Enforcer.

- When changing the mode from Sky ATP to Sky ATP with Policy Enforcer within Security Director, SRX Series devices previously enrolled with Sky ATP realms are removed and disenrolled. The enroll configuration is not removed from the SRX Series devices when you change the Policy Enforcer password immediately after changing the mode type. Instead, change the Policy Enforcer password at the same time that you change the mode type. [1238810]
- Devices must be licensed for Sky ATP before they can be assigned to a Sky ATP realm. If devices are not enrolled in Sky ATP, they will still be shown as enrolled in the Threat Prevention Realms page and the Devices > Security Devices page. [1237566]
- Select **Monitor > Threat Management > Hosts** to view infected hosts. Clicking a URL in the list should display details about that host but instead displays a warning **This host**

**is not being tracked currently because there have been no malicious events for this host in recent history.** As a workaround, click your browser refresh button to refresh the page and to display the host details. [1240071]

- On the Secure Fabric landing page, the tool tip for **SkyATP Enroll Status** always says **Device failed to enroll**. Instead, refer to the icon. A green icon indicates success; a red icon indicates failure. [1239977]
- Enrolling devices to Sky ATP through Policy Enforcer takes an average of four minutes to complete. [1222713]
- The first time you open the Monitoring pages, you will receive an **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 refresh button to refresh the page and display the information. [1239956]
- When in the **Sky ATP with PE** mode and after assigning a PEG to a threat policy with the malware profile, if you select the analysis preview option the page displays a spinning wheel and no data is shown. As a workaround, cancel out of this page and then publish and update the policy without the preview option. You can view the changes in the CLI after the job completes. [1240070]
- Tooltip text is missing from Setup Wizard steps. [1240629]
- Adding whitelists or blacklists to Sky ATP through the Threat Intelligence Open API results in Policy Enforcer failing to download feeds from Sky ATP. As a workaround, delete the whitelist or blacklist category from Sky ATP through the Threat Intelligence Open API and restart the service. If you want to add a whitelist or blacklist again, add it through the custom feeds workflow from within Security Director, or use Policy Enforcer's APIs instead of the Sky ATP Threat Intelligence Open API. [1247141]

---

## 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 rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/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 <http://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: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

## 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 <http://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 <http://www.juniper.net/support/requesting-support.html>.

---

## Revision History

December 2016—Revision 1—Policy Enforcer

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the 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.