Release Notes

Published
2025-11-16

Policy Enforcer Release Note 23.1R1

JUNIPER NETWORKS | Engineering Simplicity

Table of Contents

Introduction | 1

Finding More Information | 1

Known Behavior | 2

Known Issues | 3

New and Changed Features | 4

Product Compatibility | 4

Resolved Issues | 11

Hot Patch Releases | 12

Revision History | 14

Introduction

Junos Space® Security Director Policy Enforcer orchestrates threat remediation workflows based on the Juniper Networks Advanced Threat Prevention (ATP Cloud) solution, command-and-control (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. On the MX Series router, only DDoS policy is pushed by Policy Enforcer/Security Director. The allowlist, blocklist, and continuity check (CC) policies must be manually configured. Policy Enforcer integrates with Advanced Threat Prevention Appliance (ATP Appliance) to provide a continuous, multistage detection and analysis of Web, e-mail, and lateral spread traffic moving through the network.

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.

NOTE: For details on Security Director Insights as the integrated Policy Enforcer, see Configure Security Director Insights as Integrated Policy Enforcer.

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/.

Known Behavior

This section lists the known behavior in Policy Enforcer Release 23.1R1.

- An error may be displayed in the Status column on the vCenter Task pane when deploying vSRX in host based mode for east-west traffic. To overcome this resource pool error, you must enable DRS mode on the cluster in which you deploy vSRX device.
- When you open the vSRX console through vCenter, ignore the displayed warning.
- You can associate a tenant with only one VRF instance.
- A realm can have all the sites either with tenants or without tenants.
- Tenants and VRF-based feeds are supported only on MX Series devices.
- To take action on the feeds from Policy Enforcer, you must configure policies on the MX Series device through the CLI and not from Security Director.
- To upload certificates for Policy Enforcer, to be used in certificate-based authentication mode of Junos Space, Junos Space must be in password authentication mode to complete the Policy Enforcer settings workflow. The mode can be switched to certificate-based authentication after the Policy Enforcer settings are completed.
- 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.
- ATP Appliance zone creation or assignment cannot be done in the General Setup Wizard.
- Ensure that the time difference between the ATP Appliance and the SRX Series devices is less than 20 seconds to avoid the enrollment failure.
- When the vSRX device is disenrolled with ATP Appliance and enrolled again, you might see the device shown twice in the Feed Sources page in Security Director.
- When the feed source is JATP, you must change the Infected host state in the ATP Appliance portal. There are no Dashboard widgets to show the ATP Appliance related threats or Infected hosts in Security Director.

- During the ATP Appliance enrollment, it may state that Juniper ATP Cloud license is not present. You can ignore this warning.
- For SRX Series devices in a chassis cluster, both primary and secondary chassis cluster nodes need to be discovered in Security Director before adding them to secure fabric. If only one chassis cluster node is discovered and added to secure fabric, the feed download does not work after failover to secondary node.

Known Issues

This section lists the known issues in Policy Enforcer Release 23.1R1.

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

- You may not be allowed to edit the ClearPass connector password on the Policy Enforcer Connector page.

  Workaround: Delete the connector and add it again with the right credentials. [PR1464446]

- Sites associated with tenants (multitenant sites) are shown while creating policy enforcement group. This is applicable for guided setup also. UC-334
- You will be unable to add enforcement points to site after changing the mode when the certificate based authentication is enabled. UC-368

  After changing the Policy Enforcer mode in Policy Enforcer settings page, go to **Junos Space® Network Management Platform** > **Users** > **pe_user** and manually upload the client certificate.

  OR

  Go to Junos Space Network Management Platform and change the mode to Password Authentication and perform Policy Enforcer settings again.

- When you download feeds to a device after the realm is deleted and added again in Policy Enforcer, an internal server error is identified.

  Workaround:

  On Junos OS CLI on the SRX Series device, execute the command `request services security-intelligence download`. [PR1586287]

New and Changed Features

There are no new features and enhancements for Policy Enforcer Release 23.1R1.

For new features and enhancements in Security Director, see Junos Space Security Director Release Notes.

Product Compatibility

IN THIS SECTION

- Supported Security Director Software Versions | 4
- Supported Devices | 5
- Third-Party Wired and Wireless Access Network | 8
- Juniper Networks Contrail, Microsoft Azure, and AWS Specifications | 9
- Virtual Machine | 10
- Supported Browser Versions | 11
- Upgrade Support | 11

This section describes the supported hardware and software versions for Policy Enforcer. For Security Director requirements, see Junos Space Security Director 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 5.

Table 1: Supported Security Director Software Versions

Policy Enforcer Software Version	Compatible with Security Director Software Version	Junos OS Release (Juniper ATP Cloud Supported Devices)
23.1R1	23.1R1	Junos OS Release 15.1X49-D120 or Junos OS Release 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 ATP Cloud 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 5 for more information.

Table 2: Supported SRX Series Firewalls with Juniper ATP Cloud 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, 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

Table 2: Supported SRX Series Firewalls with Juniper ATP Cloud and Feed Types *(Continued)*

Platform	Model	Junos OS Release	Supported Threat Feeds
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

Table 3 on page 6 describes the hardware and software components that are compatible with JATP.

Table 3: Supported Hardware and Software Versions Compatible with JATP

Platform	Hardware	Software Versions
vSRX		Junos 19.1R1.6 and above
SRX Series	SRX320, SRX300	Junos 19.1R1 and above
SRX Series	SRX4100, SRX4200, SRX4600	Junos 15.1X49-D65 and above for SRX4100 and SRX4200 Junos 18.1R1 and above for SRX4600

Table 3: Supported Hardware and Software Versions Compatible with JATP *(Continued)*

Platform	Hardware	Software Versions
SRX Series	SRX340, SRX345, SRX550m	Junos 15.1X49-D60 and above
SRX Series	SRX5800, SRX5600, SRX5400	Junos 15.1X49-D50 and above
SRX Series	SRX1500	Junos 15.1X49-D33 and above

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 4 on page 7 lists the supported EX Series and QFX Series switches.

Table 4: Supported EX Series Ethernet Switches and QFX Series Switches

Platform	Model	Junos OS Release
EX Series	EX4200, EX2200, EX3200, EX3300, EX4300	Junos 15.1R6 and later
EX Series	EX9200	Junos 15.1R6 and later
EX Series	EX3400, EX2300	Junos 15.1R6 and later Junos 15.1X53-D57 and later
QFX Series	QFX5100, QFX5200 vQFX	Junos 15.1R6 and later Junos 15.1X53-D60.4

Table 5 on page 8 lists the supported MX Series routers that support the DDoS and C&C feed types.

Table 5: Supported MX Routers and Feed Types

Platform	Model	Junos OS Release	Supported Feed Types
MX Series	MX240, MX480, MX960	Junos 14.2R1 and later	DDoS
	MX240, MX480, MX960	Junos 18.4R1 and later	C&C *(Mark MX Series router as perimeter device in secure fabric).* The C&C feed is global and is overridden if the C&C custom feed is set on Policy Enforcer.
	vMX	Junos 16.2R2.8	-

Table 6 on page 8 shows the supported SDN and cloud platforms.

Table 6: 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

Table 7 on page 9 lists the third-party support and required server.

Table 7: 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.
Forescout CounterACT	Must be running software version 7.0.0. **NOTE**: To obtain an evaluation copy of CounterACT for use with Policy Enforcer.
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, Microsoft Azure, and AWS Specifications

Table 8 on page 9 shows the required components for Juniper Networks Contrail.

Table 8: 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 9 on page 10 shows the required Policy Enforcer components for AWS.

Table 9: AWS Support Components

Model	Software Version	Supported Policy Enforcer Mode
vSRX	Junos OS 15.1X49-D100.6 and later Junos OS 19.2R1 and later	vSRX policy based on workload discovery AWS with JATP

To get started with Microsoft Azure, see Getting Started with Microsoft Azure.

Table 10 on page 10 shows the required Policy Enforcer components for Microsoft Azure.

Table 10: Microsoft Azure Support Components

Model	Software Version	Supported Policy Enforcer Mode
vSRX	Junos OS 15.1X49-D110.4 and later	vSRX policy based on workload discovery

Virtual Machine

Policy Enforcer is delivered as an open virtual appliance (OVA) or a kernel-based virtual machine (KVM) package to be deployed inside your VMware ESX or Quick Emulator (QEMU)/KVM network with the following configuration:

- 4 CPUs
- 16 GB RAM
- 300 GB disk space

Table 11: 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

Table 11: Supported Virtual Machine Versions *(Continued)*

Virtual Machine	Version
QEMU/KVM	CentOS Release 7.9 or later

Supported Browser Versions

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

Table 12: Supported Browser Versions

Browser	Version
Google Chrome	75.*x*
Firefox	67.0 and later

Upgrade Support

You can upgrade to Policy Enforcer Release 23.1R1 from Policy Enforcer Release 22.3R1.

For complete upgrade instructions, see Upgrading Your Policy Enforcer Software.

For more information about the Security Director upgrade path, see Upgrading Security Director.

Resolved Issues

This section list the issues fixed in Policy Enforcer Release 23.1R1.

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

- When you configure Policy Enforcer with **api/v2/controller/configs** an error message is displayed. [PR1573126]
- The Finish button does not work as expected in adding the realms workflow. [PR1574592]
- The NSX micro service is not available in Security Director Insights Policy Enforcer. [PR1655449]
- The CLI fails to generate, when you select **Deny** or **Reject** in the Adaptive Threat Profile page. [PR1694539]

For resolved issues in Security Director, see Junos Space Security Director Release Notes.

Hot Patch Releases

IN THIS SECTION

- Installation Instructions | 12
- Resolved Issues | 13

This section describes the new features, installation procedure, and resolved issue in Policy Enforcer Release 23.1R1 hot patch.

NOTE: Security vulnerabilities are addressed in the Policy Enforcer Release 23.1R1 hot patch.

Installation Instructions

During hot patch installation, the script performs the following operations:

- Stops controller, feed-collector and feed-provider services of Policy Enforcer.
- Backs up existing configuration files and libraries.

- Updates the Red Hat Package Manager (RPM) file for Policy Enforcer.
- Restarts the controller, feed-collector and feed-provider.

> **NOTE**: You must install the hot patch on Policy Enforcer Release 23.1 or on any previously installed hot patch. The hot patch installer backs up all the files which are modified or replaced during hot patch installation.

Perform the following steps in the CLI:

1. Download the Policy Enforcer 23.1R1 Patch Policy_Enforcer-23.1R1-XX-PE-Upgrade.rpm from the download site.
   Here, XX is the hot patch version.
2. Copy the `Policy_Enforcer-23.1R1-XX-PE-Upgrade.rpm` file to the `/tmp` location.
3. Verify the checksum of the hot patch for data integrity:
   `md5sum Policy_Enforcer-23.1R1-XX-PE-Upgrade.rpm`.
4. Install the rpm using the command:
   rpm -Uvh Policy_Enforcer-23.1R1-XX-PE-Upgrade.rpm

> **NOTE**: We recommend that you install the latest available hot-patch version, which is the cumulative patch.

Resolved Issues

Table 13 on page 13 lists the resolved issues in the Policy Enforcer Release 23.1R1 Hot Patch.

Table 13: Resolved Issues in the Policy Enforcer Release 23.1R1 Hot Patch

PR	Description	Hot Patch Version
PR1814706	The ports 443 and 8080 of the standalone Policy Enforcer server support TLS1.0 and TLS1.1.	v2

Table 13: Resolved Issues in the Policy Enforcer Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1825122	Dynamic object feed fails to update the last updated timestamp.	v2
PR1570837	Policy Enforcer fails to resolve the IP address of the AWS resources after fetching the tags from AWS resources.	v1

Revision History

Release	Release Date	Updates
Policy Enforcer Release 23.1R1	18 October, 2023—Revision 1	Intial Release Notes
Policy Enforcer Release 23.1R1 Hot Patch V1	26 February, 2024—Revision 2	Added Resolved Issues
Policy Enforcer Release 23.1R1 Hot Patch V2	29 October, 2024—Revision 3	Added Resolved Issues

Copyright © 2024 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.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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. Copyright © 2025 Juniper Networks, Inc. All rights reserved.