

Release Notes: Policy Enforcer Release 17.1R2

25 October 2017

Contents

Introduction	2
Installing the Policy Enforcer 17.1R2 Software Patch	2
Product Compatibility	3
Supported Security Director Software Versions	3
Supported Devices	3
Third-Party Wired and Wireless Access Network	5
Virtual Machine	5
Supported Browser Versions	5
Upgrade Support	6
New and Changed Features	6
Known Behavior	6
Known Issues	7
Resolved Issues	9
Documentation Feedback	9
Requesting Technical Support	10
Self-Help Online Tools and Resources	10
Opening a Case with JTAC	10
Revision History	11

Introduction

Policy Enforcer orchestrates threat remediation workflows based on threat detection by Juniper Sky ATP solution or custom threat feeds and enforces these policies on Juniper's EX/QFX switches as well as 802.1x enabled third party wired and wireless switches. In addition, Policy Enforcer integrates with VMware NSX solution to deliver advanced Next Generation Firewall (NGFW) feature set using vSRX for VMware micro-segmentation deployments

Installing the Policy Enforcer 17.1R2 Software Patch

A Policy Enforcer 17.1R2 software patch is available to address some ClearPass issues and resolves the following two problem reports:

- The Clearpass connector does not block infected hosts after upgrading to Policy Enforcer 17.1R2. [1314308]
- After upgrading to Policy Enforcer 17.1R2 and using the third-party switch as a connector, editing the Connector page may cause the blocking infected host feature to no longer work. [1311544]



NOTE: You must have Security Director 17.1R2 and Policy Enforcer 17.1R2.3 already installed prior to installing this software patch.

To install the Policy Enforcer 17.1R2 software patch:

1. Download the Policy_Enforcer-17.1R2-16_PE_patch.x86_64.rpm file from <http://www.juniper.net/support/downloads/?p=sdpe#sw>.
2. On your Policy Enforcer virtual appliance, change directory to where you downloaded the RPM bundle and install it using the following command:

```
[root@hostname~]# rpm -Uvh filename.rpm
```

For example:

```
[root@hostname~]# rpm -Uvh Policy_Enforcer-17.1R2-16_PE_patch.x86_64.rpm
```

It may take a few minutes to install the software patch. Until the installation completes and services are restarted, do not make any Policy Enforcer-related changes within Security Director. Once installed, the Policy Enforcer screens within Security Director and any schema changes are updated. The configuration settings you used when you deployed the Policy Enforcer VM are retained.

Product Compatibility

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, please see the Security Director 17.1R2 release notes.

- [Supported Security Director Software Versions on page 3](#)
- [Supported Devices on page 3](#)
- [Third-Party Wired and Wireless Access Network on page 5](#)
- [Virtual Machine on page 5](#)
- [Supported Browser Versions on page 5](#)
- [Upgrade Support on page 6](#)

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 (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
17.1R1	17.1R1	Junos 15.1X49-D80 and above
17.1R2	17.1R2	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 3](#) 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 300, SRX 320	Junos 15.1X49-D90 and above	CC, Geo IP

Table 2: Supported SRX Series Devices and Feed Types (*continued*)

Platform	Model	Junos OS Release	Supported Threat Feeds
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 does not support the SMTP e-mail attachment scan feature.

In the 17.1R2 release, Policy Enforcer supports SRX Series devices running Junos OS Release 17.3R1. Junos OS Release 17.3R1 supports the same Policy Enforcer features as that of Junos OS Release 15.1X49-D70 Release. As such, SMTP e-mail is not supported.

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, EX4300	Junos 15.1R6 and above	Sky ATP with PE
EX Series	EX9200	Junos 15.1R6 and above	Sky ATP with PE
EX Series	EX3400, EX 2300	Junos 15.1R6 and above	Sky ATP with PE
QFX Series	QFX5100, QFX 5200	Junos 15.1R6 and above	Sky ATP with PE

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 6.6.0 software version.
Cisco ISE	Must be running 2.1 software version.



NOTE: Juniper Networks tested Cisco 2950 with 12.2(55)SE7 and Cisco WS-C3850-48P with 03.02.01.SE.

If you are using the Juniper Networks EX4300 to integrate with the third-party switches, the EX4300 must be running Junos OS 15.1R6 or later.

Virtual Machine

Policy Enforcer is delivered as an OVA or 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 4: 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 5: Supported Browser Versions

Browser	Version
Google Chrome	54.x
Internet Explorer	11 on Windows 7

Table 5: Supported Browser Versions (*continued*)

Browser	Version
Firefox	46 and above

Upgrade Support

Upgrading Policy Enforcer follows the same rules as for upgrading Security Director. You can upgrade only from the most previously released version. This includes the minor releases (R1, R2, etc.) For example, Policy Enforcer 17.1R2 can be upgraded only 17.1R1. The upgrade path to Policy Enforcer 17.1R2 is as follows: 16.1R1 -> 16.2R1 -> 17.1R1 -> 17.1R2.

For more information on the Security Director upgrade path, see [Upgrading Security Director](#).

New and Changed Features

This section describes the new features and enhancements to existing features in Policy Enforcer Release 17.1R2

- **CISCO ISE Support**—Policy Enforcer now supports threat remediation use cases with Cisco ISE as controller in addition to Clearpass.
- **Support PEG for Third-Part Switch Connectors**—Policy Enforcer now supports Policy Enforcement Group (PEG) for third-party connectors using IP addresses.
- **Policy Enforcer KVM**—You can now install Policy Enforcer with the kernel-based virtual machine (KVM) hypervisor in addition to the VMware ESXi hypervisor.
- **No Selection Mode**—If you make no selection under Sky ATP Configuration Type, a “no selection” mode is now available to provide threat prevention using the custom feed support already in Policy Enforcer. This mode does not require you to have a Sky ATP account.
- **Custom Feed Infected Host per Site**—You can now upload custom infected host feeds for one or more sites. This is supported in all modes except for Sky ATP mode.

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Policy Enforcer for Security Director 17.1R2.

- Policy Enforcer supports only the default global domain in Junos Space Network Management.
- When editing a Policy Enforcement Group, you cannot change the Group type. If you need to change the Group type, delete the Policy Enforcement Group and create a new one.
- Secure Fabric has connectors and devices as enforcement points that can be assigned to a site through the list builder.

- When a switch fails to update the VLAN access control list (VACL) and the infected host has an error failed state, the switch will continue to try to update the VACL until it is successful.
- If an infected host is moved from a wired network interface controller (NIC) to wireless or from a wireless to a wired NIC, it is not automatically blocked until there is another malware detection at the new NIC. This is due to the change in the MAC address.
- When an infected host *A* is moved from *site1* to *site2* and *site2* has no prior infected hosts, then host *A* is blocked in *site2* only when the next network-wide poll for the endpoints is triggered. By default this is 24 hours from the last triggered time. You can change this polling time in the PE Settings window in Security Director.
- The third-party adapter package for KVM displays version 17.1R1 instead of 17.1R2. For example:

```
[user@host]# cat /etc/redhat-release
CentOS release 6.8 (Final)
Policy Enforcer Package Version: 17.1R2-3-
3rd Party Adapter Package Version: 17.1R1-24
```

Known Issues

This section lists the known issues in hardware and software in Policy Enforcer version 17.1R2.

- Enrolling devices to Sky ATP through Policy Enforcer takes an average of four minutes to complete. Enrolling devices are done serially, not in parallel. [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]
- Connectors assigned to a site cannot be deleted. You must first unassign it from the site and then go to the Connectors window (**Administration > Policy Enforcer > Connectors**) to delete it.
- An infected host can be blocked 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. [1292394]
- You can configure only one Radius server as a controller for a connector. [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 may fail when the 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. [1296535]

- Even when a device is unavailable (for example, the device is down), the removal of the device or site from the realm may state it as a successful dis-enroll.
- If you entered incorrect credentials in the Realm window, the **OK** button is disabled. As a workaround, close this window, re-open it and enter your correct credentials. [1310817]
- After upgrading the Policy Enforcer software, logs are incorrectly appended to the latest logs (config_server.log.1) instead of following the log file rotation method. [1310695]
- Disenrolling the site in the infected custom feed does not remove the firewall filters from the switch for IP addresses that are in the custom feed. As a workaround, remove all the IPs from the custom feed and then disenroll the site from the Infected host feed page. [1309819]
- In a multi-site scenario with a Radius server as the DOT1X for AAA services, assigning all sites and the enforcement points (firewalls and switches) within a single Sky ATP realm may cause issues in picking the correct threat prevention infected host policy. As a workaround, after creating a connector for the Radius Controller and assigning it to all the sites, register or create a unique Sky ATP realm and associate it with a site. [1309881]
- After upgrading Policy Enforcer from 17.1R1 to 17.1R2, resolving a blocked host in the Monitoring page does not clear the firewall filters. As a workaround, manually resolve all the hosts in the monitoring page prior to upgrading to 17.1R2. After the upgrade, set the host's investigation status back to **Open**. This will re-apply the firewall filters onto the switch. [1309908]
- When multiple sites are configured with multiple realms (and all sites have connectors), the Sky ATP policy overwrites all SRX Series devices in the site instead of the specific SRX Series device. [1308737]
- If you go directly to the summary page instead of following each step in the guided setup, the summary page may appear blank. As a workaround, go follow each step in the guided setup. [1309366]
- You cannot delete the configuration for an SRX Series device when the threat prevention policy is associated with multiple PEGS. [1309383]
- Resolving an infected host fails when there is no endpoint session available in the Radius server. [1311081]
- The following minor UI issues are present:
 - For connectors with IP subnets, sometimes the subnets cannot be moved to available.
 - 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 or popup. [1310813]

- The Clearpass connector does not block infected hosts after upgrading to Policy Enforcer 17.1R2. [1314308] (This issue is fixed with the Policy Enforcer 17.1R2 software patch. See [“Installing the Policy Enforcer 17.1R2 Software Patch” on page 2](#))
- After upgrading to Policy Enforcer 17.1R2 and using the third-party switch as a connector, editing the Connector page may cause the blocking infected host feature to no longer work. [1311544] (This issue is fixed with the Policy Enforcer 17.1R2 software patch. See [“Installing the Policy Enforcer 17.1R2 Software Patch” on page 2](#))

Resolved Issues

This section lists the issues fixed in hardware and software in Policy Enforcer Release 17.1R2.

- If a vSRX is properly enrolled in Sky ATP and you create a site within Policy Enforcer with that vSRX and a connector, the secure fabric page for that site shows the vSRX enroll status as failed. [1284258]
- If a site is created with a CPPM connector, the site can be created only based on a location-based policy enforcement group. It cannot be created with an IP-based policy enforcement group. [1288247]
- Moving the C&C Threat Score slider in the Threat Prevention Policy window (**Configure > Threat Prevention > Policy**), for example from 10 to 8, may cause the Actions dropdown menu to appear empty. Click the arrow in the Actions menu to see the options. [1296098]
- Removing a site from a realm may remove the SRX Series device from the Secure Fabric site. As a workaround, re-add the device to the site. [1295460]
- Create a threat prevention policy with the following options and save the policy:
 - Include malware in policy
 - HTTP file download enabled
 - SMTP attachments enabled
 - Threat score set to Permit 1-10

When you edit this same policy, the threat score now shows Permit 1-9 and Block 10. As a workaround, change the threat score to Permit 1-10 before you save. [1297962]

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: <https://prsearch.juniper.net/>
- Find product documentation: <http://www.juniper.net/documentation/>
- 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://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 <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

July 2017—Revision 1—Policy Enforcer

Copyright © 2017 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.