Policy Enforcer Release Notes

Security Director 16.2
May 2017
Revision 3

Contents

Policy Enforcer Release Notes 2
Introduction 2
Product Compatibility 2
Supported Security Director Software Versions 2
Supported Devices 2
Supported Browser Versions 4
Installing the Policy Enforcer 16.2R1 Software Patch 4
Known Behavior 4
New and Changed Features 5
Aggregation Switch Not Needed 5
Email Attachments 5
Log File Debugging 5
Custom Feed Refresh From a Remote Server 5
Known Issues 5
Documentation Feedback 6
Requesting Technical Support 6
Self-Help Online Tools and Resources 6
Opening a Case with JTAC 7
Revision History 7

Policy Enforcer Release Notes

- Introduction

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

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, please see the Security Director 16.2 release notes.

- Supported Security Director Software Versions on page 2
- Supported Devices on page 2
- Supported Browser Versions on page 4

Supported Security Director Software Versions

Policy Enforcer is supported only on specific Security Director software versions as shown in Table 1 on page 2.

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

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 2 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 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

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 running 15.1X49-D80 does not support the SMTP e-mail attachment scan feature.

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	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

Supported Browser Versions

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

Table 4: Supported Browser Versions

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

Installing the Policy Enforcer 16.2R1 Software Patch

This section describes how to install the Policy Enforcer 16.2R1 software patch.

NOTE: You must have Security Director 16.2R1 already installed prior to installing this software patch. No prior installation of Policy Enforcer is required; if you do have Policy Enforcer installed (any version), this software patch will overwrite it. If you have a multi-node Junos Space fabric, you must perform these steps on each individual node.

1. Download the **Policy-Enforcer-16.2R1-Patch.sh** file from http://www.juniper.net/support/downloads/?p=sdpe to the **/tmp** folder of the Junos Space Network Management Platform server.

2. Change directory to the **/tmp** folder.

3. Change the permissions of the **Policy-Enforcer-16.2R1-Patch.sh** file to allow read, write and execute permissions for everyone using the following command:

   ```
   chmod 777 Policy-Enforcer-16.2R1-Patch.sh
   ```

4. Execute the installation script using the following command:

   ```
   sh Policy-Enforcer-16.2R1-Patch.sh
   ```

   It may take a few minutes for the script to complete.

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Policy Enforcer for Security Director 16.2R1.

- SRX High Availability is supported in this release of Policy Enforcer.

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

New and Changed Features

This section describes the new features and enhancements to existing features in Policy Enforcer version 16.2R1.

- Aggregation Switch Not Needed on page 5
- Email Attachments on page 5
- Log File Debugging on page 5
- Custom Feed Refresh From a Remote Server on page 5

Aggregation Switch Not Needed

Starting with Policy Enforcer version 16.2R1, an aggregation switch is not required. Policy Enforcer blocks the infected host at the switch level with just an SRX Series device and a Layer 2 or Layer 3 switch.

Email Attachments

Email management for SMTP lets enrolled devices transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, the file is given a threat score between 0-10 with 10 being the most malicious. In addition, emails are checked against administrator-configured blacklists and whitelists. If an email matches the blacklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

Log File Debugging

A REST API now lets you access Policy Enforcer log files and extract them as a single .zip file.

Custom Feed Refresh From a Remote Server

Using feeds from Sky ATP and custom feeds you configure, ingress and egress traffic is monitored for suspicious content and behavior. Starting with Security Director 16.2, you can use custom feeds from a remote server in addition to feeds from a local system.

Known Issues

This section lists the known issues in hardware and software in Policy Enforcer version 16.2R1.

- 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]

- The **top compromised hosts** widget in 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. [1262410]
- The **Top Scanned File Categories**, **Top Infected File Categories**, and **Top Malware** dashboard widgets do not show any data even though data is present. [1266118]

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**. 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