

# Security Director

---

## Policy Enforcer

Published  
2020-09-25

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

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.

*Security Director Policy Enforcer*

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

## About the Documentation | x

Documentation and Release Notes | x

Documentation Conventions | x

Documentation Feedback | xiii

Requesting Technical Support | xiii

Self-Help Online Tools and Resources | xiv

Creating a Service Request with JTAC | xiv

## 1

## Overview of Policy Enforcer and Sky ATP

Juniper Networks Software-Defined Secure Network Overview | 16

Benefits of Juniper Networks Software-Defined Secure Network | 17

Policy Enforcer Overview | 17

Supported Topologies | 19

Role-Based Access Control for Threat Management | 19

Benefits of Policy Enforcer | 20

Sky ATP Overview | 22

## 2

## Concepts and Configuration Types to Understand Before You Begin

Policy Enforcer Components and Dependencies | 26

Policy Enforcer Configuration Concepts | 31

Sky ATP Configuration Type Overview | 32

Features By Sky ATP Configuration Type | 35

Available UI Pages by Sky ATP Configuration Type | 36

Comparing the SDSN and non-SDSN Configuration Steps | 38

## 3

## Installing Policy Enforcer

**Policy Enforcer Installation Overview | 41**

**Deploying and Configuring the Policy Enforcer with OVA files | 42**

**Installing Policy Enforcer with KVM | 49**

Installing Policy Enforcer with virt-manager | 50

Installing Policy Enforcer with virt-install | 51

Configuring Policy Enforcer Settings | 52

Connecting to the KVM Management Console | 58

**Policy Enforcer Ports | 59**

**Identifying the Policy Enforcer Virtual Machine In Security Director | 61**

**Obtaining a Sky ATP License | 62**

**Creating a Sky ATP Cloud Web Portal Login Account | 63**

**Loading a Root CA | 64**

**Upgrading Your Policy Enforcer Software | 65**

## 4

## Configuring Policy Enforcer Settings and Connectors

**Policy Enforcer Settings | 70**

**Policy Enforcer Connector Overview | 72**

Benefits of Policy Enforcer Connector | 74

**Creating a Policy Enforcer Connector for Public and Private Clouds | 74**

**Creating a Policy Enforcer Connector for Third-Party Switches | 84**

**Editing and Deleting a Connector | 88**

Editing a Connector | 89

Deleting a Connector | 90

**Viewing VPC or Projects Details | 91**

**Integrating ForeScout CounterACT with Juniper Networks SDSN | 93**

Configuring the DEX Plug-in | 94

Configuring the Web API Plug-in | 98

Creating ForeScout CounterACT Connector in Security Director | 100

ClearPass Configuration for Third-Party Plug-in | 104

Cisco ISE Configuration for Third-Party Plug-in | 111

5

**Guided Setup for Sky ATP with SDSN**

Using Guided Setup for Sky ATP with SDSN | 124

6

**Guided Setup for Sky ATP**

Using Guided Setup for Sky ATP | 128

7

**Guided Setup for No Sky ATP (No Selection)**

Using Guided Setup for No Sky ATP (No Selection) | 132

8

**Configuring Sky ATP with SDSN (without Guided Setup)**

Configuring Sky ATP with SDSN (Without Guided Setup) Overview | 137

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 138

Secure Fabric Overview | 141

Adding Enforcement Points | 142

| 144

Editing or Deleting a Secure Fabric | 146

Policy Enforcement Groups Overview | 146

Creating Policy Enforcement Groups | 147

Threat Prevention Policy Overview | 149

Benefits of Threat Prevention Policy | 150

Creating Threat Prevention Policies | 151

Threat Policy Analysis Overview | 157

Geo IP Overview | 158

Creating Geo IP Policies | 158

9

## **Configuring Sky ATP (without Guided Setup)**

**Configuring Sky ATP (No SDSN and No Guided Setup) Overview | 162**

**Sky ATP Realm Overview | 163**

**Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 164**

**Threat Prevention Policy Overview | 166**

Benefits of Threat Prevention Policy | 168

**Creating Threat Prevention Policies | 169**

10

## **Configuring Cloud Feeds Only**

**Configuring Cloud Feeds Only | 176**

11

## **Configuring No Sky ATP (No Selection) (without Guided Setup)**

**Secure Fabric Overview | 179**

| 180

**Creating Policy Enforcement Groups | 182**

**Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist | 184**

**Creating Custom Feeds, Infected Host | 189**

**Threat Prevention Policy Overview | 193**

Benefits of Threat Prevention Policy | 194

**Creating Threat Prevention Policies | 195**

12

## **Threat Prevention - Configure**

**Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 204**

**Sky ATP Realm Overview | 206**

**Modifying Sky ATP Realm | 207**

**Custom Feed Sources Overview | 209**

Benefits of Custom Feed Sources | 209

**Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist | 210**

Example: Creating a Dynamic Address Custom Feed and Firewall Policy	215
Creating Custom Feeds, Infected Host	217
Creating Custom Feeds, DDoS	220
Configuring TTL Settings for Custom Feeds	223
Sky ATP Email Management Overview	224
Sky ATP Email Management: SMTP Settings	226
Sky ATP Email Management: Allowlist and Blocklists	229
Email Management: Configure IMAP	230
Sky ATP Malware Management Overview	233
File Inspection Profiles Overview	233
Creating File Inspection Profiles	235
Creating Allowlist and Blocklists	236
Implementing Threat Policy on VMWare NSX	238
VMWare NSX Integration with Policy Enforcer and Sky ATP Overview	238
Implementation of Infected Hosts Policy Overview	240
Registering NSX Micro Service as Policy Enforcer Connector Instance Overview	241
Before You Begin	241
Infected Hosts Workflow in VMware vCenter Server	241
Configuring VMware NSX with Policy Enforcer	244
Example: Creating a Firewall Rule in VMWare vCenter Server Using SDSN_BLOCK Tag	246

## Threat Prevention- Monitor

Policy Enforcer Dashboard Widgets	252
Infected Hosts Overview	253
Infected Host Details	254
Command and Control Servers Overview	256
Command and Control Server Details	257
HTTP File Download Overview	259

## **HTTP File Download Details | 260**

File Summary | 261

HTTP Downloads | 262

## **SMTP Quarantine Overview | 262**

## **Email Attachments Scanning Overview | 264**

## **Email Attachments Scanning Details | 265**

File Summary | 266

## **IMAP Block Overview | 267**

## **File Scanning Limits | 269**

## **All Hosts Status Details | 270**

## **DDoS Feeds Status Details | 272**

14

## **Troubleshooting**

### **Policy Enforcer Log File Locations | 275**

### **Troubleshooting Common Policy Enforcer Problems | 275**

Troubleshooting Policy Enforcer Installation | 276

Troubleshooting Sky ATP Realms and Enrolling Devices | 277

Troubleshooting Threat Policies and Policy Enforcement Groups | 277

HTTPS-Based Malware Not Detected | 278

### **Troubleshooting ClearPass Issues | 278**

Viewing Logs Files | 279

Configuration Issues | 281

Error Code 500 | 282

Unable to Block Infected Endpoint | 282

Unable to Quarantine Infected Endpoint | 284

Unable to Clear Blocked or Quarantined Endpoint | 284

15

## **Migration Instructions for Spotlight Secure Customers**

### **Moving From Spotlight Secure to Policy Enforcer | 286**

Spotlight Secure and Policy Enforcer Deployment Comparison | 286

License Requirements | 287



Sky ATP and Spotlight Secure Comparison Table | **287**

Migrating Spotlight Secure to a Policy Enforcer Configuration Overview | **288**

Installing Policy Enforcer | **289**

Configuring Advanced Threat Prevention Features: Spotlight Secure/Policy Enforcer  
Comparison | **295**

# About the Documentation

## IN THIS SECTION

- Documentation and Release Notes | x
- Documentation Conventions | x
- Documentation Feedback | xiii
- Requesting Technical Support | xiii

Use this guide to configure Policy Enforcer component of Junos Space Security Director. Policy Enforcer integrates with Sky ATP to provide centralized threat management and monitors your software-defined secure network.

## Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

## Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub</b> <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

## GUI Conventions

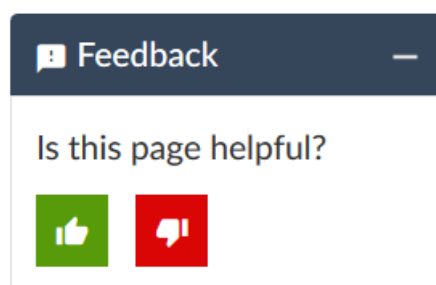
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use 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 Juniper Care or Partner Support Services 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 <https://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/>
- Create a service request online: <https://myjuniper.juniper.net>

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

## Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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://support.juniper.net/support/requesting-support/>.

# 1

CHAPTER

## Overview of Policy Enforcer and Sky ATP

---

Juniper Networks Software-Defined Secure Network Overview | 16

Policy Enforcer Overview | 17

Benefits of Policy Enforcer | 20

Sky ATP Overview | 22

---

# Juniper Networks Software-Defined Secure Network Overview

The Juniper Networks Software-Defined Secure Network (SDSN) provides end-to-end network visibility, allowing enterprises to secure their entire network, both physical and virtual. Using threat detection and policy enforcement, an SDSN solution automates and centrally manages security in a multi-vendor environment.

The Juniper Networks SDSN solution is comprised of the following components:

- A threat detection engine—Cloud-based Sky ATP detects known and unknown malware. Known threats are detected using feed information from a variety of sources, including command control server and GeolP. Unknown threats are identified using various methods such as sandboxing, machine learning, and threat deception.
- Centralized policy management—Junos Space Security Director, which also manages SRX Series devices, provides the management interface for the SDSN solution called Policy Enforcer. Policy Enforcer communicates with Juniper Networks devices and third-party devices across the network, globally enforcing security policies and consolidating threat intelligence from different sources. With monitoring capabilities, it can also act as a sensor, providing visibility for intra- and inter-network communications.
- Expansive policy enforcement—In a multi-vendor enterprise, SDSN enforces security across Juniper Networks devices, cloud-based solutions, and third-party devices. By communicating with all enforcement points, SDSN can quickly block or quarantine threat, preventing the spread of bi-lateral attacks within the network.
- User intent-based policies—Create policies according to logical business structures such as users, user groups, geographical locations, sites, tenants, applications, or threat risks. This allows network devices (switches, routers, firewalls and other security devices) to share information, resources, and when threats are detected, remediation actions within the network.

With user intent-based policies, you manage clients based on business objectives or user and group profiles. The following are two examples of a user intent policy:

- Quarantine users in HR in Sunnyvale when they're infected with malware that has a threat score greater than 7.
- Block any user in Marketing when they contact a Command and Control (C&C) server that has a threat score greater than 6 and then send an e-mail to an IT administrator.

Using user intent-based policies allows network devices (switches, routers, firewalls and other security devices) to share information, resources, and when threats are detected, remediation actions within the network.

Unlike rule-based policies, which can contain several rules, you can define only one set of parameters for each user intent-based policy defined on a device.



## Benefits of Juniper Networks Software-Defined Secure Network

- **Management and visibility** - Enables you to view traffic across the network, dynamically deploy security policies and block threats. SDSN manages the entire network infrastructure as a single enforcement domain, thereby providing enforcement points across the network. Uses machine learning and data mining tools to offer effective threat management while producing detailed data access and user activity reports.
- **Comprehensive security** - Ensures that the same security policies are applied across all of the devices in the network. It extends security to each layer of the network, including routers, switches, and firewalls.
- **Protection from advanced malware** - Provides automated offense identification and consolidates the threat intelligence with threat hunting activities to simplify and focus attention on the highest priority offenses.
- **Automated policy or enforcement orchestration** - Provides real-time feedback between the security firewalls. Reduces the risk of compromise and human error by allowing you to focus on maximizing security and accelerating operations with a simple, concise rule set.
- **Scalability** - Supports up to 15,000 devices.
- **Third-party integration** - Provides APIs to integrate with the ecosystem partners for capabilities such as cloud access security, network access control, and endpoint protection, and additional threat intelligence feeds.

### RELATED DOCUMENTATION

*Understanding Juniper SDSN for VMware NSX Integration*(Micro-segmentation via vSRX Integration with NSX Manager and Junos Space Security Director)

[Policy Enforcer Overview | 17](#)

[Policy Enforcer Components and Dependencies | 26](#)

## Policy Enforcer Overview

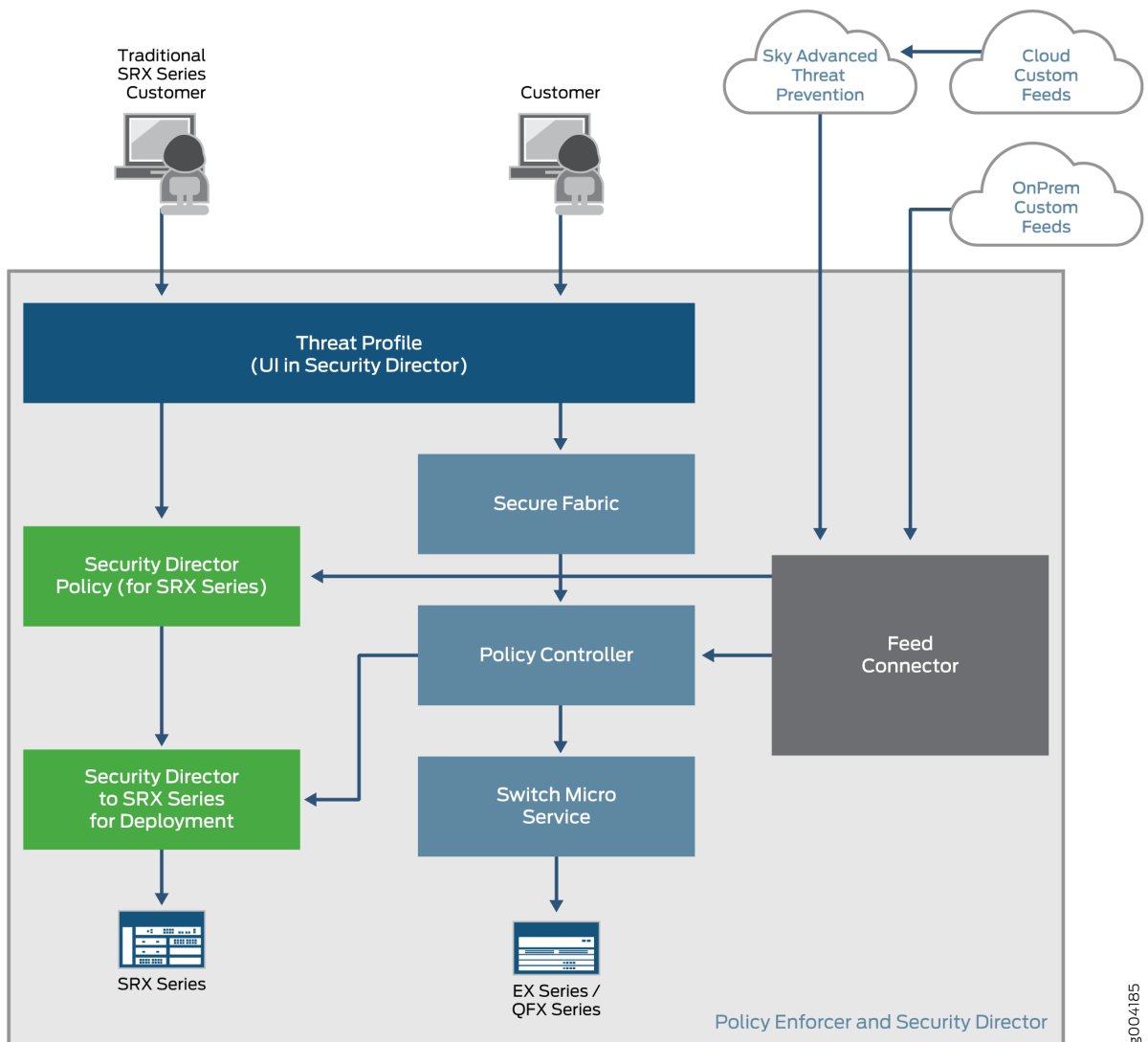
Policy Enforcer, a component of the Junos Space Security Director user interface, integrates with Sky ATP to provide centralized threat management and monitoring to your software-defined secure network, giving you the ability to combine threat intelligence from different solutions and act on that intelligence from one management point.

It also automates the enforcement of security policies across the network and quarantines infected endpoints to prevent threats across firewalls and switches. Working with Sky ATP, it protects

perimeter-oriented threats as well as threats within the network. For example, if a user downloads a file from the Internet and that file passes through an SRX Series firewall, the file can be sent to the Sky ATP cloud for malware inspection. If the file is determined to be malware, Policy Enforcer identifies the IP address and MAC address of the host that downloaded the file. Based on a user-defined policy, that host can be put into a quarantine VLAN or blocked from accessing the Internet.

Figure 1 on page 18 illustrates the flow diagram of Policy Enforcer over a traditional SRX Series configuration.

Figure 1: Comparing Traditional SRX Customers to Policy Enforcer Customers



## Supported Topologies

Policy Enforcer supports the following topologies:

- Client to Layer 2 switch to Layer 3 SRX (IRB)
- Client to Layer 2 switch to Layer 3 switch (IRB)
- Client to Layer 2/Layer 3 switch (IRB)

## Role-Based Access Control for Threat Management

The Policy Enforcer must have the following predefined roles or privileges to perform the threat management. Users without these privileges will not see any pages related Policy Enforcer and Sky ATP in Security Director UI.

Threat Management has the following task groups and tasks:

- Threat Management Policy
  - Create Threat Management Policy
  - Modify Threat Management Policy
  - Delete Threat Management Policy
- Dynamic Address Group
  - Create Dynamic Address
  - Modify Dynamic Address
  - Delete Dynamic Address

To create and view the user roles, select **Network Management Platform > Role Based Access Control > User Account**.

### RELATED DOCUMENTATION

---

[Policy Enforcer Components and Dependencies | 26](#)

---

[Policy Enforcer Configuration Concepts | 31](#)

---

[Sky ATP Overview | 22](#)

---

[Policy Enforcer Installation Overview | 41](#)

---

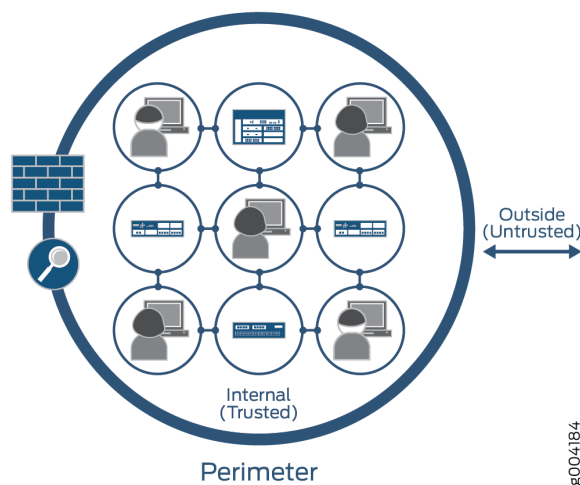
[Using Guided Setup for Sky ATP with SDSN | 124](#)

---

## Benefits of Policy Enforcer

Most enterprise computer security revolves around creating a wall around the perimeter of an organization. See [Figure 2 on page 20](#).

Figure 2: Perimeter-Defined Security Model



With this perimeter oriented security, networks are built with an inherently trusted model where the applications or users connecting to a network (for example, VLAN) can fundamentally talk to each other and network security solutions like firewalls and Intrusion Prevention Systems (IPS) are deployed in the perimeter to provide security. Firewalls are often configured with all possible rules in an effort to prevent unknown malware, application and network attacks from penetrating the enterprise. This architecture is based on a model where it is assumed that “Everything already inside the network is fundamentally trusted” and “Everything outside the network is untrusted” so the perimeter is the location where all security controls are deployed.

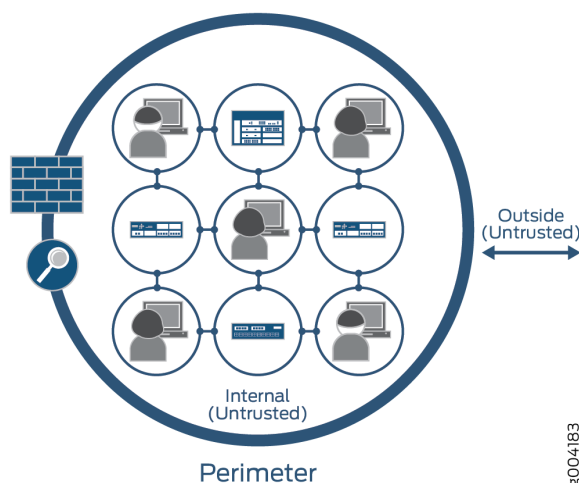
This architecture is consistent across data centers, and campus and branch configurations. Unfortunately, there are flaws to this security architecture. They don’t help in protecting against internal threats. Despite the popularity of firewalls, the sophistication of applications and malware in recent years has found a way to circumvent perimeter defenses. Once inside the enterprise, these threats can easily spread; where someone’s infected laptop or desktop could make Enterprise networks a botnet army and become a source of internal and external attacks. Enterprises can protect against internal threats by deploying multiple layers of firewalls, but that requires careful planning since it is difficult to take all internal traffic through a separate layer of firewalls.

The security framework become a highly fragmented approach due to multiple administrators, management systems and reliance on a lot of manual coordination among different administrators and systems:

- There is a network security team that manages security policies on perimeter firewalls primarily to manage external threats.
- There is a network operations team, that typically manages security policies by using network and application isolation to protect against internal attacks and unauthorized access.
- Then there is third team, an IT team, that manages end-points such as laptops, desktops and application servers to make sure that they have the correct security posture.

In contrast, Policy Enforcer and Software-Defined Secure Networks (SDSN), see [Figure 3 on page 21](#), simplifies network security by providing protection based on logical policies and not security devices. Policy Enforcer does provide perimeter security, but it's no longer just protecting the inside from the outside. The fact that somebody is connected to the internal network does not mean that they can get unrestricted access to the network. This model is fundamentally more secure because even if one application on the network is compromised, companies can limit the spread of that infection/threat to other potentially more critical assets inside the network.

**Figure 3: Policy Enforcer and Software-Defined Security Model**



Policy Enforcer is a model where the information security is controlled and managed by security software. New devices are automatically covered by security policies, instead of having to identify it's IP address as with other models. Because it's software-defined, environments can be moved without affecting security policies and controls already in place. Other advantages include:

- Better and more detailed security—By providing better visibility into network activity, you can respond faster to cyber threats and other security incidents. Threats can be detected faster by leveraging threat intelligence from multiple sources (including third-party feeds) and the cloud. A central control lets you analyze security challenges without interfering with standard network activity and to distribute security

policies throughout your organization. For example, you can selectively block malicious traffic while allowing normal traffic flow.

- Scalability and cost savings—A software-based model allows you to quickly and easily scale security up or down based on your immediate needs all without having to add or subtract hardware that is expensive to buy and maintain.
- Simpler solution—Hardware security architectures can be complex due to the servers and specialized physical devices that are required. In a software model, security is based on policies. Information can be protected anywhere it resides without depending on its physical location.

#### RELATED DOCUMENTATION

---

[Policy Enforcer Overview | 17](#)

---

[Sky ATP Overview | 22](#)

---

[Using Guided Setup for Sky ATP with SDSN | 124](#)

---

[Using Guided Setup for Sky ATP | 128](#)

---

[Configuring Sky ATP with SDSN \(Without Guided Setup\) Overview | 137](#)

## Sky ATP Overview

Sky ATP is a cloud-based solution that integrates with Policy Enforcer. Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time. Your sensitive data is secured even though it is in a cloud shared environment. Security administrators can update their defenses when new attack techniques are discovered and distribute the threat intelligence with very little delay.

Sky ATP offers the following features:

- Communicates with firewalls and switches to simplify threat prevention policy deployment and enhance the anti-threat capabilities across the network.
- Delivers protection against “zero-day” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Checks inbound and outbound traffic with policy enhancements that allow users to stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral movement.
- Provides deep inspection, actionable reporting, and inline malware blocking.
- Provides feeds for GeoIP, C&C, allowlist and blocklist, infection hosts, custom configured feeds and file submission.

**NOTE:** Whitelist and allowlist has been used interchangeably throughout this document. Similarly, blacklist and blocklist are also used interchangeably.

Figure 4 on page 23 lists the Sky ATP components.

Figure 4: Sky ATP Components

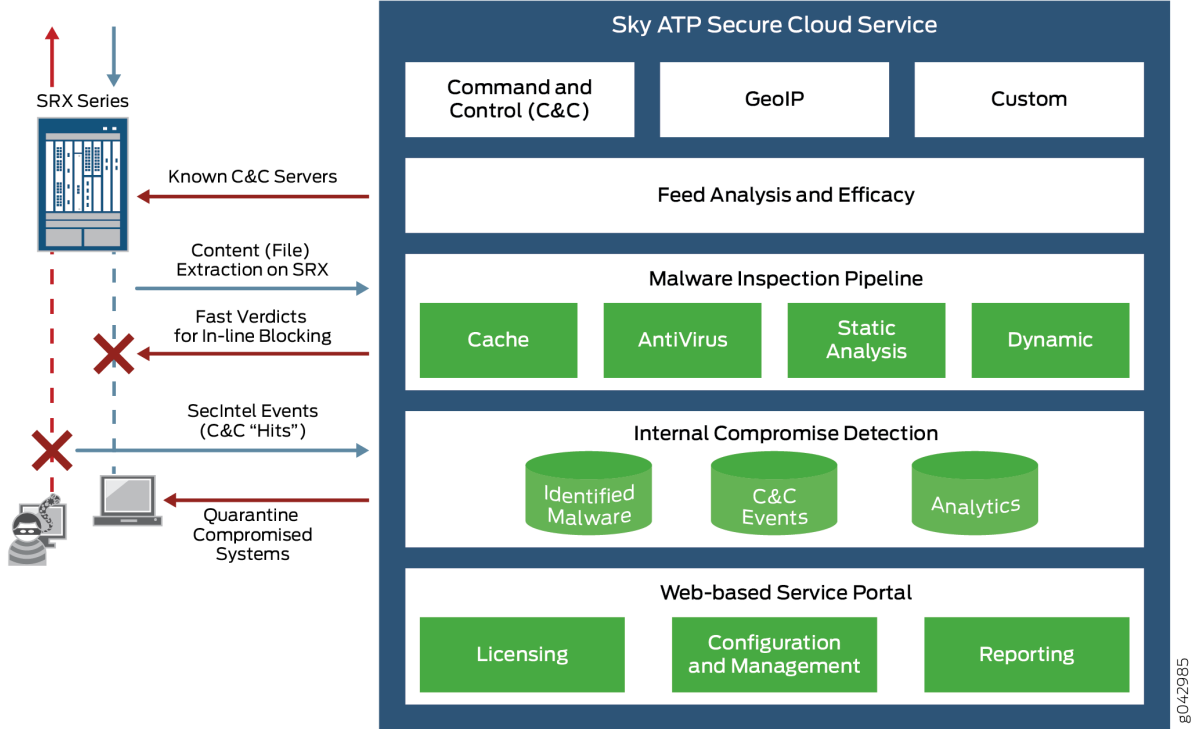


Table 3 on page 23 briefly describes each Sky ATP component's operation.

Table 3: Sky ATP Components

Component	Operation
Command and control (C&C) cloud feeds	C&C feeds are essentially a list of servers that are known command and control for botnets. The list also includes servers that are known sources for malware downloads. See <a href="#">"Command and Control Servers Overview"</a> on page 256.
GeoIP cloud feeds	GeoIP feeds is an up-to-date mapping of IP addresses to geographical regions. This gives you the ability to filter traffic to and from specific geographies in the world.

Table 3: Sky ATP Components (*continued*)

Component	Operation
Infected host cloud feeds	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or other exhibit other symptoms. See <a href="#">“Infected Hosts Overview” on page 253</a> .
Custom Feeds	Lists you customize by adding IP addresses, domains, and URLs to your own lists. See <a href="#">“Custom Feed Sources Overview” on page 209</a> .
Allowlist and blocklists	An allowlist is simply a list of known IP addresses that you trust and a blocklist is a list that you do not trust. See <a href="#">“Creating Allowlist and Blocklists” on page 236</a> .
Malware inspection pipeline	Performs malware analysis and threat detection.
Internal compromise detection	Inspects files, metadata, and other information.

## RELATED DOCUMENTATION

---

[Sky ATP Realm Overview | 163](#)


---

[Using Guided Setup for Sky ATP | 128](#)


---

[Configuring Sky ATP \(No SDSN and No Guided Setup\) Overview | 162](#)



# 2

CHAPTER

## Concepts and Configuration Types to Understand Before You Begin

---

Policy Enforcer Components and Dependencies | **26**

Policy Enforcer Configuration Concepts | **31**

Sky ATP Configuration Type Overview | **32**

Features By Sky ATP Configuration Type | **35**

Available UI Pages by Sky ATP Configuration Type | **36**

Comparing the SDSN and non-SDSN Configuration Steps | **38**

---

## Policy Enforcer Components and Dependencies

The Policy Enforcer management interface is a component of Junos Space Security Director and requires the following to be configured and deployed:

- **Junos Space Virtual Appliance**—Junos Space is a comprehensive network management solution that simplifies and automates management of Juniper Networks switching, routing, and security devices. Junos Space Virtual Appliance includes the complete Junos Space software package as well as the Junos OS operating system. It requires users to create a virtual machine (VM) in order to deploy the appliance.
- **Security Director**—Junos Space Security Director provides centralized and orchestrated security policy management through a web-based interface. Security administrators can use Security Director to manage all phases of the security policy life cycle for every SRX Series physical and virtual device.
- **Policy Enforcer**—Policy Enforcer itself is installed on a VM and uses RESTful APIs to communicate with both Security Director and Sky Advanced Threat Prevention (ATP). Policy Enforcer contains two components:
  - **Policy Controller**—Defines the logical grouping of the network into secure fabric, automates the enrollment of SRX Series devices with Sky ATP, and configures the SRX firewall policies.
  - **Feed Connector**—Aggregates the cloud and customer feeds and is the server for SRX Series devices to download feeds.
- **Sky ATP**—Sky ATP employs a pipeline of technologies in the cloud to identify varying levels of risk, and provides a higher degree of accuracy in threat protection. It integrates with SRX Series gateways to deliver deep inspection, inline malware blocking, and actionable reporting.

Sky ATP's identification technology uses a variety of techniques to quickly identify a threat and prevent an impending attack, including:

- **Rapid cache lookups** to identify known files.
- **Dynamic analysis** that involves unique deception techniques applied in a sandbox to trick malware into activating and self-identifying.
- **Machine-learning algorithms** to adapt to and identify new malware.
- **SRX Series device**—SRX Series gateways provide security enforcement and deep inspection across all network layers and applications. Users can be permitted or prohibited from accessing specific business applications and Web applications, regardless of the network ports and protocols that are used to transmit the applications.

Figure 5 on page 27 illustrates how the components in the Policy Enforcer Deployment Model interact.

Figure 5: Components of the Policy Enforcer Deployment Model

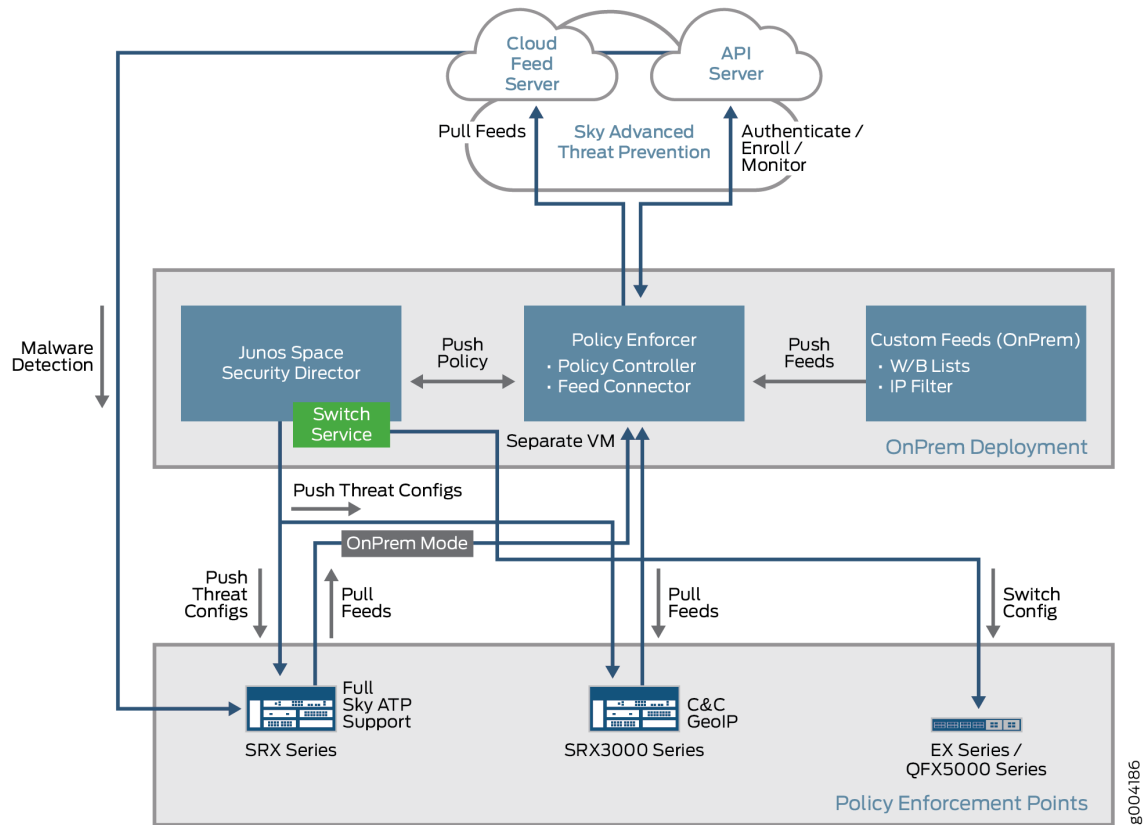
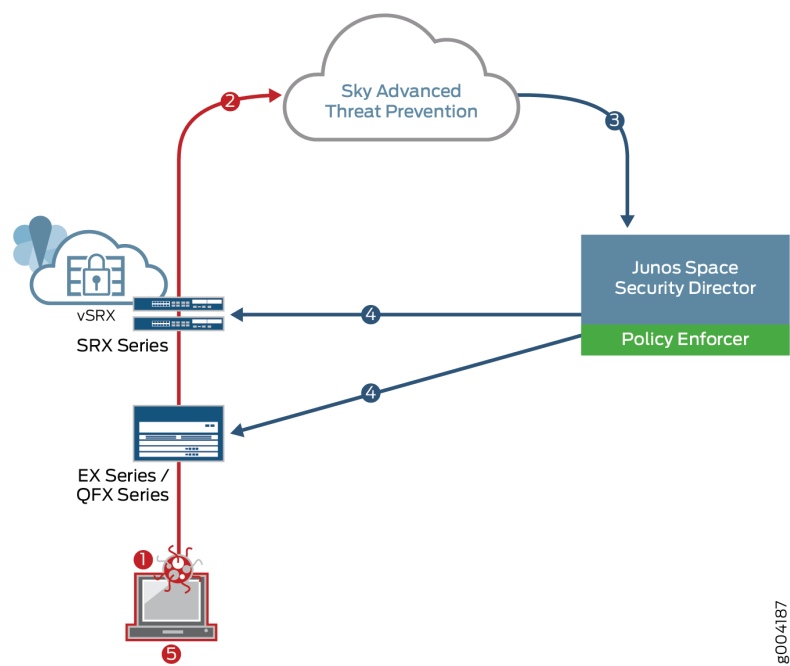


Figure 6 on page 28 shows an example infected endpoint scenario to illustrate how some of the components work together.

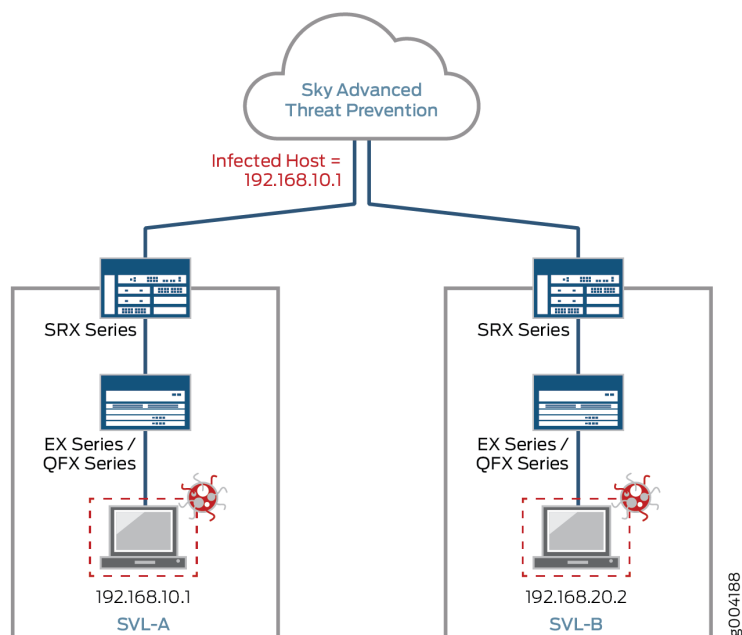
Figure 6: Blocking an Infected Endpoint



Step	Action
1	A user downloads a file from the Internet.
2	Based on user-defined policies, the file is sent to the Sky ATP cloud for malware inspection.
3	The inspection determines this file is malware and informs Policy Enforcer of the results.
4	The enforcement policy is automatically deployed to the SRX Series device and switches.
5	The infected endpoint is quarantined.

Policy Enforcer can track the infected endpoint and automatically quarantine it or block it from accessing the Internet if the user moves from one campus location to another. See [Figure 7 on page 29](#).

Figure 7: Tracking Infected Endpoint Movement

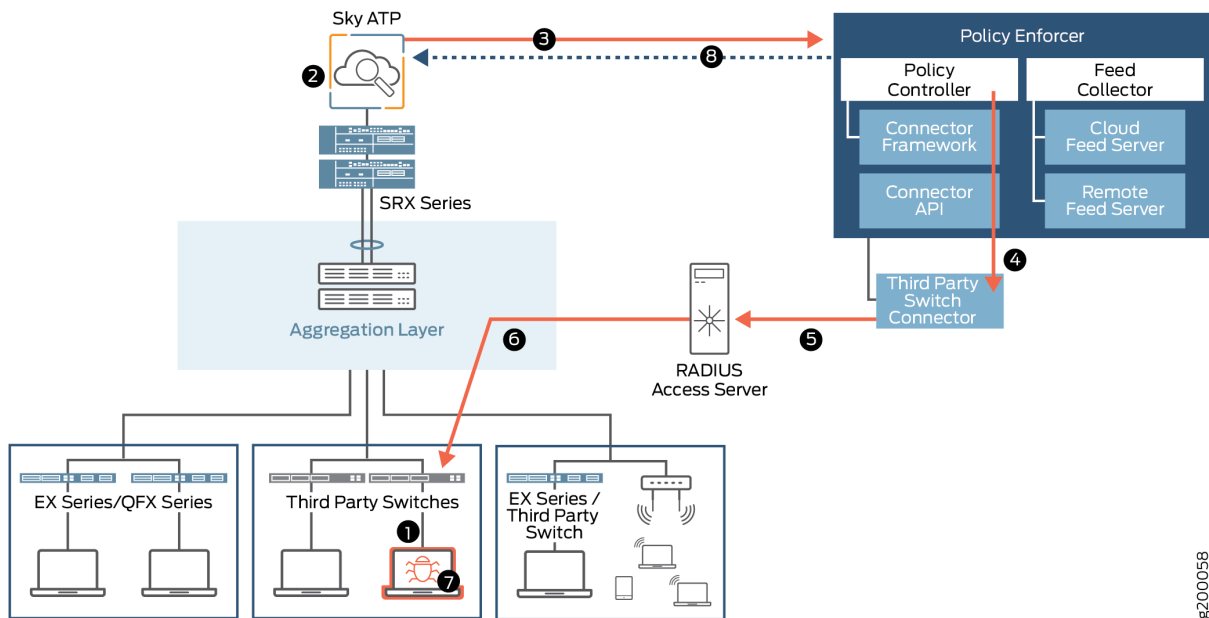


In this example, Sky ATP identifies the endpoint as having an IP address of 192.168.10.1 and resides in SVL-A. The EX Series switch quarantines it because it has been labeled as an infected host by Sky ATP. Suppose the infected host physically moves from location SVL-A to location SVL-B. The EX Series switch (in SVL-B) microservice tracks the MAC address to the new IP address and automatically quarantines it. Policy Enforcer then informs Sky ATP of the new MAC address-to-IP address binding.

Policy Enforcer can also quarantine infected hosts even if those hosts are connected to third-party switches, as shown in [Figure 8 on page 30](#).

For Policy Enforcer to provide threat remediation to endpoints connecting through third-party devices, it must be able to authenticate those devices and determine their state. It does this using a tracking and accounting threat remediation plug-in to gather information from a RADIUS server and enforce policies such as terminate session and quarantine. For more information, see [“Policy Enforcer Connector Overview” on page 72](#)

Figure 8: Third-Party Switch Support



8200058

Step	Action
1	An end-user authenticates to the network through IEEE 802.1X or through MAC-based authentication.
2	Sky ATP detects the end point is infected with malware and adds it to the infected host feed.
3	Policy Enforcer downloads the infected host feed.
4	Policy Enforcer enforces the infected host policy using the Connector. See <a href="#">"Policy Enforcer Connector Overview" on page 72</a> .
5	The Connector queries the RADIUS server for the infected host endpoint details and initiates a Change of Authorization (CoA) for the infected host.
6	The CoA can be either block or quarantine the infected host.
7	The enforcement occurs on the NAC device the infected host is authenticated with.
8	Policy Enforcer communicates the infected host details back to Sky ATP.

## RELATED DOCUMENTATION

[Policy Enforcer Overview](#) | 17

---

[Policy Enforcer Configuration Concepts | 31](#)

---

[Sky ATP Overview | 22](#)

---

[Policy Enforcer Installation Overview | 41](#)

---

[Using Guided Setup for Sky ATP with SDSN | 124](#)

---

[Using Guided Setup for Sky ATP | 128](#)

---

[Configuring Sky ATP with SDSN \(Without Guided Setup\) Overview | 137](#)

---

## Policy Enforcer Configuration Concepts

You have some options for how you can approach the initial setup of Sky ATP and Policy Enforcer. There is a “Guided Setup” approach which walks you through the necessary steps for getting the product up and running. This is the recommended approach. If you prefer, you can manually configure each part of the product.

Either way, before you begin the configuration, you need to understand the concepts behind the configuration items required to successfully deploy threat management policies across your network. These items include security realms for Sky ATP, secure fabric for sites, and policy groups for endpoints. These are explained in this section.

- **Security Realm**—When configuring Sky ATP or Policy Enforcer with Sky ATP, there are Realm selection fields at the top of several pages. A security realm is a group identifier for an organization used to restrict access to Web applications. You must create at least one security realm to login into Sky ATP. Once you create a realm, you can enroll SRX Series devices into the realm. You can also give more users (administrators) permission to access the realm.

If you have multiple security realms, note that each SRX Series device can only be bound to one realm, and users cannot travel between realms.

- **Policy Enforcement Groups**—A policy enforcement group is a grouping of endpoints to which threat prevention policies are applied. Create a policy enforcement group by adding endpoints (firewalls, switches, subnets, set of end users) under one common group name and later applying a threat prevention policy to that group.

Some information to know about enforcement groups is as follows: Determine what endpoints you will add to the group based on how you will configure threat prevention, either according to location, users and applications, or threat risk. Endpoints cannot belong to multiple policy enforcement groups.

- **Threat Prevention Policies**—Once you have a Threat Prevention Policy, you assign one or more Policy Enforcement Groups to it. Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control servers, GeolP, infected hosts, and malware. Using feeds from Sky ATP and custom feeds you configure, ingress and egress traffic is monitored for suspicious

content and behavior. Based on a threat score, detected threats are evaluated and action may be taken once a verdict is reached.

- **Secure Fabric**—For your configuration you must create one or more sites for your secure fabric. Secure fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices), used in policy enforcement groups. When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. This is how threat prevention is aggregated across your secure fabric.

Some information to know about sites is as follows: When you create a site, you must identify the perimeter firewalls so you can enroll them with Sky ATP. If you want to enforce an infected host policy within the network, you must assign a switch to the site. Devices cannot belong to multiple sites.

## RELATED DOCUMENTATION

[Sky ATP Configuration Type Overview | 32](#)

[Using Guided Setup for Sky ATP with SDSN | 124](#)

[Using Guided Setup for Sky ATP | 128](#)

[Policy Enforcer Overview | 17](#)

[Sky ATP Overview | 22](#)

# Sky ATP Configuration Type Overview

Sky ATP with Policy Enforcer can be used in four different configuration types, which will be explained here.

**NOTE:** The license you purchase determines if you can use the available configurations and feature sets for your selected Sky ATP Configuration Type.

Configuration Type is set here in the UI: **Administration > Policy Enforcer > Settings**.

The following Sky ATP Configuration Types and corresponding workflows are available. Workflows are the items you configure for each selection.

**Sky ATP with SDSN**—This is the full version of the product. All Policy Enforcer features and threat prevention types are available.



Here is the Sky ATP with SDSN workflow:

- Secure Fabric
- Policy Enforcement Group
- Sky ATP Realm
- Threat Prevention Policies for the following threat types:
  - C&C Server
  - Infected Hosts
  - Malware
  - Geo IP

**Sky ATP**—This includes all threat prevention types, but does not include the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer. All enforcement is done through SRX Series Device policies.

Here is the Sky ATP workflow:

- Sky ATP Realm
- Threat Prevention Policies for the following threat types:
  - C&C Server
  - Infected Hosts
  - Malware
  - Geo IP

**Cloud feeds only**—The prevention types available are command and control server, infections hosts, and Geo IP feeds. Policy Enforcer Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies are also available. All enforcement is done through SRX Series Device policies.

Here is the Cloud feeds only workflow:

- Secure Fabric
- Policy Enforcement Group
- Sky ATP Realm
- Threat Prevention Policies for the following threat types:
  - C&C Server
  - Infected Hosts
  - Geo IP

**No Sky ATP (no selection)**—You would make no Sky ATP selection to configure SDSN using custom feeds. Custom feeds are available for dynamic address, allowlist, blocklist, and infected hosts. With this setting, there are no feeds available from Sky ATP, but the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer are available. Infected hosts is the only prevention type available.

Here is the No selection workflow:

- Secure Fabric
- Policy Enforcement Group
- Custom Feeds
- Threat Prevention Policies for the following threat type:
  - Infected Hosts

**NOTE:** Moving between configuration types is not supported in all cases. You can only move from one Sky ATP Configuration Type to a “higher” configuration type. You cannot move to a lower type. Please note the following hierarchy:

- Sky ATP with SDSN (highest)
- Sky ATP
- Cloud feeds only
- No Sky ATP - No selection (lowest)

For each configuration type, certain features and UI pages are available. Please see the links below for details.

- [Features By Sky ATP Configuration Type on page 35](#)
- [Available UI Pages by Sky ATP Configuration Type on page 36](#)

## RELATED DOCUMENTATION

[Policy Enforcer Overview | 17](#)

[Policy Enforcer Components and Dependencies | 26](#)

[Benefits of Policy Enforcer | 20](#)

[Policy Enforcer Configuration Concepts | 31](#)

## Features By Sky ATP Configuration Type

For each configuration type, certain features and UI pages are available.

Refer to the following table for the features available for each configuration type.

**Table 4: List of features by Sky ATP Configuration Type**

Feature	Sky ATP with SDSN	Sky ATP	Cloud feeds only	No Sky ATP (no selection)
Full Threat Prevention Support	YES  Support with Policy Enforcement Groups across the entire Secure Fabric (including Third-party switch support)	YES  Support with existing SRX Series policies. (No Secure Fabric, Policy Enforcement Group or Third-party switch support)	Not Available	Not Available
SRX Series Device Malware Scanning	YES	YES	Not Available	Not Available
SRX Series Device Infected Host Blocking with Sky ATP	YES	YES	Not Available	Not Available
Cloud Feeds for Command and Control Servers and GeolP with Sky ATP	YES	YES	YES	Not Available
Infected Hosts Custom Feeds	YES	YES	YES	YES
Dynamic Address Custom Feeds	YES	YES	YES	YES
Custom Allowlist and Blocklists	YES	YES	YES	YES

## RELATED DOCUMENTATION

[Available UI Pages by Sky ATP Configuration Type | 36](#)
[Sky ATP Configuration Type Overview | 32](#)

## Available UI Pages by Sky ATP Configuration Type

For each configuration type, certain features and UI pages are available.

Refer to the following table for the UI pages available for each configuration type.

**Table 5: List of available UI pages by Sky ATP Configuration Type**

UI Page	Sky ATP with SDSN	Sky ATP	Cloud feeds only	No Sky ATP (no selection)
<i>Monitor Pages: Threat Prevention</i>				
Hosts	YES	YES	Not Available	Not Available
C&C Servers	YES	YES	Not Available	Not Available
HTTP File Download	YES	YES	Not Available	Not Available
SMTP Quarantine	YES	YES	Not Available	Not Available
Email Attachments	YES	YES	Not Available	Not Available
Manual Upload	YES	YES	Not Available	Not Available
All Hosts Status	YES	YES	YES	YES
DDoS Feeds Status	YES	Not Available	YES	YES
<i>Devices Page</i>				
Secure Fabric	YES	Not Available	YES	YES
<i>Configure Pages: Threat Prevention</i>				
Policies	YES	YES	YES	YES

Table 5: List of available UI pages by Sky ATP Configuration Type *(continued)*

UI Page	Sky ATP with SDSN	Sky ATP	Cloud feeds only	No Sky ATP (no selection)
Custom Feeds (Dynamic Address, Allowlist, Blocklist)	YES	YES	YES	YES
Custom Feeds (Infected Host, DDoS)	YES	Not Available	YES	YES
Sky ATP Realms	YES	YES	YES	Not Available
Email Management	YES	YES	Not Available	Not Available
Malware Management	YES	YES	Not Available	Not Available
<i>Shared Objects</i>				
Policy Enforcement Groups	YES	Not Available	YES	YES
Geo IP	YES	YES	YES	Not Available
<i>Administration: Policy Enforcer</i>				
Settings	YES	YES	YES	YES
Connectors	YES	Not Available	YES	YES

## RELATED DOCUMENTATION

For each configuration type, certain features and UI pages are available. Please see the links below.

[Features By Sky ATP Configuration Type | 35](#)

[Sky ATP Configuration Type Overview | 32](#)

# Comparing the SDSN and non-SDSN Configuration Steps

The remainder of this guide describes how to configure Security Director for either Policy Enforcer with Sky ATP (SDSN) or Sky ATP with no Policy Enforcer (non-SDSN). An optional quick setup configuration is available to step you through the configuration tasks. Or you can use Security Director windows to configure each step manually.

[Table 6 on page 38](#) compares the basic steps for both.

**Table 6: Comparing the SDSN Configuration Steps to the non-SDSN Configuration Steps**

SDSN Configuration Steps	Non-SDSN Configuration Steps
<p>Create your secure fabric.</p> <p>A secure fabric is a collection of sites which contain network devices such as switches, routers, firewalls, and other security devices.</p>	<p>Register one or more Sky ATP accounts.</p>
<p>Create your policy enforcement groups.</p> <p>You can create policy enforcement groups based on, for example, location or IP subnets. Policy enforcement groups are basically endpoints.</p>	<p>Select your SRX Series devices to register. Only SRX Series devices managed by Security Director are supported.</p>
<p>Register one or more Sky ATP accounts.</p>	<p>Create the Sky ATP profiles and policies. You can create C&amp;C (threat score and actions to take), malware and infected host policies.</p>
<p>Create threat prevention policies.</p> <p>Threat prevention policies provide protection and monitoring for selected threat profiles, including command &amp; control servers, infected hosts, and malware.</p>	<p>Add the Sky ATP policy as a rule in your firewall policy.</p>
<p>Apply your threat prevention policies to policy enforcement groups.</p> <p>When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. When you dynamically add sites, the policy enforcement groups and threat prevention policies are updated automatically.</p>	

RELATED DOCUMENTATION

Using Guided Setup for Sky ATP with SDSN	124
Using Guided Setup for Sky ATP	128
Configuring Sky ATP with SDSN (Without Guided Setup) Overview	137
Configuring Sky ATP (No SDSN and No Guided Setup) Overview	162
Policy Enforcer Overview	17
Benefits of Policy Enforcer	20
Policy Enforcer Components and Dependencies	26
Sky ATP Overview	22

# 3

CHAPTER

## Installing Policy Enforcer

---

Policy Enforcer Installation Overview | **41**

Deploying and Configuring the Policy Enforcer with OVA files | **42**

Installing Policy Enforcer with KVM | **49**

Policy Enforcer Ports | **59**

Identifying the Policy Enforcer Virtual Machine In Security Director | **61**

Obtaining a Sky ATP License | **62**

Creating a Sky ATP Cloud Web Portal Login Account | **63**

Loading a Root CA | **64**

Upgrading Your Policy Enforcer Software | **65**

---



# Policy Enforcer Installation Overview

Table 7 on page 41 lists the general steps to install and configure Policy Enforcer.

Table 7: Overview of Steps to Install and Configure Policy Enforcer

Step	Description	See
1	<p>Install and configure Junos Space and Security Director 16.1 or later.</p> <p><b>NOTE:</b> After installing Junos Space and Security Director, you must update to the latest Junos Space device schema. See your Junos Space Security Director documentation for more information on upgrading your schema.</p>	<p><a href="#">Junos Space Network Management Platform software download</a></p> <p><a href="#">Junos Space Security Director software download</a></p>
2	<p>Install and configure your SRX Series devices, EX Series switches or QFX Series switches. Switches are “discoverable” through Junos Space.</p> <p>For information on discovering switches, see <a href="#">“Using Guided Setup for Sky ATP with SDSN” on page 124</a>.</p>	<a href="#">Juniper Tech Library</a>
3	<p>Download, deploy and configure the Policy Enforcer virtual machine.</p> <p>You install Policy Enforcer on an industry-standard x86 server running a hypervisor, either the kernel-based virtual machine (KVM) hypervisor or the VMware ESXi hypervisor.</p>	<p><a href="#">“Deploying and Configuring the Policy Enforcer with OVA files” on page 42</a></p> <p><a href="#">“Installing Policy Enforcer with KVM” on page 49</a></p>
4	Use the Policy Enforcer Settings screen in Security Director ( <b>Administration &gt; Policy Enforcer Settings</b> ) to identify the Policy Enforcer virtual machine to communicate with.	<a href="#">“Identifying the Policy Enforcer Virtual Machine In Security Director” on page 61</a>
5	Obtain a Sky ATP license and create a Sky ATP portal account.	<p><a href="#">“Obtaining a Sky ATP License” on page 62</a></p> <p><a href="#">“Creating a Sky ATP Cloud Web Portal Login Account” on page 63</a></p>

Table 7: Overview of Steps to Install and Configure Policy Enforcer (*continued*)

Step	Description	See
6	Install the root CA on your Sky ATP-supported SRX Series devices.	<a href="#">“Loading a Root CA” on page 64</a>
7	Configure ClearPass or Cisco ISE as a connector for third-party products (non-Juniper Networks) to unify policy enforcement across all network elements.	<a href="#">“ClearPass Configuration for Third-Party Plug-in” on page 104</a> <a href="#">“Cisco ISE Configuration for Third-Party Plug-in” on page 111</a>
8	Use the Guided Setup screens in Security Director to configure Threat Prevention policies and deploy to devices. Optionally, you can configure policies without guided setup.	<a href="#">“Using Guided Setup for Sky ATP with SDSN” on page 124</a> <a href="#">“Using Guided Setup for Sky ATP” on page 128</a>

## RELATED DOCUMENTATION

[Deploying and Configuring the Policy Enforcer with OVA files | 42](#)

[Policy Enforcer Overview | 17](#)

[Benefits of Policy Enforcer | 20](#)

[Policy Enforcer Components and Dependencies | 26](#)

# Deploying and Configuring the Policy Enforcer with OVA files

As with other Juniper Networks virtual appliances, Policy Enforcer requires either a VMware ESX server version 4.0 or later or a VMware ESXi server version 4.0 or later that can support a virtual machine with the following configuration:

- 1 CPU
- 8-GB RAM
- 120-GB disk space

If you are not familiar with using VMware ESX or EXSi servers, see [VMware Documentation](#) and select the appropriate VMware vSphere version.

To deploy and configure the Policy Enforcer with OVA files, perform the following tasks:

1. Download the Policy Enforcer virtual machine OVA image from the Juniper Networks software [download page](#).

**NOTE:** Do not change the name of the Policy Enforcer virtual machine image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Policy Enforcer virtual machine can fail.

2. Launch the vSphere Client that is connected to the ESX server where the Policy Enforcer virtual machine is to be deployed.
3. Select **File > Deploy OVF Template** from the menu bar.
4. Click **Browse** to locate the OVA file you downloaded in Step 1.
5. Click **Next** and follow the instructions in the installation wizard.

It may take a few minutes to deploy your virtual machine. Once deployed, its name appears in the left side of the vSphere Client.
6. Right-click the virtual machine name in the left side of the vSphere Client and select **Open Console** to start configuring your network settings.
7. Log in to your virtual machine using **root** and **abc123** as the username and password, respectively. You will be required to change the password at a later step.

The welcome page appears.

8. Click **OK**.

The End User License Agreement (EULA) window appears.

9. Click **Accept** to acknowledge the EULA. If you do not agree with the EULA, click **Cancel**. Your configuration will stop and you will return to the main vSphere Client page.

The Network configuration page appears. See [Figure 9 on page 44](#).

Figure 9: Defining the Basic Network Configuration Settings

**Networking configuration**

Please specify the Connector networking configuration

Hostname

IP address

Network mask

Default gateway

Primary DNS Server

Secondary DNS Server

Skip DNS servers check ☒ [\*]

**Apply changes**

10. Enter the following configuration information.

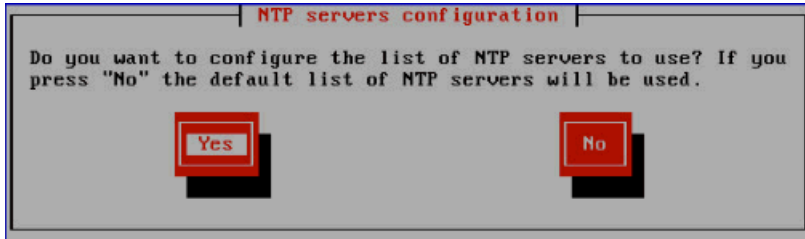
Option	Description
Hostname	Enter the hostname for the Policy Enforcer virtual machine; for example, <b>pe.juniper.net</b> .
IP address	Enter the IP address for the Policy Enforcer virtual machine.  <b>NOTE:</b> Make note of this IP address as you'll need it in a later step.
Network mask	Enter the netmask for the Policy Enforcer virtual machine.
Default gateway	Enter the IP address of the default gateway that connects your internal network to external networks.
Primary DNS server	Enter the IP address of your primary system registered to join the Domain Name System (DNS).
Secondary DNS server	Enter the IP address of a secondary DNS server. Policy Enforcer uses this address only when the primary DNS server is unavailable.
Skip DNS servers check	Select this check box if you do not want to check basic network settings. By default, the system will ping the gateway to ensure it receives a response indicating your settings are correct.

11. Click **Apply Changes**.

Your network settings are applied. A progress window indicates the status.

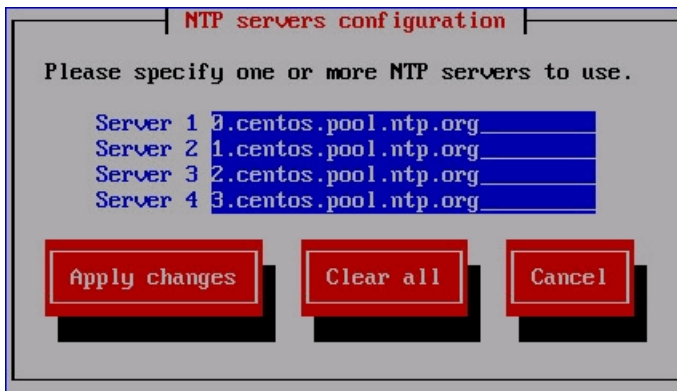
When the system is finished updating your network settings, an NTP server window appears and prompts you to configure the NTP server list. See [Figure 10 on page 45](#).

Figure 10: Prompt for Configuring the NTP Servers



12. Click **Yes** to customize the NTP server list. Click **No** to use the default list of 0, 1, 2 and 3.centos.pool.ntp.org.
13. (Optional) Specify the NTP servers to use. See [Figure 11 on page 45](#). Click **Apply Changes** to accept your edits, **Clear All** to clear all fields in this window, or **Cancel** to discard any edits and continue to the next step.

Figure 11: Configuring the NTP Servers



The Customer Information page appears. See [Figure 12 on page 46](#).

14. Enter your customer ID. This is your SiteID tied to your support account, that entitles you to use Policy Enforcer. If you don't have a support account with Juniper, then enter any unique 4-128 alphanumeric field (for example **cust01**) to identify this installation of Policy Enforcer.

Figure 12: Entering Customer Information

Customer Information

Please enter your Connector Customer ID

Customer ID

Ok

15. Click **OK**.

The Root password change page appears. See [Figure 13 on page 46](#).

Figure 13: Changing the Root Password

Root password change

Please change the root password

Password must:

- \* Cannot be empty.
- \* Be at least 6 characters in length.
- \* Must contain at least one lower case character.
- \* Must contain at least one number.
- \* Must not repeat the Login ID.
- \* Must not reverse the Login ID.
- \* Must not contain more than three repetitive characters.
- \* Must not contain number as the last character.

New root password

Confirm new root password

Ok

16. Enter and re-enter a new administrator password for the Policy Enforcer virtual machine.

Password restrictions are listed in the screen.

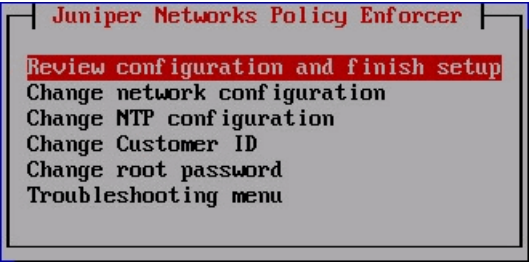
**NOTE:** Make note of this password as you'll need it in a later step.

If you forget your password, see [CentOS root password reset instructions](#).

17. Click **OK**.

The Juniper Networks Policy Enforcer page appears. See [Figure 14 on page 47](#).

Figure 14: Reviewing and Changing Your Configuration Settings.



18. Select one of the options and press **Enter**.

Option	Description
Review configuration and finish setup	<p>Lets you review the configuration settings you defined one last time before applying them to the Policy Enforcer virtual machine.</p> <p>We recommend that you do not change your configuration settings after Policy Enforcer is set up within Security Director.</p>
Change...	Select a setting to update its value.
Troubleshooting menu	Lets you ping the default gateway and custom IP address and lets you perform a DNS lookup to verify that your settings are correct.

The Review configuration page appears. See [Figure 15 on page 48](#).

Figure 15: Reviewing Your Configuration Settings

**Please review Connector configuration**

Please review Connector configuration:

**Network settings:**  
 Host name:  
 IP address:  
 Network mask:  
 Default gateway:  
 Primary DNS server:

**NTP servers:**  
 0.centos.pool.ntp.org  
 1.centos.pool.ntp.org  
 2.centos.pool.ntp.org  
 3.centos.pool.ntp.org

**Customer information:**  
 Customer ID:

19. Review your configuration settings and click **Finish setup**. To change any of the settings, click **Change configuration**.

When you click **Finish setup**, the configuration settings are applied to the Policy Enforcer virtual machine. A status page indicates the progress.

When done, the Setup Complete page appears.

**Setup Complete**

Thank you for setting up the Juniper Networks Policy Enforcer!  
 The initial setup is now done. The next steps are:

- \* Login to your Space WebUI.
- \* Go to the "Security Director" application.
- \* Select Administration -> PE Settings.
- \* Add this Connector instance.

Detailed instructions can be found in the Connector Installation and Configuration Guide.

20. Click **Finish** to return to the main vSphere Client page.



**NOTE:** Each time you log in to the Policy Enforcer virtual machine, you are given the option to review or change any of these settings.

## RELATED DOCUMENTATION

[Identifying the Policy Enforcer Virtual Machine In Security Director | 61](#)

[Policy Enforcer Overview | 17](#)

[Benefits of Policy Enforcer | 20](#)

[Policy Enforcer Components and Dependencies | 26](#)

# Installing Policy Enforcer with KVM

## IN THIS SECTION

- [Installing Policy Enforcer with virt-manager | 50](#)
- [Installing Policy Enforcer with virt-install | 51](#)
- [Configuring Policy Enforcer Settings | 52](#)
- [Connecting to the KVM Management Console | 58](#)

The Policy Enforcer Virtual Appliance Release 17.1R2 and later can be deployed on qemu-kvm (KVM) Release 1.5.3-105.el7 or later which is on CentOS Release 6.8 or later.

**NOTE:** Juniper Networks does not provide any support for installing and configuring the KVM server. You must install the virtual appliance image and configure it as per the recommended specifications for the virtual appliance. Juniper Networks will provide support only after the Policy Enforcer Virtual Appliance has booted successfully.

The prerequisites to deploy a Policy Enforcer Virtual Appliance on a KVM server are as follows:

- Knowledge about configuring and installing a KVM server.
- The KVM server and supported packages must be installed on a CentOS machine with the required kernels and packages. For information about installing a KVM server and supported packages on CentOS, refer to <http://wiki.centos.org/HowTos/KVM>.
- The Virtual Machine Manager (VMM) client must be installed on your local system.
- You use **virt-manager** or **virt-install** to install Policy Enforcer VMs. See your host OS documentation for complete details on these packages.

The following are the minimum requirements for installing the Policy Enforcer VM.

- 1 CPU
- 8-GB RAM
- 120-GB disk space

This topic includes:

## Installing Policy Enforcer with virt-manager

You can install and launch Policy Enforcer with the KVM **virt-manager** GUI package.

Ensure that sure you have already installed KVM, qemu, virt-manager, and libvirt on your host OS.

To install Policy Enforcer with **virt-manager**:

1. Download the Policy Enforcer KVM image from the Juniper software [download site](#).
2. On your host OS, type **virt-manager**. The Virtual Machine Manager appears.

**NOTE:** You must have admin rights on the host OS to use **virt-manager**.

3. Click **Create a new virtual machine**. The New VM wizard appears .
4. Enter a name for the virtual machine, select **Import existing disk image**, and click **Forward**.
5. Browse to the location of the downloaded Policy Enforcer image and select it.
6. Select **Linux** from the OS type list and select **Show all OS options** from the Version list.

- 7. Select **Red Hat Enterprise Linux 6** or later from the expanded Version list and click **Forward**.
- 8. Set the RAM to 8192 MB and set CPUs to 1. Click **Forward**.
- 9. Under Advanced Options, select **Specify shared device name** and enter the name of the bridge (typically **br0**) into the text box.
- 10. Click **Finish**. The VM manager creates the virtual machine and launches the Policy Enforcer console.

## Installing Policy Enforcer with virt-install

The **virt-install** and **virsh** tools are CLI alternatives to installing and managing Policy Enforcer VMs on a Linux host.

Ensure that sure you have already installed KVM, qemu, virt-install, and libvirt on your host OS.

**NOTE:** You must have root access on the host OS to use the **virt-install** command.

To install Policy Enforcer with **virt-install**:

- 1. Download the Policy Enforcer KVM image from the Juniper software [download site](#).
- 2. On your host OS, use the **virt-install** command with the mandatory options listed in [Table 8 on page 51](#).

**NOTE:** See the official **virt-install** documentation for a complete description of available options.

Table 8: virt-install Options

Command Option	Description
--name <i>name</i>	Name the Policy Enforcer VM.
--ram <i>megabytes</i>	Allocate RAM for the VM, in megabytes.

Table 8: virt-install Options (*continued*)

Command Option	Description
<code>--cpu <i>cpu-model</i>, <i>cpu-flags</i></code>	<p>Enable the <b>vmx</b> feature for optimal throughput. You can also enable <b>aes</b> for improved cryptographic throughput.</p> <p><b>NOTE:</b> CPU flag support depends on your host OS and CPU.</p> <p>Use <b>virsh capabilities</b> to list the virtualization capabilities of your host OS and CPU.</p>
<code>--vcpus <i>number</i></code>	Allocate the number of vCPUs for the Policy Enforcer VM.
<code>--disk <i>path</i></code>	<p>Specify disk storage media and size for the VM. Include the following options:</p> <ul style="list-style-type: none"> <li>• <b>size=gigabytes</b></li> <li>• <b>device=disk</b></li> <li>• <b>bus=ide</b></li> <li>• <b>format=qcow2</b></li> </ul>
<code>--os-type <i>os-type</i></code> <code>--os-variant <i>os-type</i></code>	Configure the guest OS type and variant.
<code>--import</code>	Create and boot the Policy Enforcer VM from an existing image.

The following example creates a Policy Enforcer VM with 8192 MB RAM, 1 vCPUs, and disk storage up to 120 GB:

```
hostOS# virt-install --name vPEM --ram 8192 --cpu SandyBridge,+vmx,-invtpsc --vcpus=1
--arch=x86_64 --disk path=/mnt/pe.qcow2,size=120,device=disk,bus=ide,format=qcow2 --os-type
linux --os-variant rhel6 --import
```

## Configuring Policy Enforcer Settings

By default, when you create the Policy Enforcer VM through `virt-manager` or `virt-install`, the console window appears for you to set up and configure the Policy Enforcer settings. You can open the console at any time after the initial configuration to review or edit your settings.

To configure Policy Enforcer settings:

1. Log in to your virtual machine using **root** and **abc123** as the username and password, respectively. You will be required to change the password at a later step.

The welcome page appears.

2. Click **OK**.

The End User License Agreement (EULA) window appears.

3. Click **Accept** to acknowledge the EULA. If you do not agree with the EULA, click **Cancel**. Your configuration will stop and you will return to the main vSphere Client page.

The Network configuration page appears. See [Figure 9 on page 44](#).

Figure 16: Defining the Basic Network Configuration Settings

**Networking configuration**

Please specify the Connector networking configuration

Hostname

IP address

Network mask

Default gateway

Primary DNS Server

Secondary DNS Server

Skip DNS servers check ☒

**Apply changes**

4. Enter the following configuration information.

Option	Description
Hostname	Enter the hostname for the Policy Enforcer virtual machine; for example, <b>pe.juniper.net</b> .
IP address	Enter the IP address for the Policy Enforcer virtual machine.  <b>NOTE:</b> Make note of this IP address as you'll need it in a later step.
Network mask	Enter the netmask for the Policy Enforcer virtual machine.

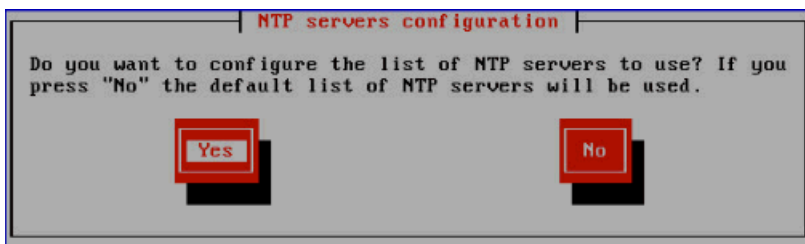
Option	Description
Default gateway	Enter the IP address of the default gateway that connects your internal network to external networks.
Primary DNS server	Enter the IP address of your primary system registered to join the Domain Name System (DNS).
Secondary DNS server	Enter the IP address of a secondary DNS server. Policy Enforcer uses this address only when the primary DNS server is unavailable.
Skip DNS servers check	Select this check box if you do not want to check basic network settings. By default, the system will ping the gateway to ensure it receives a response indicating your settings are correct.

5. Click **Apply Changes**.

Your network settings are applied. A progress window indicates the status.

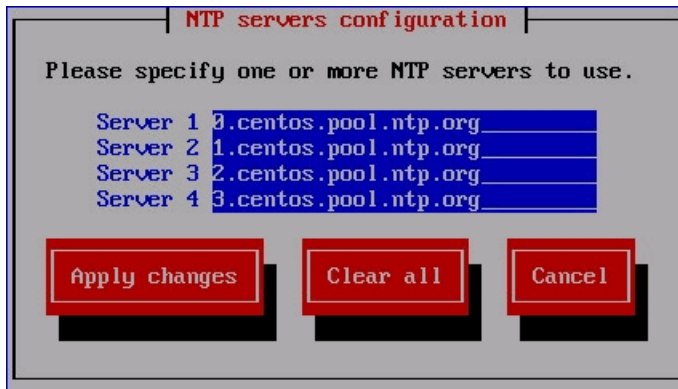
When the system is finished updating your network settings, an NTP server window appears and prompts you to configure the NTP server list. See [Figure 10 on page 45](#).

Figure 17: Prompt for Configuring the NTP Servers



6. Click **Yes** to customize the NTP server list. Click **No** to use the default list of 0, 1, 2 and 3.centos.pool.ntp.org.
7. (Optional) Specify the NTP servers to use. See [Figure 11 on page 45](#). Click **Apply Changes** to accept your edits, **Clear All** to clear all fields in this window, or **Cancel** to discard any edits and continue to the next step.

Figure 18: Configuring the NTP Servers



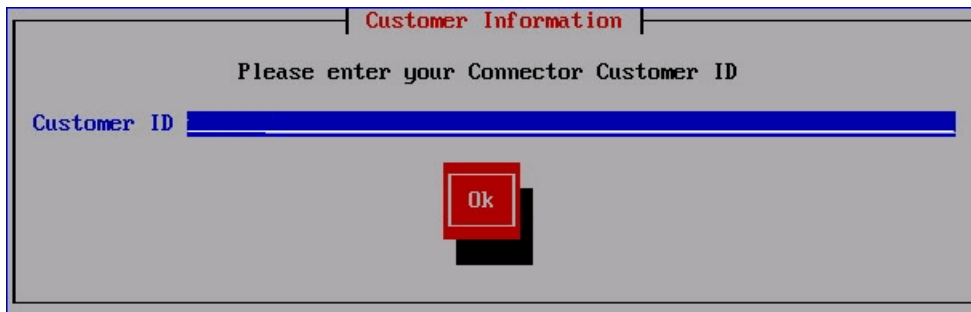
The dialog box is titled "NTP servers configuration" in red text. It contains the instruction "Please specify one or more NTP servers to use." Below this, there are four server entries, each with a label and a text field. The text fields are highlighted in blue. At the bottom, there are three red buttons: "Apply changes", "Clear all", and "Cancel".

Server	Address
Server 1	0.centos.pool.ntp.org
Server 2	1.centos.pool.ntp.org
Server 3	2.centos.pool.ntp.org
Server 4	3.centos.pool.ntp.org

The Customer Information page appears. See [Figure 12 on page 46](#).

8. Enter your customer ID. This is your SiteID tied to your support account, that entitles you to use Policy Enforcer. If you don't have a support account with Juniper, then enter any unique 4-128 alphanumeric field (for example **cust01**) to identify this installation of Policy Enforcer.

Figure 19: Entering Customer Information



The dialog box is titled "Customer Information" in red text. It contains the instruction "Please enter your Connector Customer ID". Below this, there is a label "Customer ID" followed by a long blue text input field. At the bottom center, there is a red button labeled "Ok".

9. Click **OK**.

The Root password change page appears. See [Figure 13 on page 46](#).

Figure 20: Changing the Root Password

**Root password change**

Please change the root password

Password must:

- \* Cannot be empty.
- \* Be at least 6 characters in length.
- \* Must contain at least one lower case character.
- \* Must contain at least one number.
- \* Must not repeat the Login ID.
- \* Must not reverse the Login ID.
- \* Must not contain more than three repetitive characters.
- \* Must not contain number as the last character.

New root password

Confirm new root password

**Ok**

10. Enter and re-enter a new administrator password for the Policy Enforcer virtual machine.

Password restrictions are listed in the screen.

**NOTE:** Make note of this password as you'll need it in a later step.

If you forget your password, see [CentOS root password reset instructions](#).

11. Click **OK**.

The Juniper Networks Policy Enforcer page appears. See [Figure 14 on page 47](#).

Figure 21: Reviewing and Changing Your Configuration Settings.

**Juniper Networks Policy Enforcer**

**Review configuration and finish setup**

- Change network configuration
- Change NTP configuration
- Change Customer ID
- Change root password
- Troubleshooting menu



12. Select one of the options and press **Enter**.

Option	Description
Review configuration and finish setup	Lets you review the configuration settings you defined one last time before applying them to the Policy Enforcer virtual machine.  We recommend that you do not change your configuration settings after Policy Enforcer is set up within Security Director.
Change...	Select a setting to update its value.
Troubleshooting menu	Lets you ping the default gateway and custom IP address and lets you perform a DNS lookup to verify that your settings are correct.

The Review configuration page appears. See [Figure 15 on page 48](#).

Figure 22: Reviewing Your Configuration Settings

```

Please review Connector configuration

Please review Connector configuration:

Network settings:
  Host name:
  IP address:
  Network mask:
  Default gateway:
  Primary DNS server:

NTP servers:
  0.centos.pool.ntp.org
  1.centos.pool.ntp.org
  2.centos.pool.ntp.org
  3.centos.pool.ntp.org

Customer information:
  Customer ID:

[Finish setup] [Change configuration]
  
```

13. Review your configuration settings and click **Finish setup**. To change any of the settings, click **Change configuration**.

When you click **Finish setup**, the configuration settings are applied to the Policy Enforcer virtual machine. A status page indicates the progress.

When done, the Setup Complete page appears.



14. Click **Finish** to return to the main vSphere Client page.

**NOTE:** Each time you log in to the Policy Enforcer virtual machine, you are given the option to review or change any of these settings.

## Connecting to the KVM Management Console

By default, when you create the Policy Enforcer VM the console window appears for you to set up and configure the Policy Enforcer settings. You can open the console at any time after the initial configuration to review or edit your settings. To do this, you must have the **virt-manager** package or **virsh** installed on your host OS.

To connect to the Policy Enforcer console using **virt-manager**:

1. Launch **virt-manager**.
2. Highlight the Policy Enforcer VM you want to connect to from the list of VMs displayed.
3. Click **Open**.
4. Select **View>Text Consoles>Serial 1**. The Policy Enforcer console appears.

To connect to the Policy Enforcer console with **virsh**:

1. Use the virsh console command on the Linux host OS. For example:

```
user@host# virsh console PE-kvm-2
Connected to domain PE-kvm-2
```

2. The Policy Enforcer console appears.

## RELATED DOCUMENTATION

[Policy Enforcer Installation Overview | 41](#)

[Policy Enforcer Ports | 59](#)

# Policy Enforcer Ports

You will need to open ports for Policy Enforcer to communicate with other products and devices.

[Table 9 on page 59](#) lists the ports that Policy Enforcer uses to communicate with Security Director.

**Table 9: Policy Enforcer Ports to Communicate with Security Director**

Service	Protocol	Port	In	Out
HTTPS	TCP	8080	X	
HTTPS	TCP	443		X

[Table 10 on page 59](#) lists the ports that Policy Enforcer uses to communicate with SRX Series Devices.

**Table 10: Policy Enforcer Ports to Communicate with SRX Series Devices**

Service	Protocol	Port	In	Out
HTTPS	TCP	443	X	

[Table 11 on page 60](#) lists the ports that Policy Enforcer uses to communicate with the Sky ATP server to download feeds.

**NOTE:** Connectivity between Sky ATP and Policy Enforcer is certificate-based. Once the trust is established, every request is within a context of valid token.

**Table 11: Policy Enforcer Ports to Communicate with cloudfeeds.sky.junipersecurity.net**

Service	Protocol	Port	In	Out
HTTPS	TCP	443		X

Table 12 on page 60 lists the remaining Policy Enforcer services.

**Table 12: Policy Enforcer Services**

Service	Comments
DNS	Used for basic network connection.
NTP	Used to synchronize system clocks with the Network Time Protocol (NTP).

If you are using NSX with Policy Enforcer (or Security Director), the following ports must be opened on NSX.

**Table 13: NSX Ports**

Port	In	Out	Comments
443	X		Used for communication between NSX and Security Director.
7804	X		Used for outbound SSH based auto discovery of devices.
22	X		Used for host management and image upload over sftp.

The following ports must be opened from Policy Enforcer, Junos Space, and SRX Series devices for bidirectional traffic between nodes:

- Security Director or Policy Enforcer to Internet—8080, 443
- Policy Enforcer to SRX Series devices—8080, 443
- Policy Enforcer to Security Director—443, 8080

## RELATED DOCUMENTATION

## Identifying the Policy Enforcer Virtual Machine In Security Director

You must identify the Policy Enforcer virtual machine in Security Director so that they can communicate with each other. To do so, follow these steps:

1. Log in to Security Director and select **Administration > PE Settings**.
2. Enter the IP address of the Policy Enforcer virtual machine and the root password and click **OK**.
3. Select a Threat Prevention Type:
  - Sky ATP with PE—All SDSN features and threat prevention types are available.

**NOTE:** If you upgrade from cloud feeds or Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention. Use the setup wizard to expedite the process configuring threat prevention policies.

- Sky ATP—All threat prevention types are available: Command and control server, Geo IP, and Infected hosts.

**NOTE:** If you upgrade from cloud feeds only to Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention, and you must re-enroll them with Sky ATP. Use the setup wizard to expedite the process configuring threat prevention policies.

- Cloud Feeds only—Command and control server and Geo IP are the only threat prevention types available.

For more information on these threat prevention types, see [“Policy Enforcer Settings” on page 70](#).

If you change the Policy Enforcer VM password (see [Deploying and Configuring the Policy Enforcer Virtual Machine](#)), the Policy Enforcer VM still communicates with Security Director even if you do not update the Policy Enforcer password in the **Administration > PE Settings** window in Security Director.

You can, however, update the information in the PE Settings page with the new password to keep your credentials consistent.

## RELATED DOCUMENTATION

---

[Obtaining a Sky ATP License | 62](#)

---

[Policy Enforcer Overview | 17](#)

---

[Benefits of Policy Enforcer | 20](#)

---

[Policy Enforcer Components and Dependencies | 26](#)

# Obtaining a Sky ATP License

Contact your local sales office or a Juniper Networks partner to place an order for a Sky ATP premium license. Once the order is complete, an authorization code is e-mailed to you. You will use this code in conjunction with your SRX Series device serial number to generate a premium license entitlement. (Use the **show chassis hardware** CLI command to find the serial number of the SRX Series device.)

To obtain a Sky ATP premium or basic license, follow these steps:

1. Go to [https://www.juniper.net/generate\\_license/](https://www.juniper.net/generate_license/) and log in with your Juniper Networks Customer Support Center (CSC) credentials.
2. In the Generate Licenses list, select J Series Service Routers and SRX Series Devices.
3. Using your authorization code and SRX Series serial number, follow the instructions to generate your license key. (Note that you do not enter this license key anywhere.)

Once generated, your license key is automatically transferred to the cloud server. It can take up to 24 hours for your activation to be updated in the Sky ATP cloud server

The free version does not require you to generate a license. The SRX Series device only needs to be enrolled to the cloud, and it will automatically be entitled to the free version.

Unlike with physical SRX Series devices, you must install Sky ATP premium licenses onto your vSRX instances. Installing the Sky ATP license follows the same procedure as with most standard vSRX licenses. For more information on installing the Sky ATP license onto your vSRX instance, see the *License Management and vSRX Deployments* section within [Managing the Sky Advanced Threat Prevention License](#).

## RELATED DOCUMENTATION

[Creating a Sky ATP Cloud Web Portal Login Account | 63](#)[Policy Enforcer Overview | 17](#)[Benefits of Policy Enforcer | 20](#)[Policy Enforcer Components and Dependencies | 26](#)

## Creating a Sky ATP Cloud Web Portal Login Account

To create a Sky ATP account, you must first have a Customer Support Center (CSC) user account. For more information, see [Creating a User Account](#). If you forget to do this step, you will be reminded during the quick setup.

1. Go to <https://sky.junipersecurity.net> and select your region. On the next screen, click **Create a security realm**.
2. Enter the following required information and continue to click **Next** until you are finished:
  - Your single sign-on or Juniper Networks CSC credentials.
  - A security realm name — for example, **Juniper-Mktg-Sunnyvale**. Realm names can only contain alphanumeric characters and the dash (“-”) symbol.
  - Your contact information.
  - An e-mail address and password. This will be your login information to access the Sky ATP management interface.
3. When you click **Finish**, you are automatically logged in and taken to the Sky ATP Web UI dashboard.

## RELATED DOCUMENTATION

[Loading a Root CA | 64](#)[Using Guided Setup for Sky ATP with SDSN | 124](#)[Using Guided Setup for Sky ATP | 128](#)

# Loading a Root CA

After the Policy Enforcer virtual machine is configured and created and before creating any ATP policy, you must set up certificates on any Sky ATP-supported SRX Series device. For a list of SkyATP- supported devices, see [Sky ATP Supported Platforms Guide](#).

**NOTE:** The following is simply an example. You will need to modify the group name, profile and policy name to match your configuration.

To set up certificates for Policy Enforcer:

1. Create the CA profile using the following CLI command. A CA profile configuration contains information specific to a CA.

```
root@host# request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa
root@host# request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca
domain-name www.juniper.net subject "CN=www.juniper.net,OU=IT,O=Juniper
Networks,L=Sunnyvale,ST=CA,C=US" email security-admin@juniper.net
```

2. Configure the CA profile.

**NOTE:** The CA profile name must be policyEnforcer.

```
root@host# set security pki policyEnforcer ssl-inspect-ca ca-identity ssl-inspect-ca
root@host# set security pki policyEnforcer ssl-ca ca-identity ssl-ca
```

3. Load the default trusted CA.

```
root@host# request security pki ca-certificate ca-profile-group load ca-group-name All-Trusted-CA-Def
filename default
```

4. Enable HTTPS on the threat prevention policy.

When creating your threat prevention policy (in Security Director, select **Configure>Threat Prevention > Policy**), enable the **Scan HTTPS** option to scan files downloaded over HTTPS. For more information on creating threat prevention policies, see the Security Director online help.

When you enable HTTPS on the threat prevention policy, Policy Enforcer sends the following configuration to the devices:



```
##Security Firewall Policy : trust - untrust##
set security policies from-zone trust to-zone untrust policy
PolicyEnforcer-Rule1-1 then permit application-services ssl-proxy profile-name
policyEnforcer
##Security Firewall Policy : global ##
set security policies global policy PolicyEnforcer-Rule1-1 then permit
application-services ssl-proxy profile-name policyEnforcer
##SSL Forward proxy Profile Configurations##
set services ssl proxy profile policyEnforcer trusted-ca all
set services ssl proxy profile policyEnforcer root-ca ssl-inspect-ca
```

5. Export the locally generated certificate from the SRX Series device and install it on clients as a trusted CA to avoid some of the certificate errors that may occur.

Each website or browser behaves slightly different. Some require exceptions to be added to your browser to display the content while others may not work because the local certificate is weak.

```
root@host# request security pki local-certificate export certificate-id
ssl-inspect-ca type pem filename ssl-inspect-ca.pem
```

6. (Optional) You can limit some certificate warning messages using the following CLI command:

```
root@host# set services ssl proxy profile policyEnforcer actions
ignore-server-auth-failure
```

## Upgrading Your Policy Enforcer Software

To upgrade to the latest release of Policy Enforcer, download and run the rpm file available from Juniper Network's software download page. You must have a version of Policy Enforcer already installed to run the upgrade script. If you do not, download the latest software version from the [Policy Enforcer software download page](#) and follow the [Policy Enforcer Installation Overview](#) instructions.

**NOTE:** You can upgrade only from the previous release. For example, you can upgrade from 16.1R1 to 16.1R2 or from 16.1R2 to 17.1. You cannot skip a release. For example, upgrading from 16.1R1 to 17.1R1 is not supported.

To upgrade your Policy Enforcer software to the latest release:

1. Access the Policy Enforcer software download page  
<https://www.juniper.net/support/downloads/?p=sdpe>
2. Select the Software tab.
3. From the Version drop-down menu, select the version you want to install.
4. From under the Application Package heading, download the Policy Enforcer RPM to your Policy Enforcer virtual appliance.
5. 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-18.1R1-470-PE-Upgrade.rpm
```

It may take a few minutes to install the RPM bundle. 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.

To verify your upgrade:

- In Security Director, select **Administration > PE settings**. This page shows the current installed Policy Enforcer version number.
- Check the log file for any errors.
- (Upgrading from 16.1R1 to 16.2R1) Check the `/var/log/pe_upgrade.log` file for any errors. The following is an example output of the `pe_upgrade.log` file for a successful upgrade.

```
Location: /var/log/pe_upgrade.log
Update text:
Preparing... ##### [100%]

  1:Policy_Enforcer ##### [100%]
Upgrading..
root
Stopping services
Service: feed_scheduler
Stopping service...
```

```

Service stopped
Service: feed_server
Stopping service...
Service stopped
Service: config_server
Stopping service...
Service stopped
Extracting spotlight-connector package
Extracting security-common-lib package
Executing sql table
Copying spotlight-connector package
Copying security-common-lib package
Starting services
Service: config_server
Starting service...
Service started
Service: feed_server
Starting service...
Service started
Service: feed_scheduler
Starting service...
Service started
root
Done.

```

- (Upgrading from 17.1R1 to 17.2R1) Check the following log files for errors:
  - /var/log/pe\_upgrade\_17\_2.log
  - /var/log/pe\_upgrade\_17\_2\_3rd\_party\_adapter.log
  - /var/log/pe\_upgrade\_nsx.log

### NSX Migration Instructions from Policy Enforcer Release 17.1R1 to 17.2R1

After successfully upgrading to Policy Enforcer Release 17.2R1 and when all the Policy Enforcer services and NSX micro service are up and running, the administrator must run the **nsxmicro\_sdsn\_migrate** script manually. After the successful installation of the script, the SDSN resources such as Connector instance, Secure Fabric, and Policy Enforcement Groups (PEG) are created for the NSX Managers that are already discovered in Security Director.

If the SDSN resources are already present in the upgraded version of the software, a message is displayed showing that the NSX Manager with SDSN resources are already present in the NSX database.

## RELATED DOCUMENTATION

[Policy Enforcer Installation Overview](#) | 41

# 4

CHAPTER

## Configuring Policy Enforcer Settings and Connectors

---

Policy Enforcer Settings | **70**

Policy Enforcer Connector Overview | **72**

Creating a Policy Enforcer Connector for Public and Private Clouds | **74**

Creating a Policy Enforcer Connector for Third-Party Switches | **84**

Editing and Deleting a Connector | **88**

Viewing VPC or Projects Details | **91**

Integrating ForeScout CounterACT with Juniper Networks SDSN | **93**

ClearPass Configuration for Third-Party Plug-in | **104**

Cisco ISE Configuration for Third-Party Plug-in | **111**

---

# Policy Enforcer Settings

To access this page, in the Security Director UI, navigate to **Administration > Policy Enforcer > Settings**.

## Before You Begin

- Policy Enforcer Release version and Security Director Release version must be compatible. The Settings page shows the current release version of Policy Enforcer. If there is an incompatibility, an error message is shown that there is a mismatch between Security Director and Policy Enforcer release versions. To know more about the supported software versions, see *Policy Enforcer Release Notes*.

You cannot proceed further if the Policy Enforcer and Security Director Release versions are incompatible.

- A valid Policy Enforce VM password is required to have a fully functional Policy Enforcer. If the password is valid, a message is shown at the top of the Settings page that the Policy Enforcer Space user (pe\_user) password is currently valid and the date by when the password expires. The pe\_user has the same capabilities as the super user.

If the password is invalid, an error message is shown at the top of the Settings page. To fix this issue, login to the Policy Enforcer VM, change the root password, and then enter a new value in the Settings page.

- Policy Enforcer with Security Director can be used in four different configuration types. For each configuration type, certain features are available. Read the following topic: [“Sky ATP Configuration Type Overview” on page 32](#) before you make a Sky ATP Configuration Type selection on the Policy Enforcer Settings page.
- If you are using Sky ATP without SDSN or Cloud Feeds only, you must still download Policy Enforcer and create a policy enforcer virtual machine.
- Sky ATP license and account are needed for all configuration types (Sky ATP with SDSN, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to [“Policy Enforcer Installation Overview” on page 41](#) for instructions on obtaining a Sky ATP premium license.

To set up a Sky ATP Configuration Type, you must do the following:

1. Enter the IP address for the policy enforcer virtual machine. (This is the IP address you configured during the PE VM installation. You can locate this IP address in the vSphere Center portal.)
2. Enter the password for the policy enforcer virtual machine. (This is the same password you use to login to the VM with your root credentials. Note that the username defaults to root )

**NOTE:** Refer to [“Deploying and Configuring the Policy Enforcer with OVA files” on page 42](#) for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.

3. Select a Sky ATP Configuration Type. If you do not select a type, Policy Enforcer works in *default mode*. (See [“Sky ATP Configuration Type Overview” on page 32](#) for more information.)

- **Sky ATP with SDSN**—All Policy Enforcer features and threat prevention types are available.

**NOTE:** If you upgrade from cloud feeds or Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention. Use guided setup to expedite the process configuring threat prevention policies.

See the following topics to configure Sky ATP with SDSN:

- [Using Guided Setup for Sky ATP with SDSN on page 124](#)
- [Configuring Sky ATP with SDSN \(Without Guided Setup\) Overview on page 137](#)
- **Sky ATP**—All threat prevention types are available: Command and control server, Geo IP, and Infected hosts.

**NOTE:** If you upgrade from cloud feeds only to Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention, and you must re-enroll them with Sky ATP. Use the setup wizard to expedite the process configuring threat prevention policies.

See the following topics to configure Sky ATP:

- [Using Guided Setup for Sky ATP on page 128](#)
- [Configuring Sky ATP \(No SDSN and No Guided Setup\) Overview on page 162](#)
- **Cloud feeds only**—Command and control server, infected hosts, and Geo IP are the threat prevention types available.

See the following topic to configure Cloud feeds only:

- [Configuring Cloud Feeds Only on page 176](#)
- **No Selection**—Custom feeds only. Infected hosts is the prevention type available.

See the following topic to configure “no selection”:

- [Using Guided Setup for No Sky ATP \(No Selection\) on page 132](#)

4. Polling timers affect how often the system polls to discover endpoints. There are two polling timers, one that polls network wide and one that polls site wide. They each have default settings, but you can change those defaults to poll more or less often.
  - Network wide polling interval (value in hours): The default is 24 hours. You can set this range from between 1 to 48 hours. This timer polls all endpoints added to the secure fabric.
  - Site wide polling interval (value in minutes): The default is 5 minutes. You can set this range from 1 minute to 60 minutes. This timer polls infected endpoints moving within the sites that are a part of Secure fabric.
5. Click the **Download** button to view or save Policy Enforcer data logs to your local system. These logs are in a compressed file format.

## RELATED DOCUMENTATION

[Comparing the SDSN and non-SDSN Configuration Steps | 38](#)

[Using Guided Setup for Sky ATP with SDSN | 124](#)

[Using Guided Setup for Sky ATP | 128](#)

[Configuring Cloud Feeds Only | 176](#)

[Using Guided Setup for No Sky ATP \(No Selection\) | 132](#)

[Policy Enforcer Dashboard Widgets | 252](#)

# Policy Enforcer Connector Overview

Configure a connector for third-party products (non-Juniper Networks) to unify policy enforcement across all network elements. This protects endpoints, wired and wireless, connecting to third-party devices as well as Juniper devices.

For Policy Enforcer to provide threat remediation to endpoints connecting through third-party devices, it must be able to authenticate those devices and determine their state. It does this using a tracking and accounting threat remediation plug-in to gather information from a RADIUS server and enforce policies such as terminate session and quarantine.



**NOTE:** All third-party switches being used with Policy Enforcer must support AAA/RADIUS and Dynamic Authorization Extensions to RADIUS protocol (RFC 3579 and RFC 5176).

**NOTE:** All Cisco Systems switch models that adhere to Radius IETF attributes and support Radius Change of Authorization from Aruba ClearPass are supported by Policy Enforcer for threat remediation.

Once configured, the connector uses an API to gather endpoint MAC address information from the RADIUS server. If a host is found to be suspicious, the RADIUS server sends a CoA to disconnect the active session and quarantine the host. Once the threat has been mitigated, the interface can return to the network again, but must be authorized to do so by Policy Enforcer using the plug-in and information gathered from the RADIUS server.

Once you have a connector configured, the following information is provided on the Connectors main page.

**Table 14: Connectors Information- Main Page**

Field	Description
Name	The name you entered for the connector.
Type	This field always reads Third Party Switch at this time.
Status	<p>The current status of the connector. (Active or Inactive.)</p> <p>Hover over the status to see more details of connector instances and their respective status.</p> <p>The following statuses are shown:</p> <ul style="list-style-type: none"> <li>• Active status with green icon—All connector instances inside a connector are active</li> <li>• Inactive status with red icon—All connector instances inside a connector are inactive</li> <li>• Active status with red icon—One of the connectors is inactive and other connectors are active.</li> <li>• In progress status with green icon—All connectors are still in progress.</li> <li>• Pending (not in progress) status with green icon—All connectors are still pending.</li> </ul>
Description	Specifies the description of a connector.
Identity Server	Specifies the IP address of the product management server.
IP Address	The IP address of the ClearPass RADIUS server.

## Benefits of Policy Enforcer Connector

- **Custom threat feed and automation** - Automates the threat remediation workflows for third-party products.
- **RESTful APIs** - Provides a network vendor agnostic mechanism for threat remediation. Enables you to automate configuration and management of physical, logical, or virtual devices.

### RELATED DOCUMENTATION

[ClearPass Configuration for Third-Party Plug-in | 104](#)

[Cisco ISE Configuration for Third-Party Plug-in | 111](#)

[Creating a Policy Enforcer Connector for Third-Party Switches | 84](#)

# Creating a Policy Enforcer Connector for Public and Private Clouds

To access this page, select **Administration > Policy Enforcer > Connectors**.

### Before You Begin

- For Amazon Web Services (AWS) connector:
  - Create access key and password for your AWS account. This will be a unique username and password for your Amazon account required to create a connector. See [Managing Access Keys for Your AWS Account](#).
  - Create Virtual Private Clouds(VPC) for the required region. See [Getting Started With Amazon VPC](#).
  - Instantiate the vSRX instance in the required VPC and set the tag identifier, for example AWS\_SDSN\_VSRX. This tag identifier must match with the vSRX instance tag key in AWS.

- Create a Security Group in AWS required to create a threat prevention policy for the AWS connector.
- Deploy workloads in the required VPC and set the resource tags to the workloads.

To configure threat remediation for a public or private cloud, you must install and register the threat remediation plug-in with Policy Enforcer as follows:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Click the create icon (+).

The Create Connector page appears.

3. Complete the configuration using the information in [Table 15 on page 75](#).

4. Click **OK**.

**NOTE:** Once configured, you select the connector name as an Enforcement Point in your Secure Fabric.

**Table 15: Fields on the Create Connector Page for AWS and Contrail**

Field	Description
<i>General</i>	
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63 characters maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Connector Type	Select Amazon Web Services or Contrail from the list to connect to your secure fabric and create policies for this network.

Table 15: Fields on the Create Connector Page for AWS and Contrail (*continued*)

Field	Description
IP Address/URL	<p>Enter the IP (IPv4 or IPv6) address or URL of AWS or Contrail.</p> <p>For AWS, this field is set to <a href="http://www.aws.amazon.com">www.aws.amazon.com</a>, by default. This is where all VPCs are located. You cannot edit this field.</p>
Port	<p>For AWS connector, the port is set to 443 by default and you cannot edit this field.</p> <p>For Contrail connector, provide the port number as 8081.</p>
Username	<p>Enter the username of the server for the selected connector type.</p> <p>For AWS, enter the generated access key for your Amazon account. This is not same as your Amazon account username.</p>
Password	<p>Enter the password for the selected connector type.</p> <p>For AWS, enter your secret password generated along with your access key. This is not same password as your amazon account.</p>
<i>Network Details</i>	

Table 15: Fields on the Create Connector Page for AWS and Contrail (*continued*)

Field	Description
<b>Connector Type: AWS</b>  Virtual Private Clouds	<p>One or more virtual networks under the AWS account are discovered. They are called virtual private cloud (VPC). Only VPCs having vSRX instances deployed are managed. The VPCs are region specific. Select a region from the Region list and the corresponding VPCs are listed. By default, the VPCs for the first available region are listed.</p> <p>Security Director suggests a default Secure Fabric site name for the VPC, in the <code>&lt;connector name&gt;_&lt;vpc name&gt;_site</code> format. Click the Secure Fabric site name to edit it. When you edit the name, you will also see the other Secure Fabric sites that do not have any switches or connectors assigned to them. You can also assign these Secure Fabric sites to the connectors. If the edited site name is already existing with a connector or a switch, an alert message is shown and the Secure Fabric site name is reverted to its previous name.</p> <p>You must enable either Threat Remediation or Next Generation Firewall options or both. You cannot create a connector instance without enabling at least one option. If you navigate to the next page without enabling these options, an error message is shown insisting the user to enable either Threat Remediation or Next Generation Firewall to proceed further.</p> <p>You can get a detailed view of the VPC by hovering over the name and clicking the Detailed View icon. See <a href="#">“Viewing VPC or Projects Details” on page 91</a>.</p> <p><b>NOTE:</b> You can perform search on VPCs. Search is not supported for the site names.</p>

Table 15: Fields on the Create Connector Page for AWS and Contrail (*continued*)

Field	Description
<b>Connector Type: Contrail</b>  Project	<p>Tenant information determined from the Contrail connector is listed.</p> <p>Security Director suggests a default site name for the project, in the &lt;connector name&gt;_&lt;project name&gt;_site format. Click the site name to edit it. When you edit the site name, you will also see the other sites that do not have any switches or connectors assigned to them. You can also assign these sites to the connectors. If the edited site name is already existing with a connector or a switch, an alert message is shown and the site name is reverted to its previous name.</p> <p>You must enable either Threat Remediation or Next Generation Firewall options or both. You cannot create a connector instance without enabling at least one of the two options. If you navigate to the next page without enabling these options, an error message is shown insisting the user to enable either Threat Remediation or Next Generation Firewall to proceed further.</p> <p>You can get a detailed view of the project by hovering over the name and clicking the Detailed View icon. See <a href="#">“Viewing VPC or Projects Details” on page 91</a>.</p> <p><b>NOTE:</b> You can perform search on Project names. Search is not supported for the site names.</p>
Subnets	<p>The subnet information for Contrail and AWS is determined from the respective systems. For AWS, subnets are the availability zones and for Contrail, subnets are virtual networks. You can create Policy Enforcement Groups for one or more of the subnets, if threat remediation is selected.</p> <p>Both AWS and Contrail subnets are allocated to be within the tenant IP Address Management (IPAM) scheme.</p>
Configuration	

Table 15: Fields on the Create Connector Page for AWS and Contrail (*continued*)

Field	Description
Configuration	

Table 15: Fields on the Create Connector Page for AWS and Contrail (*continued*)

Field	Description
	<p><i>Metadata</i></p> <p>Specifies the resource tag information and the resource tag values that you have determined from the projects or VPC. The tag information appears only if the Next Generation Firewall option is enabled.</p> <p>For AWS connector, the resource tag values are fetched from AWS for all the endpoints and then mapped them to the Security Director generated metadata names.</p> <p>Based on the resource tag name, Security Director checks if a metadata with the same resource tag name is already available. If available, it automatically maps the resource tag name to its metadata. If there is no match found, Security Director suggests a new metadata name for the corresponding tag. The suggested metadata name is same as the resource tag name. You can also edit the suggested metadata name and customize the resource tag name.</p> <p>However, in the Generated MetaData Name column, you cannot use the following predefined metadata names:</p> <ul style="list-style-type: none"> <li>• Tenant</li> <li>• Provider</li> <li>• Controller</li> </ul> <p>If you provide these names, an appropriate error message is shown to choose a different name.</p> <p>Select the Map option to map the resource tag to the generated Security Director Metadata while creating the connector instance. If the Map option is not selected, the connector instance is created for a project or VPC without any resource tags. For example, if you have multiple resource tags for a project, you can choose one or more resource tags to map to the corresponding generated metadata, by selecting the Import option. The project or VPC with the selected resource tags are created when the connector instance is created.</p> <p>Mapping of Contrail and AWS connector resource tags to Security Director metadata enables you to create the next generation firewall policy definitions for the source and destination rules, based on the metadata expressions.</p>



Table 15: Fields on the Create Connector Page for AWS and Contrail (*continued*)

Field	Description
	<p>Policy Enforcer dynamically determines the matching VM instances in AWS or Contrail connector to the metadata expressions and pushes the IP address content as dynamic address groups to the enforcement points in the tenant specific vSRX firewall instance.</p> <p>In the Configuration Value column, provide any additional information required for this particular connector connection. For example, if the connector type is ForeScout CounterACT, you are required to provide the WebAPI username and password. Similarly for other connectors if the additional configuration parameters are required, they are listed in this column.</p> <p>After the successful completion, the subnet you have created is mapped to that particular connector instance.</p> <p>For AWS, provide the following configuration parameters:</p> <ul style="list-style-type: none"> <li>• SRX username—Specify the username of the vSRX device that you have instantiated for a VPC.</li> <li>• SRX identifier tag—Specify the tag name of the vSRX device, if the recommended vSRX name was not used. If you do not specify any value for this field, Policy Enforcer uses vSRX as a default tag name to identify the device.</li> </ul> <p>This enables discovery of this particular vSRX device in Junos Space. This vSRX device is also added to a specific secure fabric site.</p> <ul style="list-style-type: none"> <li>• Infected Host Security Group—Specify the security group name that you would want to tag an infected workload for threat remediation.</li> <li>• SRX authentication key—Specify the authentication key file to access the vSRX device. Editing this in the grid prompts you to either upload the authentication key file or view an already existing uploaded authentication key.</li> </ul> <p>For Contrail, provide the following configuration parameters:</p>

Table 15: Fields on the Create Connector Page for AWS and Contrail (*continued*)

Field	Description
	<ul style="list-style-type: none"> <li>• SRX username</li> <li>• SRX password</li> <li>• Infected host security group</li> </ul>

**NOTE:**

- For AWS and Contrail connectors, the site association is achieved in the Connectors page itself.
- When a connector is added to the site, Policy Enforcer discovers the vSRX Series associated with the connector and assigns it to the site. Hover over the connector name to view the corresponding vSRX with its IP address as a tool tip.
- If the mode in PE Setting page is SDSN with SKYATP, then you must create a SkyATP realm and assign the sites associated with the VPC or Project to the realm. Otherwise the vSRX instances in the VPC or Project does not download the dynamic address group objects, that is the list of workloads in the VPC or Project that match a policy metadata expression.

**Threat Remediation Workflow**

Once you create an AWS or a Contrail connector with Threat Remediation option, a site is created in the Secure Fabric page.

Perform the following actions for threat remediation:

1. Select **Configure > Threat Prevention > Sky ATP Realms**.

Select the associated Secure Fabric sites to the respective VPC or Project that is successfully added. Add the secure fabric site to a Sky ATP realm and enrol the vSRX devices to the Sky ATP. Enroll devices by clicking **Add Devices** in the list view once the realm is created.

2. Select **Configure > Shared Objects > Policy Enforcement Groups**.

Click the add icon to create a new policy enforcement group. You will see a list of all subnets that you have created in a VPC. Select the required subnets for this VPC and create a policy enforcement group. Associate this policy enforcement group to threat remediation policy.

3. Select **Configure > Threat Prevention > Policies**.

Click the add icon to create a new threat prevention policy. Add the threat prevention policy, including profiles for one or more threat types. The security group that you had selected during connector configuration is used when the host gets infected within a corresponding VPC.

## Next Generation Firewall Workflow

When you create an AWS or a contrail connector with Next Generation Firewall option, it means that for a particular VPC, Layer 7 firewall policy is enabled. Perform the following actions to enable next generation firewall:

1. Select **Configure > Firewall Policy**.
2. Select the policy for which you want to define rules and click **Add Rule**.  
The Create Rules page appears.
3. In the General tab, enter the name of the rule and description of the rule
4. In the Source tab, click **Select** for the Address(es) field to select the source address.

The Source Address page appears.

- In the Address Selection field, click **By Metadata Filter** option.
- In the Metadata Provider field, select **PE** as a provider from the list.
- In the Metadata Filter field, all the generated metadatas during the connector configuration are listed. Using these metadatas, create a required metadata expression. For example, Application = Web and Tier = App.
- In the Matched Addresses field, addresses matching the selected metadata are listed. This address is used as a source address. For every metadata expression, a unique dynamic address group(DAG) is created.
- Click **Ok** and complete configuring other parameters for the rule.
- Publish and update the configuration immediately or schedule it later.

## RELATED DOCUMENTATION

---

[Policy Enforcer Connector Overview | 72](#)

---

[Editing and Deleting a Connector | 88](#)

---

[Viewing VPC or Projects Details | 91](#)

# Creating a Policy Enforcer Connector for Third-Party Switches

To access this page, select **Administration > Policy Enforcer > Connectors**.

**Before You Begin**

- Have your ClearPass, Cisco ISE, and , ForeScout server information available.
- To obtain an evaluation copy of ForeScout CounterACT to use with Policy Enforcer, click [here](#).
- Once configure, you select the Connector as an Enforcement Point in your Secure Fabric.
- Review the “[Policy Enforcer Connector Overview](#)” on [page 72](#) topic.
- To create a connector for a public or a private cloud, see “[Creating a Policy Enforcer Connector for Public and Private Clouds](#)” on [page 74](#).

To configure threat remediation for third-party devices, you must install and register the threat remediation plug-in with Policy Enforcer as follows:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Click the create icon (+).

The Create Connector page appears.

3. Complete the configuration using the information in [Table 16 on page 84](#).

4. Click **OK**.

**NOTE:** Once configured, you select the connector name as an Enforcement Point in your Secure Fabric.

Table 16: Fields on the Create Connector Page

Field	Description
<i>General</i>	

Table 16: Fields on the Create Connector Page (*continued*)

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63 characters maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Connector Type	Select the required third-party network of devices to connect to your secure fabric and create policies for this network. The available connectors are Cisco ISE, HP ClearPass, and ForeScout CounterACT.
IP Address/URL	Enter the IP (IPv4 or IPv6) address of the product management server.
Port	Select the port to be used from the list. When this is left blank, port 443 is used as the default.
Username	<p>Enter the username of the server for the selected connector type.</p> <ul style="list-style-type: none"> <li>• ClearPass—Enter the Client ID created while setting up the ClearPass API client. See <a href="#">“ClearPass Configuration for Third-Party Plug-in” on page 104</a> for details.</li> <li>• Cisco ISE—Enter the username you used when you created the API Client in the Cisco ISE UI. See <a href="#">“Cisco ISE Configuration for Third-Party Plug-in” on page 111</a>.</li> <li>• ForeScout—Enter the username of your DEX plugin. See <a href="#">“Integrating ForeScout CounterACT with Juniper Networks SDN” on page 93</a>.</li> </ul>

Table 16: Fields on the Create Connector Page (*continued*)

Field	Description
Password	<p>Enter the password of the server for the selected connector type.</p> <ul style="list-style-type: none"> <li>• ClearPass—Enter the Client Secret string created while setting up the ClearPass API client. See <a href="#">“ClearPass Configuration for Third-Party Plug-in”</a> on page 104 for details.</li> </ul> <p><b>WARNING:</b> When the Access Token Lifetime expires, you must generate a new Client Secret in ClearPass and update it here too.</p> <ul style="list-style-type: none"> <li>• Cisco ISE—Enter the password you used when you created the API Client in the Cisco ISE UI. See <a href="#">“Cisco ISE Configuration for Third-Party Plug-in”</a> on page 111.</li> <li>• ForeScout—Enter the password of your DEX plugin. See <a href="#">“Integrating ForeScout CounterACT with Juniper Networks SDSN”</a> on page 93.</li> </ul>
DEX User Role (For ForeScout connector type only)	<p>Enter the Data Exchange (DEX) user role information to authenticate and connect to the ForeScout connector. See <a href="#">“Integrating ForeScout CounterACT with Juniper Networks SDSN”</a> on page 93.</p>
<i>Network Details</i>	

Table 16: Fields on the Create Connector Page (*continued*)

Field	Description
Subnets	<p><b>Connector Type: ClearPass, ForeScout CounterACT, and Cisco ISE</b></p> <p>Add subnet information to the connector configuration so you can include those subnets in groups and then apply policies to the groups. When using Junos Space, Policy Enforcer is able to dynamically discover subnets configured on Juniper switches. Policy Enforcer does not have the same insight with third-party devices.</p> <p>When you add subnets as part of the connector configuration, those subnets become selectable in Policy Enforcement Groups.</p> <p>To add subnet information, do one of the following:</p> <ul style="list-style-type: none"> <li>Click <b>Upload File</b> to upload a text file with an IP address list.</li> </ul> <p>Note that the file you upload must contain only one item per line (no commas or semi colons). All items are validated before being added to the list.</p> <p>OR</p> <ul style="list-style-type: none"> <li>Manually enter the IP addresses. For example: 192.168.0.1/24.</li> </ul> <p>Click the add icon (+) to add more IP addresses.</p> <p><b>NOTE:</b> It is mandatory to add at least one IP subnet to a connector. You cannot proceed to next step without adding a subnet.</p>
<i>Configuration</i>	
Configuration	<p>Provide any additional information required for this particular connector connection. After the successful completion, the subnet you have created is mapped to that particular connector instance.</p> <p><b>NOTE:</b> For ClearPass and Cisco ISE connectors no additional configuration information are required.</p>

**NOTE:**

- You can associate ClearPass, Cisco ISE, or Forescout connector to a site only in your Secure Fabric.
- When a connector is added to the site, Policy Enforcer discovers the vSRX Series associated with the connector and assigns it to the site. Hover over the connector name to view the corresponding vSRX with its IP address as a tool tip.



**WARNING:** Ensure that the correct credentials are provided for the ClearPass, Cisco ISE, and ForeScout identity servers. If the initial connection fails, an error message is shown only at that time. Once that message disappears, the status of connectivity to the identity server is not shown in Policy Enforcer. Note that the identity servers are only queried on-demand.

## RELATED DOCUMENTATION

[Policy Enforcer Connector Overview | 72](#)

[ClearPass Configuration for Third-Party Plug-in | 104](#)

[Cisco ISE Configuration for Third-Party Plug-in | 111](#)

[Editing and Deleting a Connector | 88](#)

[Viewing VPC or Projects Details | 91](#)

## Editing and Deleting a Connector

## IN THIS SECTION

- [Editing a Connector | 89](#)
- [Deleting a Connector | 90](#)

You can edit or delete a connector from the Connector page.



## Editing a Connector

To edit a connector:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Select the connector you want to edit , and then click the pencil icon.

The Edit Connector page appears displaying the same options that were used to create a new connector. Note that you cannot edit the Name and IP Address/URL fields.

For the AWS connector, when you select a new region, you must enter the configuration parameters for the VPCs in that region. This enables you to maintain different vSRX authentication keys across different regions.

For AWS and Contrail connectors, you can enable or disable the threat remediation and next generation firewall features. If you disable the next generation firewall feature from a project or VPC, that particular project or VPC connector instance will be deleted. The VPCs are deleted from the corresponding regions.

A warning message is shown if you edit the existing generated metadata name. If you edit the existing metadata name, duplicate metadata objects are created that are associated to a firewall policy. To edit the metadata name, select **Configure > Shared Objects > Object Metadata** and edit the required metadata name. Also if the firewall policies are associated with this metadata, select **Configure > Firewall Policy > Policies** and edit the corresponding metadata expression.

To delete the mapping of the tag name with the generated metadata, disable the Map option for the corresponding project or VPC. A warning message is shown that there could be a firewall policy associated with this metadata. Select **Configure > Firewall Policy > Policies** and edit the corresponding metadata expression. The mapping is deleted at the end of the edit workflow. You can also enable the Import option for the tags that were not mapped to the generated metadata while creating the connector.

3. Modify the required field values and click **Save** to save your changes.

If you discover a new connector instance, you can enable the threat remediation or next generation firewall option. A new site is created when you enable one of these options. You must add these new sites to a realm to perform the threat remediation. At the end of the edit connector workflow, a reminder message is shown to add the sites to a realm.

**NOTE:**

- During the AWS connector editing, if you change the region, changes that you have made in the current session are discarded. An alert message is shown when you change the region.
- During the ClearPass or Cisco ISE connector editing, you cannot delete subnets that are already assigned to a policy enforcement group. However, you can add of any new subnets and edit their descriptions.

## Deleting a Connector

To delete a connector:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

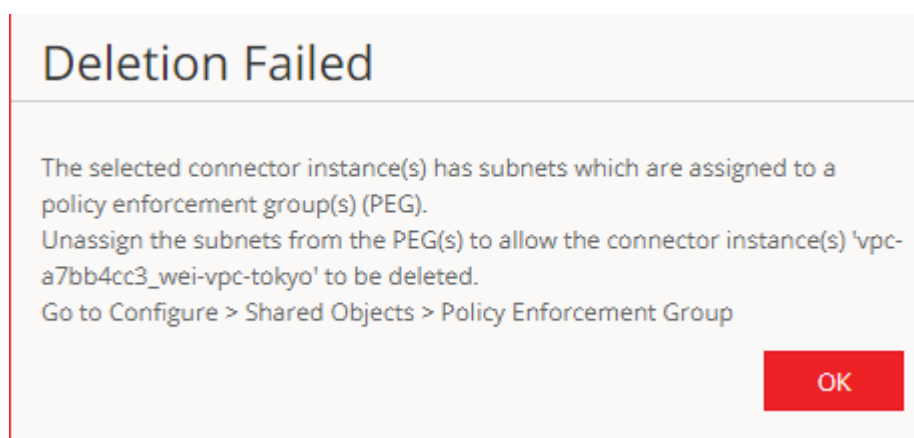
2. Select the connector that you want to delete, and select the delete icon (X).

Deleting a connector deletes the connector instances and its references as well. A warning message is shown listing all the connector instances that will be deleted, before deleting the connector.

3. Click **Delete** to delete your selection.

If the connector instances that you want to delete has PEG assigned, a warning message is shown to unassign the subnets from PEG first and then delete the connector, as shown in [Figure 23 on page 90](#).

**Figure 23: Deletion Failed Warning**



For AWS and Contrail connectors, if there are connector instances with PEG assigned, only those connector instances are not deleted. However, other connector instances without PEG assigned are deleted.

**NOTE:**

- You cannot delete the ClearPass or Cisco ISE connector if its subnets are assigned to a policy enforcement group. You must unassign those subnets from that particular policy enforcement group and then delete the connector.
- You cannot delete a connector if it is assigned as an enforcement point to a site. Before deleting a connector, you must unassign it from the site on Secure Fabric.

**RELATED DOCUMENTATION**

[Policy Enforcer Connector Overview | 72](#)

[Creating a Policy Enforcer Connector for Third-Party Switches | 84](#)

## Viewing VPC or Projects Details

To view the complete details of a VPC or a project:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Select the connector you want to edit , and then click the pencil icon.

The Edit Connector page appears displaying the same options that were used to create a new connector.

3. In the Network Details section, get a detailed view by hovering over the VPC or project name and click the Detailed View icon before the VPC or project name.

The Detailed View page appears, as shown in [Figure 24 on page 92](#).

Figure 24: Detailed View Page

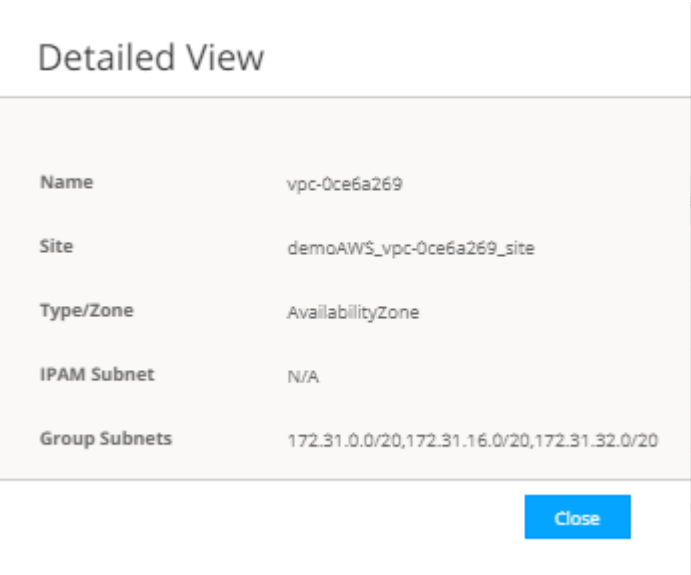


Table 17 on page 92 explains fields on the Detailed View page.

Table 17: Fields on the Detailed View Page

Field	Description
Name	Specifies name of a VPC or project.
Secure Fabric	Specifies the site to which the VPC or project s allocated.
Type/Zone	Specifies the connector type. For example, virtual network for Contrails and AvailabilityZone for AWS.
IPAM Subnet	Specifies the IP Address Management (IPAM) subnets allocated to the respective VPC or project.
Group Subnets	<p>Specifies the group of subnets allocated to the VPC or project.</p> <p>For Contrail, you will see a key value of Tier. For example, the group is called web and assigned subnet is x.x.x.x/xx. For AWS, you will see only the group of subnets.</p> <p>For Contrail, they are still group of subnets. However, each of the subnets are allocated to a tag, for example, database, tier, application, and so on.</p>

RELATED DOCUMENTATION

# Integrating ForeScout CounterACT with Juniper Networks SDSN

## IN THIS SECTION

- Configuring the DEX Plug-in | 94
- Configuring the Web API Plug-in | 98
- Creating ForeScout CounterACT Connector in Security Director | 100

This topic provides instructions on how to integrate the third-party device ForeScout CounterACT with Juniper Networks Software-Defined Secure Networks (SDSN) solution to remediate threats from infected hosts for enterprises. ForeScout CounterACT is an agentless security appliance that dynamically identifies and evaluates network endpoints and applications the instant they connect to your network. CounterACT applies an agentless approach and integrates with SDSN to block or quarantine infected hosts on Juniper Networks' devices, third-party switches, and wireless access controllers with or without 802.1x protocol integration.

To integrate ForeScout CounterACT with SDSN, you must create a connector in Policy Enforcer that enables CounterACT to connect to your secure fabric and create policies for CounterACT. Before you configure the ForeScout CounterACT connector, you must ensure that ForeScout CounterACT is installed and running with the Open Integration Module (OIM). The ForeScout OIM consists of two plug-ins: Data Exchange (DEX) and Web API. Install both the plug-ins and ensure that they are running. You must configure these plug-ins before you create a connector in Policy Enforcer.

If you do not have ForeScout CounterACT installed in your network, obtain an evaluation copy from [here](#).

This topic includes the following sections:

## Configuring the DEX Plug-in

The DEX plug-in receives API information about infected hosts from the ForeScout CounterACT connector. Messages from infected hosts are either blocked or quarantined.

When you configure the DEX plug-in, you also configure a new property, Test, for DEX. When configured, this property ensures that Web services are available for Policy Enforcer, monitors the network status, and validates usernames and passwords.

To configure the DEX plug-in:

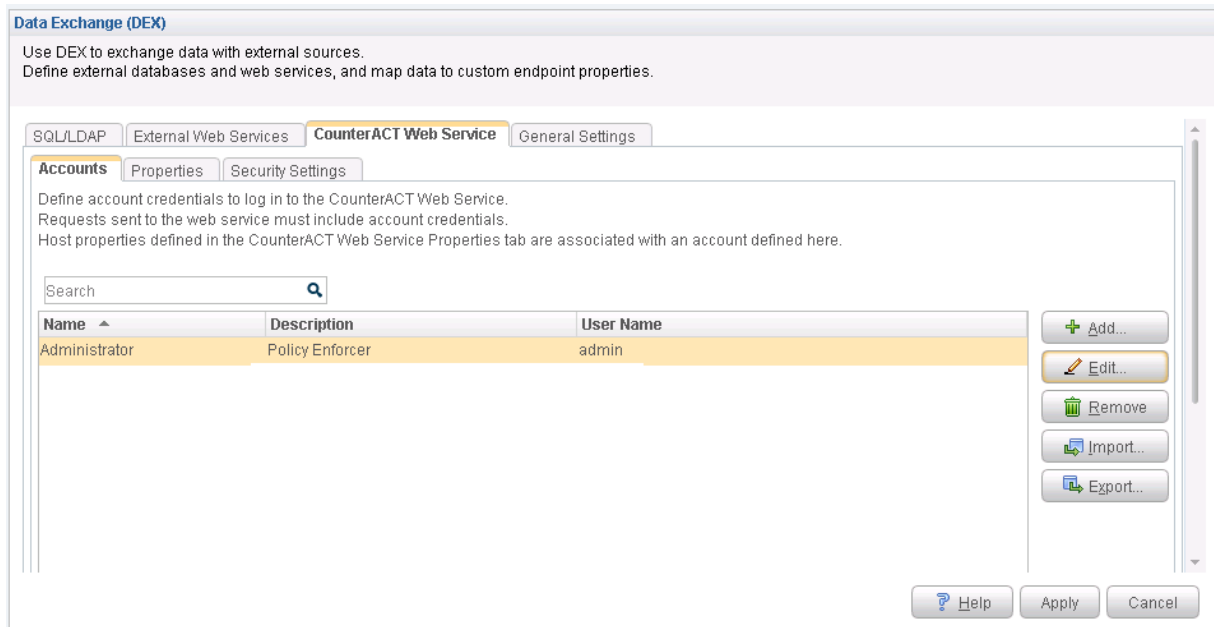
1. Select **Tools > Options > Data Exchange (DEX)** in the CounterACT UI.

The Data Exchange configuration page appears.

2. On the Data Exchange (DEX) page, select the **CounterACT Web Services > Accounts** tab, as shown in [Figure 25 on page 94](#).

The DEX Accounts page appears.

**Figure 25: DEX Accounts Page**



3. Select **Add**.

The Add page appears.

4. In the Name field, enter the name for the CounterACT Web service account.

Enter this name in the DEX User Role field (see Step 3) while configuring the ForeScout connector in Security Director.

5. In the Description field, enter a brief description of the purpose of the Web service account.
6. In the Username field, enter the username that will be used to authorize CounterACT to access the Web service account.
7. In the Password field, enter the password that will be used to authorize CounterACT to access this Web service account.
8. Click **OK**.
9. In the Properties tab, click **Add**.

The General pane of the Add Property from CounterACT Web Service wizard opens, as shown in [Figure 26 on page 96](#).

Figure 26: Add Property-General Pane Page

**Add Property from CounterACT Web Service**

**General**

Define a host property that is set via the CounterACT Web Service. Associate the property with a CounterACT web service account. Only requests submitted to the web service using this account can set the property.

Property Name

Property Tag (ASCII only)

Description

Account

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

10. Add properties such as block, quarantine, and Test, as shown in [Figure 27 on page 97](#).

You must include the Test property. Otherwise, you cannot add CounterACT as a third-party connector to Policy Enforcer successfully.



Figure 27: DEX Properties Page

**Data Exchange (DEX)**

Use DEX to exchange data with external sources.  
Define external databases and web services, and map data to custom endpoint properties.

SQL/LDAP External Web Services **CounterACT Web Service** General Settings

Accounts **Properties** Security Settings

Define host properties that are set by the CounterACT Web Service.  
Each host property defined in this tab is associated with one of the accounts in the CounterACT Web Service Accounts tab.  
To set a property, a client must send a request that uses the account credentials of the associated account for authentication.

Search

Name	Description	Type	Account
block	Policy Enforcer Block Action	Boolean	Administrator
quarantine	Policy Enforcer Quarantine Action	Boolean	Administrator
Test		Boolean	Administrator

+ Add...  
Edit...  
Remove  
Import...  
Export...

Help Apply Cancel

11. In the Security Settings tab, click **Add** and add the IP address range from where communication is expected, as shown in [Figure 28 on page 97](#).

Figure 28: Add IP Range Page

**Add IP Range**

☐ All IPs

☒ IP Range    -

OK Cancel

Click **OK**. The IP address appears in the IP Address Range list, as shown in [Figure 29 on page 98](#).

Figure 29: DEX Security Settings Page

The screenshot shows the 'Data Exchange (DEX)' configuration window. The 'CounterACT Web Service' tab is selected, and within it, the 'Security Settings' sub-tab is active. The main area contains instructions to define security settings and manage IP ranges. A table with one row shows the IP address range '172.30.77.104'. To the right of the table are buttons for 'Add...', 'Remove', and 'Edit...'. At the bottom right are 'Help', 'Apply', and 'Cancel' buttons.

**Data Exchange (DEX)**

Use DEX to exchange data with external sources.  
Define external databases and web services, and map data to custom endpoint properties.

SQLLDAP External Web Services **CounterACT Web Service** General Settings

Accounts Properties **Security Settings**

Define security setting for CounterACT Web Service.

Manage the list of IP ranges that are allowed to access CounterACT Web Service.

IP Address Range
172.30.77.104

+ Add...  
Remove  
Edit...

? Help Apply Cancel

12. On the Data Exchange (DEX) page, click **Apply**.

The configuration is saved and the configuration settings are applied.

## Configuring the Web API Plug-in

The Web API plug-in enables external entities to communicate with CounterACT by using simple, yet powerful Web service requests based on HTTP interaction. You configure the Web API plug-in to create an account for Policy Enforcer integration.

To configure the Web API plug-in:

1. Select **Tools > Options > Web API** in the CounterACT UI.

The Web API page appears.

2. In the User Settings tab, select **Add**.

The Add Credentials page appears.

3. Use the same username and password that you created for the DEX configuration (see Step 6 and Step 7) and click **OK**, as shown in [Figure 30 on page 99](#).

Figure 30: Web API User Settings Page

**Web API**

**User Settings** Client IPs

Manage user credentials and authentication settings of CounterACT Web APIs.

**User Credentials**

Manage the credential of users that are allowed to access CounterACT Web APIs.

Search

**Users** ^

admin
-------

+ Add...

Remove

Edit...

Apply Cancel

4. Select the **Client IPs** tab and click **Add**.

Add the Policy Enforcer IP address into the access list.

5. Click **OK**.

The IP address appears in the IP Address Range list, as shown in [Figure 31 on page 100](#).

Figure 31: Web API Client IPs Page

**Web API**

User Settings **Client IPs**

Manage the list of client IP ranges that are allowed to access CounterACT Web APIs.

IP Address Range
172.30.77.104

+ Add...  
Remove  
Edit...

Apply Cancel

6. Click **Apply** to save and apply your configuration.

## Creating ForeScout CounterACT Connector in Security Director

After you configure the DEX and Web API plug-ins, you need to create a connector for ForeScout CounterACT in Policy Enforcer.

To create a ForeScout CounterACT connector in Junos Space Security Director:

1. Select **Security Director > Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

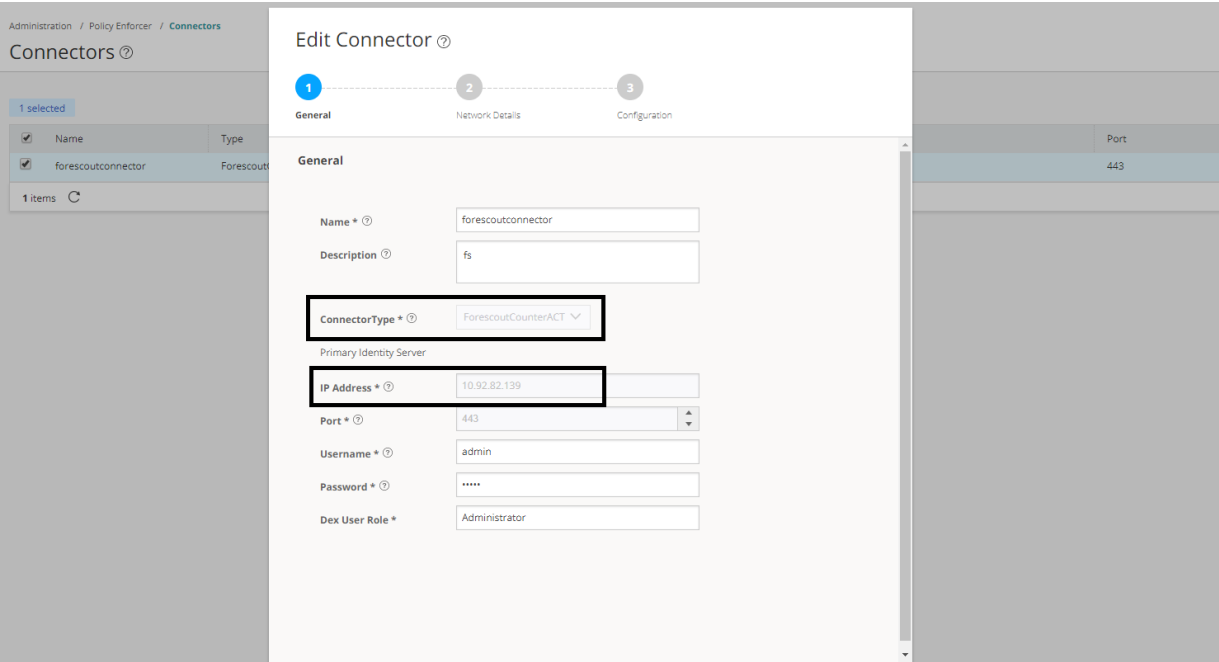
2. Click the create icon (+).

The Create Connector page appears.

3. In the General tab, select ForeScout CounterACT as the connector type and provide the username, DEX user role, and password, as shown in [Figure 32 on page 101](#). ( The DEX user role is the one that you created in [Step 4](#)).

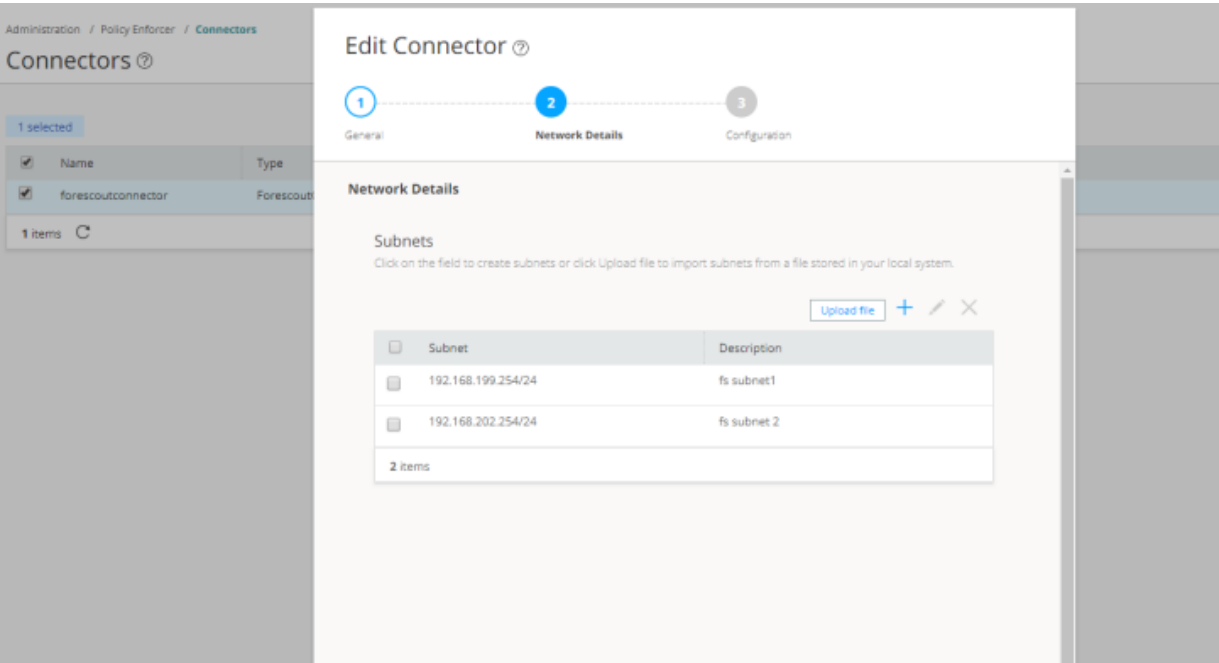
Specify 443 as the port number for communication.

Figure 32: Edit Connector Page



4. In the Network Details tab, configure the IP subnets, as shown in [Figure 33 on page 101](#). CounterACT treats the IP subnets as endpoints and takes action.

Figure 33: Edit Connector - Network Details Page



5. In the Configuration tab, specify the Web API username and password, as shown in [Figure 34 on page 102](#).

Figure 34: ForeScout Connector - Configuration Tab

**Edit Connector** ?

1 General 2 Network Details 3 **Configuration**

---

**Configuration**

Configuration

Enter configuration values for the configuration keys.

Configuration Key	Configuration Value
User ID of CounterACT web application	admin
Password of CounterACT web application	*****

Cancel Back Finish

6. Click **Finish**.

A new ForeScout CounterACT connector is created.

7. Verify that the communication between Policy Enforcer and CounterACT is working.

After installing ForeScout CounterACT and configuring a connector, in the CounterACT UI, create policies for CounterACT to take the necessary action on the infected hosts. The Hosts page lists compromised hosts and their associated threat levels, as shown in [Figure 35 on page 103](#).

Figure 35: Host Information

ENGLABSISDSN-WINDO...	10.92.83.154	Subnet_101	005056bb37f6				
ENGLABSISDSN-WINDO...	10.92.83.153	Subnet_101	005056bb754f				
ENGLABSISDSN-WINDO...	10.92.83.144	Subnet_101	005056bb2326				
ENGLABSISDSN-WINDO...	10.92.83.155	Subnet_101	005056bb4fc0				
ENGLABSISDSN-WINDO...	10.92.83.143	Subnet_101	005056bb2dbf				
192.168.199.9	192.168.199.9	Subnet_101	00505693c442				
192.168.199.5	192.168.199.5	Subnet_101	7819f77096e8				
192.168.199.3	192.168.199.3	Subnet_101	d067e5468910			10.92.81.115:ge-0/0/4	ge-0/0/4 (missing alias)
192.168.199.25	192.168.199.25	Subnet_101	005056bb0eab			10.92.81.115:ge-0/0/2	ge-0/0/2 (missing alias)
192.168.199.22	192.168.199.22	Subnet_101	005056bb667f				
192.168.199.21	192.168.199.21	Subnet_101	005056bb72b9				
192.168.199.20	192.168.199.20	Subnet_101	005056bb5e1b			10.92.81.115:ge-0/0/2	ge-0/0/2 (missing alias)

Profile	Compliance	All policies
<b>IP Address:</b> 192.168.199.25 <b>Connectivity:</b> Internal <b>MAC Address:</b> 005056bb0eab		
<b>Host Information</b>		
IP Address:	192.168.199.25	
MAC Address:	005056bb0eab	
NIC Vendor:	VMWARE, INC.	
Block:	Yes	1/31/18 12:11:58 PM
Switch IP:	10.92.81.115	
Switch Hostname:	js-ex42k-01	
Switch Port Name:	ge-0/0/2	
Switch Port Alias:	ge-0/0/2 (missing alias)	
Switch IP and Port Name:	10.92.81.115:ge-0/0/2	
Switch Port VLAN:	999	
Switch Port ACL:		
Switch Port VLAN Name:	quarantine	
Switch Port Voice Device:	No	

Table 18 on page 103 shows the recommended actions performed by CounterACT on the infected hosts that are blocked or quarantined.

Table 18: Recommended Action to Be Performed on the Infected Hosts

Infected Host Policy Enforcer Action	Connection State	Action Performed by CounterACT
Blocked	Wired	Apply access control list (ACL) to block inbound and outbound traffic for a specific MAC address.
	Wireless	Apply WLAN block on the endpoint, which will block the traffic based on the wireless MAC address.
	Dot1x	Apply CoA.
Quarantined	Wired	Apply VLAN. This action is specified by Policy Enforcer.
	Wireless	Apply VLAN. This action is specified by Policy Enforcer.

## RELATED DOCUMENTATION

Policy Enforcer Connector Overview | 72

## ClearPass Configuration for Third-Party Plug-in

Policy Enforcer's ClearPass Connector communicates with the Clearpass Radius server using the Clearpass API. As part of threat remediation, Policy Enforcer's Clearpass Connector uses enforcement profiles. This section provides information for configuring Clearpass so that Policy Enforcer can invoke the appropriate enforcement profiles.

As part of the configuration, on ClearPass you will create two enforcement profiles, one for quarantine and one for terminate. Then you will use them in the ClearPass enforcement policy. Once ClearPass is configured, you will configure a ClearPass Connector on Policy Enforcer.

### NOTE:

- Always use a third-party switch that supports 802.1x, Radius CoA, Radius Accounting, and DHCP snooping features. Enabling DHCP snooping is important which configures the Radius attribute, Framed-IP-Address. Only after configuring Framed-IP-Address, Policy Enforcer can detect the session related to the infected-host IP addresses and terminate the session.
- The stale sessions in ClearPass cannot be terminated and therefore, the actual East-West traffic block will not be active until you reauthenticate the session. You must ensure to clear the stale sessions in ClearPass frequently.

On ClearPass you will configure the following:

- API Client
- Custom Attribute
- Enforcement Profiles
- Enforcement Policy

To configure the API Client:














1. In ClearPass, navigate to **Administration > API Services > API Clients** and create a client with the following attributes:

**NOTE:** You must login as ClearPass Guest to see the API services menu.



- Client ID: sdsncient
- Enabled: Select the check box for **Enable API client**
- Operator Profile: Create a profile from Administrator > Operator Logins > Profiles for the API client with minimum access privileges as shown in [Figure 36 on page 105](#).

Figure 36: ClearPass API Client Operator Profile Minimum Privileges

Operator Profile	
Name:	<b>sdsnop</b>
Description:	
Operator logins:	Enabled
Privileges:	<div>  <b>API Services</b> <b>Custom</b> </div> <div>  Allow API Access  Allow Access         </div> <div>  <b>Guest Manager</b> <b>Custom</b> </div> <div>  Active Sessions  Full Access         </div> <div>  Active Sessions History  Read Only         </div> <div>  <b>Policy Manager</b> <b>Custom</b> </div> <div>  Identity - Endpoints  Read and Write         </div> <div>  Insight - Endpoints  Read and Write         </div>
Skin:	
Start Page:	(Default)
Language:	(Default)
Time Zone:	(GMT-08:00) America/Los Angeles; Pacific Time

- Grant Type: Select **Client credentials** (grant\_type = client\_credentials)
- Client Secret: Copy and save this. It will not be shown again.
- Access Token Lifetime: Enter 5 minutes as a time-frame.


Figure 37: ClearPass Edit API Client




**ClearPass Guest**

Home » Administration » API Services » API Clients

## Edit API Client (sdsncient)

Use this form to edit the API client 'sdsncient'.

 Changing properties other than the description will invalidate any existing access tokens.

Edit API Client	
* Client ID:	sdsncient <small>The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.</small>
Description:	<div></div> <small>Use this field to store comments or notes about this API client.</small>
Enabled:	<input checked="" type="checkbox"/> Enable API client
* Operator Profile:	sdsnop <small>The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.</small>
* Grant Type:	Client credentials (grant_type=client_credentials) <small>Only the selected authentication method will be permitted for use with this client ID.</small>
Client Secret:	 Encrypted, not shown <input type="checkbox"/> Generate a new client secret
Access Token Lifetime:	5 minutes <small>Specify the lifetime of an OAuth2 access token.</small>
<div>  <b>Save Changes</b>  <b>Cancel</b> </div>	

\* required field

2. Click **Save Changes**.

To configure a Custom Attribute:

- Select ClearPass Policy Manager and navigate to **Administration > Dictionaries > Attributes** to create a custom attribute. Then add it into the Dictionary: sdsnEpStatus. Enter the following:
  - Entity Type: **Endpoint**
  - Name: sdsnEpStatus (Note that you must use this name - sdsnEpStatus)
  - Data Type: **List**
  - Is Mandatory: **Yes**
  - Allowed Values: **healthy, blocked, quarantine**
  - Default Value: **healthy**

Figure 38: ClearPass Edit Attribute

Administration » Dictionaries » Attributes

**Attributes**

Filter:  contains

#	<input type="checkbox"/> Name ▲	Entity	Data Type
1.	<input type="checkbox"/> sdsnEpStatus	Endpoint	List

Showing 1-1 of 1

Edit Attribute

Entity	EndPoint	
Name	<input type="text" value="sdsnEpStatus"/>	
Data Type	List	
Is Mandatory	Yes	
Allowed Value	<input type="text" value="healthy, blocked, quarantine"/> (e.g., example1,example2,example3)	
Default Value (optional)	<input type="text" value="healthy"/> Select from the list	

2. Click **Save**.

To configure Enforcement Profiles:

1. In ClearPass, navigate to **Configuration > Enforcement > Profiles** and create two enforcement profiles.
2. Profile 1: Create the following profile to quarantine infected endpoints:
  - Name: **JNPR SDSN Quarantine**
  - Description: **Quarantine profile for SDSN**
  - Type: **RADIUS**
  - Action: **Accept**

Figure 39: ClearPass Enforcement Profile: Quarantine

**ClearPass Policy Manager**

[Support](#) | [Help](#) | [Logout](#)  
admin (Super Administrator)

Configuration » Enforcement » Profiles » Edit Enforcement Profile - JNPR SDSN Quarantine

### Enforcement Profiles - JNPR SDSN Quarantine

**Summary** | **Profile** | **Attributes**

**Profile:**

Name:	JNPR SDSN Quarantine
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

Type	Name	Value
1. Radius:IETF	Tunnel-Private-Group-Id	= v100
2. Radius:IETF	Tunnel-Type	= VLAN (13)
3. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
4. Radius:IETF	Acct-Interim-Interval	= 60

[Back to Enforcement Profiles](#) Copy Save Cancel

**NOTE:** The data displayed at the bottom of the screen is for example and not for configuration purposes. Note that the 4th attribute can be set for the accounting packets to be sent by the NAS device to the Clearpass Radius server.

3. Profile 2: Create the following profile to block infected endpoints:

**NOTE:** To configure this profile, copy the default system profile Juniper Terminate Session and edit the profile name and attributes.

- Name: **JNPR SDSN Terminate Session**
- Description: **Block profile for SDSN**
- Type: **RADIUS\_CoA**
- Action: **Disconnect**

**NOTE:** If there are any vendor-specific additional attributes required for the Terminate COA, those needs to be added here. For example, in the case of Juniper Networks Trapeze Wireless Clients, the JNPR SDSN Terminate Session profile requires two additional attributes: NAS-IP-Address and User-Name.

Figure 40: ClearPass Enforcement Profile: Terminate

ClearPass Policy Manager

[Support](#) | [Help](#) | [Logout](#)  
admin (Super Administrator)

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Juniper SDSN Terminate Session

Enforcement Profiles - Juniper SDSN Terminate Session

SummaryProfileAttributes

Profile:

Name:

Juniper SDSN Terminate Session

Description:

System-defined profile to disconnect user (Juniper)

Type:

RADIUS\_CoA

Action:

Disconnect

Device Group List:

-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:IETF	Acct-Session-Id	=	%{Radius:IETF:Acct-Session-Id}

Back to Enforcement Profiles

CopySaveCancel

Configure an Enforcement Policy:

In ClearPass, navigate to **Configuration > Enforcement > Policies**. Both profiles you created must be added to all the enforcement policies for endpoints addressed by Policy Enforcer.

Figure 41: ClearPass Enforcement Policy

ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#)  
admin (Super Administrator)

Configuration » Enforcement » Policies » Edit - HR Windows Policy

Enforcement Policies - HR Windows Policy

Enforcement policy has not been saved

**Summary** | Enforcement | Rules

**Enforcement:**

Name:	HR Windows Policy
Description:	
Enforcement Type:	RADIUS
Default Profile:	HR Windows Profile

**Rules:**

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Endpoint:sdsnEpStatus EQUALS blocked)	Juniper SDSN Terminate Session
2. (Endpoint:sdsnEpStatus EQUALS quarantine)	JNPR SDSN Quarantine
3. (LocalUser:Department EQUALS HR)	[RADIUS] HR Windows Profile

[Back to Enforcement Policies](#) [Copy](#) [Save](#) [Cancel](#)

**NOTE:** Rules Evaluation should be set to "First applicable."

**NOTE:** Make sure the default termination enforcement profile for each of the supported vendors is not superseded by any of its enforcement profile copies. Also make sure that all the attributes required for termination are set in the profile. (As in the previous Juniper Networks Trapeze Wireless Clients example.)

Enable Insight:

1. In ClearPass, navigate to **Administration** > **Server Manager** > **Server Configuration** for the server in use.
2. Enable Insight in the **System** tab.

Set the Log accounting Interim-update Packets as TRUE:

1. In ClearPass, navigate to **Administration** > **Server Manager** > **Server Configuration** for the server in use.
2. Select the **Service Parameters** tab.

3. In the **Select Service** drop down list, select **Radius Server** and set the Log accounting Interim-update Packets as **TRUE**.
4. Proceed to [“Creating a Policy Enforcer Connector for Third-Party Switches” on page 84](#) to finish the configuration with Policy Enforcer.

## RELATED DOCUMENTATION

[Creating a Policy Enforcer Connector for Third-Party Switches | 84](#)

[Policy Enforcer Connector Overview | 72](#)

# Cisco ISE Configuration for Third-Party Plug-in

Policy Enforcer's Cisco ISE Connector communicates with the Cisco Identity Services Engine server using the Cisco ISE API. As part of threat remediation, Policy Enforcer's Connector uses enforcement profiles. This section provides information for configuring Cisco ISE so that Policy Enforcer can invoke the appropriate enforcement profiles.

As part of the configuration, on Cisco ISE you will create two enforcement profiles, one for quarantine and one for terminate. Then you will use them in the Cisco ISE enforcement policy. Once Cisco ISE is configured, you will configure a Cisco ISE Connector on Policy Enforcer.

**NOTE:** Always use a third-party switch that supports 802.1x, Radius CoA, Radius Accounting, and DHCP snooping features. Enabling DHCP snooping is important which configures the Radius attribute, Framed-IP-Address. Only after configuring Framed-IP-Address, Policy Enforcer can detect the session related to the infected-host IP addresses and terminate the session.

On Cisco ISE you will configure the following:

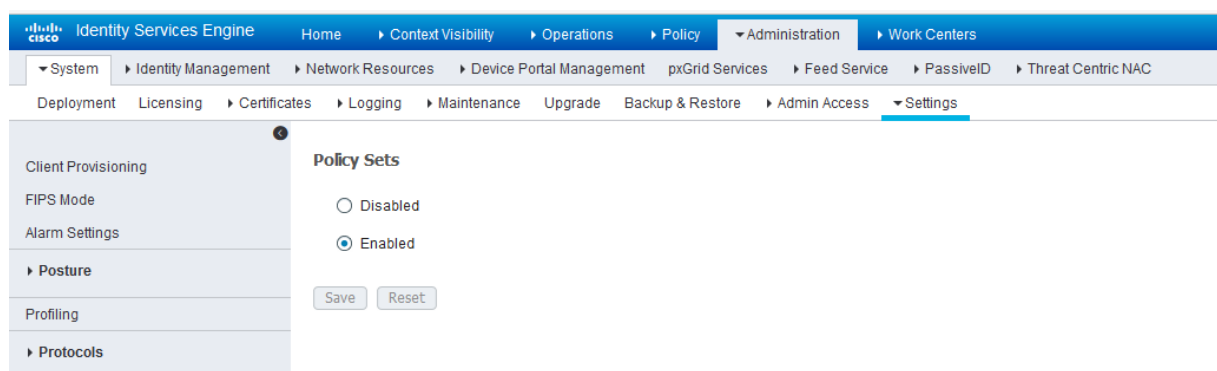
- Change policy modes
- Create an API client
- Configure network profiles
- Add a custom attribute
- Configure authorization profiles
- Set an authorization policy

On Cisco ISE, the Simple Mode policy model is selected by default. For creating an API client, Policy Sets should be enabled.

- Navigate to **Administration > System > Settings > Policy Sets** and Enable **Policy Sets** mode.

You are prompted to login again after changing the mode.

**Figure 42: Cisco ISE: Enable Policy Sets Mode**

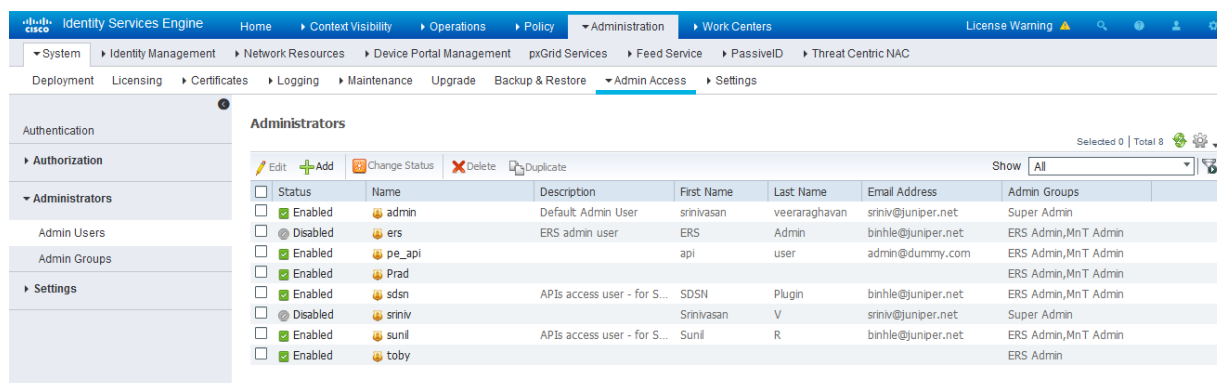


Create an API Client:

1. Using the Cisco ISE web UI, create an Admin User by navigating to **Administration > System > Admin Access > Administrator > Admin User**.
2. Create an Admin User and assign it to the following Admin Groups: **ERS Admin, MnT Admin**.

Make note of the username and password. You will need them when you configure the connector portion in Policy Enforcer later on.

**Figure 43: Cisco ISE: Create Admin User and Assign to Admin Groups**



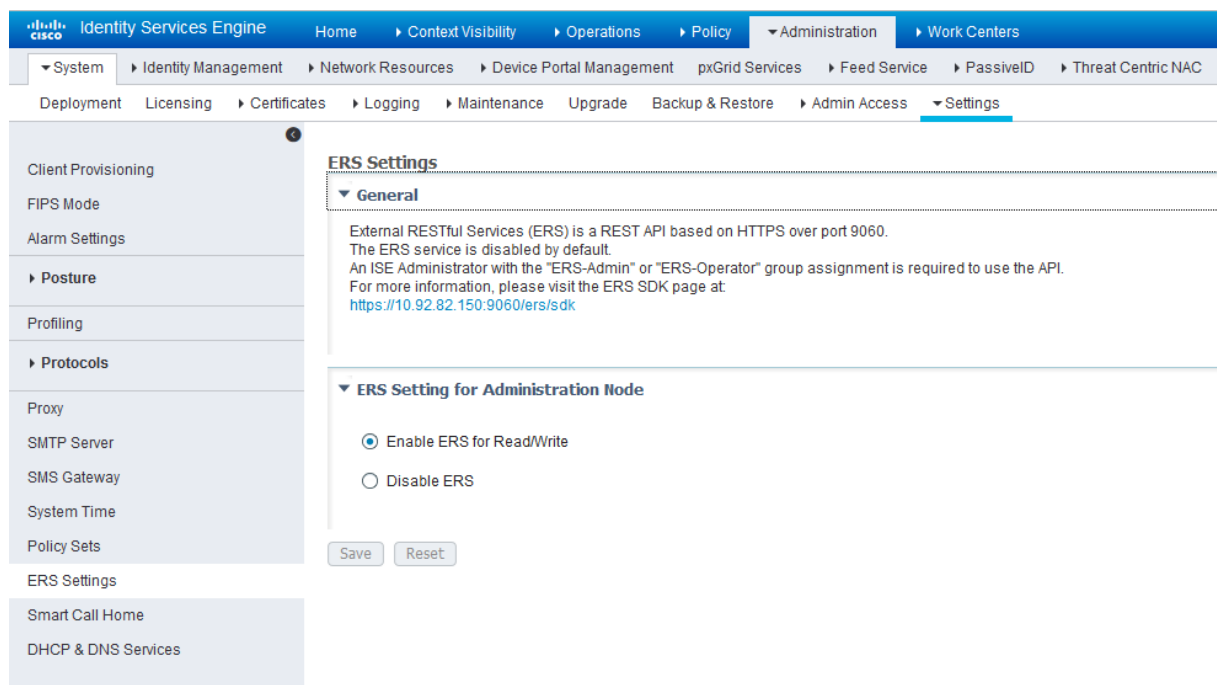
Enable the External RESTful Services API (ERS) for the Administration Node:

1. Navigate to **Administration > System > Settings > ERS Settings** and select **Enable ERS for Read/Write**.



2. Click **Save**.

**Figure 44: Cisco ISE: Enable ERS**



Configure network profiles:

Devices managed by ISE must support RADIUS CoA and have the proper network profiles assigned to handle the CoA commands sent by the ISE server:

1. Navigate to **Administration > Network Resources > Network Device Profiles** and verify the existing network device profile list.

If you are creating a new profile, proceed to the next step for information.

Figure 45: Cisco ISE: Network Device Profiles List

Name	Description	Vendor	Source
AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided
Prad		Cisco	User Defined
HPWired	Profile for HP switches	HP	Cisco Provided
HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP	Cisco Provided
HPWireless	Profile for HP wireless network access devices	HP	Cisco Provided
Juniper	Profile for Juniper Switches - created by Binh.	Juniper	User Defined
MotorolaWireless	Profile for Motorola wireless network access devices	Motorola	Cisco Provided
RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus	Cisco Provided

2. If you are configuring a new profile, you must minimally set the following:

- Enable RADIUS and add a corresponding dictionary in the supported protocol list.

Figure 46: Cisco ISE: Network Device Profile, Enable RADIUS

Network Device Profile List > [New Network Device Profile](#)

**Network Device Profile**

\* Name:

Description:

Icon:

Vendor:

**Supported Protocols**

RADIUS: ☒

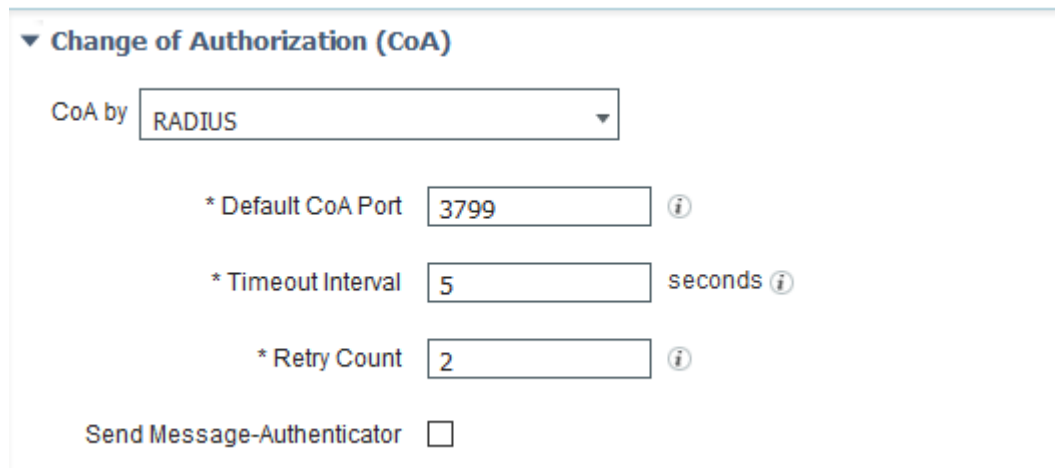
TACACS+: ☐

TrustSec: ☐

RADIUS Dictionaries:

- Enable and configure the Change of Authorization (CoA) according to the figure below.

Figure 47: Cisco ISE: Configure Change of Authorization (CoA)



**Change of Authorization (CoA)**

CoA by **RADIUS**

\* Default CoA Port **3799** ⓘ

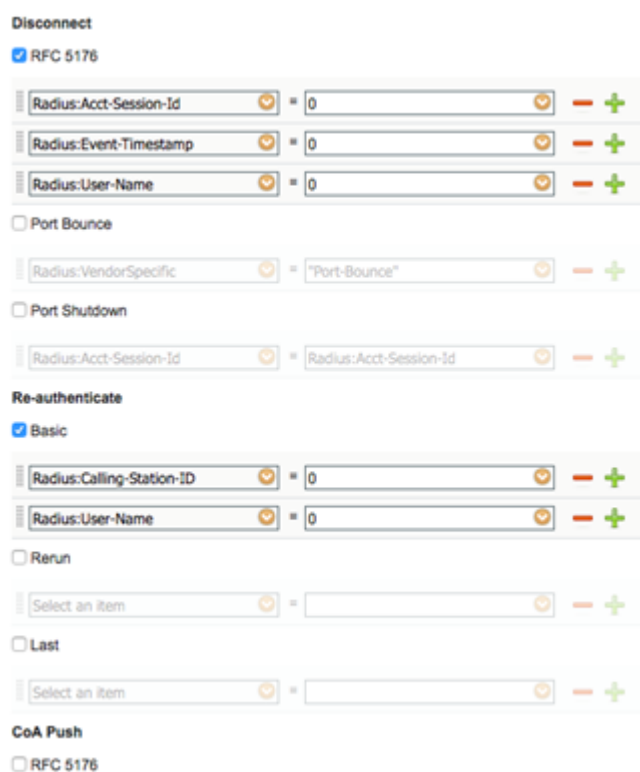
\* Timeout Interval **5** seconds ⓘ

\* Retry Count **2** ⓘ

Send Message-Authenticator ☐

- Configure the Disconnection and Re-authenticate operation with the proper RADIUS attributes and vendor specific VSA to handle the standard disconnect and reauthenticate operations. Below is the sample configuration for Juniper's EX devices.

Figure 48: Sample Configuration for Juniper EX



**Disconnect**

☒ RFC 5176

Radius:Acct-Session-Id = 0 - +

Radius:Event-Timestamp = 0 - +

Radius:User-Name = 0 - +

☐ Port Bounce

Radius:VendorSpecific = "Port-Bounce" - +

☐ Port Shutdown

Radius:Acct-Session-Id = Radius:Acct-Session-Id - +

**Re-authenticate**

☒ Basic

Radius:Calling-Station-ID = 0 - +

Radius:User-Name = 0 - +

☐ Rerun

Select an item = - +

☐ Last

Select an item = - +

**CoA Push**

☐ RFC 5176

Configure a custom attribute.

1. Navigate to **Administration > Identity Management > Settings > Endpoint Custom Attribute** and add attribute **sdsnEpStatus** with type string.

**Figure 49: Cisco ISE: Add Attribute sdsnEpStatus**

The screenshot displays the Cisco ISE Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' tab is active, showing a sub-menu with 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', 'PassiveID', and 'Threat Centric NAC'. Under 'Identity Management', the 'Settings' sub-tab is selected, leading to the 'Endpoint Custom Attributes' page.

On the left sidebar, the following options are listed: 'User Custom Attributes', 'User Authentication Settings', 'Endpoint Purge', and 'Endpoint Custom Attributes' (which is highlighted).

The main content area is titled 'Endpoint Custom Attributes'. It features a section 'Endpoint Attributes (for reference)' with a table listing several attributes:

Required	Attribute Name	Data Type
	PostureApplicable	STRING
	LogicalProfile	STRING
	EndPointPolicy	STRING
	OperatingSystem	STRING
	BYODRegistration	STRING
	PortalUser	STRING
	LastAUPAcceptanceHours	INT

Below the reference table, there is a section for adding a new 'Endpoint Custom Attribute'. It includes a text input field for 'Attribute name' containing 'sdsnEpStatus' and a dropdown menu for 'Type' set to 'String'. There are also minus and plus icons next to the type dropdown, and 'Reset' and 'Save' buttons at the bottom.

2. Verify the attribute under **Policy > Policy Elements > Dictionaries > System > Endpoints**.

Figure 50: Cisco ISE: Verify Attribute

The screenshot shows the Cisco ISE web interface. The top navigation bar includes 'Identity Services Engine' and tabs for 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' tab is active, and the 'Policy Elements' sub-tab is selected. The left sidebar shows a tree view of 'Dictionaries' with 'System' expanded, listing various protocols like ACIDEX, ACTIVE DIRECTORY, APIC, CDP, CERTIFICATE, CiscoPEP, CWA, DEVICE, DHCP, ENDPOINTPURGE, EndPoints (highlighted), EPS, and Guest. The main content area is titled 'Dictionaries > EndPoints' and shows a 'Dictionary Attributes' table. The table has columns for Name, Internal Name, and Description. The attributes listed are BYODRegistration, EndPointPolicy, LastAUPAcceptanceHo..., LogicalProfile, OperatingSystem, PortalUser, PostureApplicable, and sdsnEpStatus.

Name	Internal Name	Description
<input type="checkbox"/> BYODRegistration	BYODRegistration	BYODRegistration
<input type="checkbox"/> EndPointPolicy	EndPointPolicy	EndPointPolicy
<input type="checkbox"/> LastAUPAcceptanceHo...	LastAUPAcceptanceHo...	LastAUPAcceptanceHours
<input type="checkbox"/> LogicalProfile	LogicalProfile	LogicalProfile
<input type="checkbox"/> OperatingSystem	OperatingSystem	OperatingSystem
<input type="checkbox"/> PortalUser	PortalUser	PortalUser
<input type="checkbox"/> PostureApplicable	PostureApplicable	PostureApplicable
<input type="checkbox"/> sdsnEpStatus	sdsnEpStatus	sdsnEpStatus

3. Navigate to **Policy > Policy Elements > Conditions > Authorization > Simple Conditions**. Add there authorization simple conditions using the **sdsnEpStatus** attribute you created.

In the screen below,, there are three conditions created using sdsnEpStatus attribute. The condition names do not need to be the same as in the screen here, but the expressions must be matched. These conditions will be used in Policy Sets to handle the threat remediation for managed endpoints as described later in the Policy Sets setting section. Only the sdsnEpStatus-blocked and sdsnEpStatus-quarantine conditions will be used there. sdsnEpStatus-healthy is created for fulfillment purpose and can be ignored for now.

Figure 51: Cisco ISE: Configure Simple Conditions, Match Expression

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' tab is active, and the left sidebar shows 'Policy Elements' expanded with 'Conditions' selected. The main content area is titled 'Authorization Simple Condition List > sdsnEpStatus-blocked' and 'Authorization Simple Conditions'. The configuration form includes:
 

- \* Name: sdsnEpStatus-blocked
- Description: sdsnEpStatus is blocked
- \* Attribute: EndPoints:sdsnEpStatus
- \* Operator: Equals
- \* Value: blocked

 There are 'Save' and 'Reset' buttons at the bottom of the form.

Figure 52: Cisco ISE: Configure Simple Conditions, Match Expression

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a different condition. The top navigation bar and left sidebar are identical to Figure 51. The main content area is titled 'Authorization Simple Condition List > sdsnEpStatus-quarantine' and 'Authorization Simple Conditions'. The configuration form includes:
 

- \* Name: sdsnEpStatus-quarantine
- Description: sdsnEpStatus is quarantine
- \* Attribute: EndPoints:sdsnEpStatus
- \* Operator: Equals
- \* Value: quarantine

 There are 'Save' and 'Reset' buttons at the bottom of the form.

Configure permission/authorization profiles.

You can create the authorization profiles corresponding to “block” and “quarantine” actions as fits your needs. In the sample configuration provided here, the block action will result as total denial access to the network, and the quarantine profile will move the endpoint to another designated VLAN.

1. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

Refer to the figures below for sample configurations.

**Figure 53: Cisco ISE: Configure Authorization Profiles**

**Standard Authorization Profiles**  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 | Total 14

[Edit](#)
[Add](#)
[Duplicate](#)
[Delete](#)

Show: All

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLU
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/> DenyAccess		Default Profile with access type as Access-Reject
<input type="checkbox"/> PermitAccess		Default Profile with access type as Access-Accept
<input type="checkbox"/> cisco_wired_ise_v111		Users authorized on c2690 will get v111
<input type="checkbox"/> cisco_wired_ise_v215		Users authorized on c2600 will get v111
<input type="checkbox"/> jnpr_wired_ise_v112		Users authorized on ex4300-04 will get v112
<input type="checkbox"/> jnpr_wired_ise_v140		Users authorized on ex4300-04 will get v140
<input type="checkbox"/> sdsn_quarantine_profile		Profile for quarantined endpoints
<input type="checkbox"/> wired_cisco_user		
<input type="checkbox"/> wired_jnpr_user		

**Figure 54: Cisco ISE: Configure Authorization Profiles**



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The left sidebar contains a navigation menu with the following items: Authentication, Allowed Protocols, Authorization, Authorization Profiles, Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > sdsn\_quarantine\_profile' and 'Authorization Profile'. It contains the following fields and options:

- Name:** sdsn\_quarantine\_profile
- Description:** Profile for quarantined endpoints
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Any
- Service Template:** ☐
- Track Movement:** ☐ (i)
- Passive Identity Tracking:** ☐ (i)

Below these fields are two sections:

- Common Tasks:**
  - ☐ ACL
  - ☐ VLAN
- Advanced Attributes Settings:**

Attribute	Value	Tag ID	Action
Radius:Acct-Interim-Interval	60		
Radius:Tunnel-Medium-Type	802	1	Edit Tag
Radius:Tunnel-Private-Group-ID	200	1	Edit Tag
Radius:Tunnel-Type	VLAN	1	Edit Tag

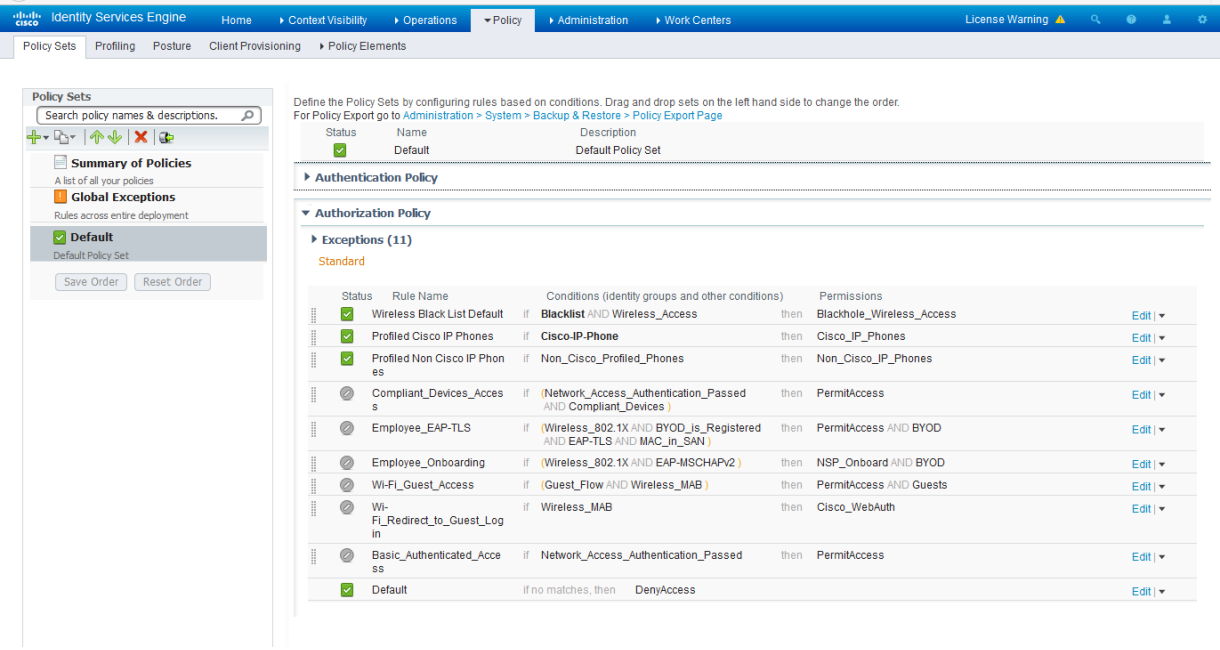
**NOTE:** For blocking a host, the default 'DenyAccess' profile is used.

Set the authorization policy:

1. Create two rules as Local Exceptions, applying the conditions and authorization/permission profiles we created in the previous step. Names may be different, but these two rules must be at the top of the Exception list.

Refer to the figure below for a sample configuration.

Figure 55: Cisco ISE: Local Exception Rules, Example



**NOTE:** Find this under **Policy > Policy Sets > Authorization Policy**.

2. Proceed to “[Creating a Policy Enforcer Connector for Third-Party Switches](#)” on page 84 to finish the configuration with Policy Enforcer.

RELATED DOCUMENTATION

- [Creating a Policy Enforcer Connector for Third-Party Switches | 84](#)
- [Policy Enforcer Connector Overview | 72](#)

# 5

CHAPTER

## Guided Setup for Sky ATP with SDSN

---

[Using Guided Setup for Sky ATP with SDSN](#) | 124

---

# Using Guided Setup for Sky ATP with SDSN

Guided Setup is the most efficient way to complete your initial configuration. Locate Guided Setup from the **Configuration > Guided Setup > Threat Prevention** menu.

- The Sky ATP Configuration type you select on the Policy Enforcer Settings page determines the guided setup process. Guided setup provides all the configuration items you need for your chosen type. See [“Sky ATP Configuration Type Overview” on page 32](#) for details on each configuration type.
- Before you begin the guided setup process, you must enter the IP address and login credentials for the policy enforcer virtual machine on the Policy Enforcer Settings page. If you haven’t yet done that, go to **Administration > Policy Enforcer > Settings** and enter the necessary information. See [“Policy Enforcer Settings” on page 70](#) for more information.
- A Sky ATP license and account are needed for all Sky ATP Configuration Types. (Sky ATP with SDSN, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium or basic license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to [“Obtaining a Sky ATP License” on page 62](#) for instructions on obtaining a Sky ATP license.
- There are some concepts you should understand before you begin the configuration. It is recommended you read about them here in advance. [“Policy Enforcer Configuration Concepts” on page 31](#).

The Guided Setup process offers five steps for configuring Sky ATP with SDSN threat prevention. Click **Start Setup** to begin.

1. **Secure Fabric**—Secure Fabric is a collection of network devices (switches, routers, firewalls, and other security devices), used by users or user groups, to which policies for aggregated threat prevention are applied. Once created, secure fabric is located under Devices. For secure fabric, the following is configured:

- **Sites**—A site is a collection of network devices participating in threat prevention. Using quick setup, you can create your own site, but note that a device can only belong to one site and you must remove it from the any other site where it is used to use it elsewhere.

Click **Add Devices** in the Device Name column or in the IP address column to add devices to a site. Using the check boxes in the device list, you should indicate which devices are firewalls or switches. Policy Enforcer needs to know which devices are firewalls so they can be enrolled in Sky ATP realms and receive feed downloads.

**NOTE:** Firewall devices are automatically enrolled with Sky ATP as part of this step. No manual enrollment is required.

2. **Policy Enforcement Group**—A policy enforcement group is a grouping of endpoints ready to receive advance threat prevention policies. Create a policy enforcement group by adding endpoints (firewalls and switches) under one common group name and later applying a security policy to that group. For policy enforcement group, the following is configured:

- Once configured, policy enforcement groups are located under **Configure > Shared Objects**. A policy enforcement groups has the following fields:
  - **Name and Description.**
  - **Group Type**—IP Address, Subnet, or Location
  - **Endpoint**—IP addresses included in the group

3. **Sky ATP Realm**— If you have not created a realm from within your Sky ATP account, you can create and register it here by clicking the + sign. Once you register a realm, you can enroll SRX Series devices into the realm. A security realm is a group identifier for an organization used to restrict access to Web applications. You can create one or multiple realms. A realm has the following configuration fields

- **Username and Password**—These are credentials you must provide, obtained through your Sky ATP account.
- **Realm**—This is the name of the realm you are creating.

If a realm is already created with a site assigned, all devices in a site are listed under the Devices in Site(s) column that includes EX Series, SRX Series, all enforcement points and devices that are originally from a realm . Devices that are marked as perimeter firewall devices are listed under the Perimeter Firewall column.

4. **Threat Prevention Policy**—A threat prevention policy requires you to create a name for the policy, choose one or more profile types depending on the type of threat prevention this policy provides (C&C Server, Infected Host, Malware), and select a log setting. Once configured, you apply policies to policy enforcement groups.

- Once configured, threat prevention policies are located under **Configure > Threat Prevention > Policies**. A policy has the following fields:
  - **Name and Description.**
  - **Profiles**—The type of threat this policy manages:
    - **C&C Server** (Command and Control Server)—A C&C server is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. A C&C profile would provide information on C&C servers that have attempted to contact and compromise hosts on your network. Information such as IP address, threat level, and country of origin are gathered.
    - **Infected Host**—An infected host profile would provide information on compromised hosts and their associated threat levels. Host information includes IP address, threat level, blocked status, when the threat was seen, command and control hits, and malware detections.

- **Malware**—A malware profile would provide information on files downloaded by hosts and found to be suspicious based on known signatures or URLs. The filename, file type, signature, date and time of download, download host, URL, and file verdict are gathered.
  - **Logging**—All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged.
  - **Group**—Once your policy is created, it is applied to the policy enforcement group.
5. **Geo IP**—Geo IP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A Geo IP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping IP address to the sources of attack traffic, geographic regions of origin can be determined, giving you the ability to filter traffic to and from specific locations in the world. For Geo IP, you configure the following:
    - **Name and Description**
    - **Countries**—Select the check box beside the countries in the Available list and click the > icon to move them to the Selected list. The countries in the Selected list will be included in the policy and action will be taken according to their threat level.
    - **Block Traffic**—Choose what traffic to block from the selected countries. Incoming traffic, Outgoing traffic, or Incoming and Outgoing traffic.
  6. The last page is a summary of the items you have configured using quick setup. Click **OK** to be taken to the Policies page under **Configure > Threat Prevention > Policies** and your policy is listed there.
  7. You must update to apply your new or edited policy configuration. Clicking the **Ready to Update** link takes you the Threat Policy Analysis page. See [“Threat Policy Analysis Overview” on page 157](#). From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.

## RELATED DOCUMENTATION

---

[Policy Enforcer Configuration Concepts | 31](#)

---

[Policy Enforcer Settings | 70](#)

---

[Configuring Sky ATP with SDSN \(Without Guided Setup\) Overview | 137](#)

---

[Using Guided Setup for Sky ATP | 128](#)

# 6

CHAPTER

## Guided Setup for Sky ATP

---

Using Guided Setup for Sky ATP | 128

---

# Using Guided Setup for Sky ATP

Guided Setup is the most efficient way to complete your initial configuration. Locate Guided Setup from the **Configuration > Guided Setup > Threat Prevention** menu.

- The Sky ATP Configuration type you select on the Policy Enforcer Settings page determines the guided setup process. Guided setup provides all the configuration items you need for your chosen type. See [“Sky ATP Configuration Type Overview” on page 32](#) for details on each configuration type.
- Before you begin the guided setup process, you must enter the IP address and login credentials for the policy enforcer virtual machine on the Policy Enforcer Settings page. If you haven’t yet done that, go to **Administration > Policy Enforcer > Settings** and enter the necessary information. See [“Policy Enforcer Settings” on page 70](#) for more information.
- A Sky ATP license and account are needed for all Sky ATP Configuration Types. (Sky ATP with SDSN, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium or basic license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to [“Obtaining a Sky ATP License” on page 62](#) for instructions on obtaining a Sky ATP license.
- There are some concepts you should understand before you begin the configuration. Read [“Sky ATP Overview” on page 22](#) for further information.

Click **Start Setup** from **Configuration > Guided Setup > Threat Prevention** to begin.

1. **Add a Sky ATP Realm**—If you have not created a realm from within your Sky ATP account, you can create it here by clicking the + sign. Once you add a realm, you can enroll SRX Series devices into the realm. A security realm is a group identifier for an organization used to restrict access to Web applications. You can create one or multiple realms. See [“Sky ATP Realm Overview” on page 163](#) for information. A realm has the following configuration fields
  - **Username and Password**—These are credentials you must provide, obtained through your Sky ATP account.
  - **Realm**—This is the name of the realm you are creating.
2. Click **Add devices** to enroll them in threat prevention before proceeding to the next step. Devices designated as perimeter firewalls are automatically enrolled with Sky ATP.
3. **Create a Policy**—You create a name for the policy, choose one or more profile types depending on the type of threat prevention this policy provides (C&C Server, Infected Host, Malware), and select a log setting.
  - Once configured, threat prevention policies are located under **Configure > Threat Prevention > Policies**. A policy has the following fields:



- **Name and Description.**
  - **Profiles**—The type of threat this policy manages:
    - **C&C Server** (Command and Control Server)—A C&C server is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. A C&C profile provides information on C&C servers that have attempted to contact and compromise hosts on your network. Information such as IP address, threat level, and country of origin are gathered.
    - **Infected Host**—An infected host profile provides information on compromised hosts and their associated threat levels. Host information includes IP address, threat level, blocked status, when the threat was seen, command and control hits, and malware detections.
    - **Malware**—A malware profile provides information on files downloaded by hosts and found to be suspicious based on known signatures or URLs. The filename, file type, signature, date and time of download, download host, URL, and file verdict are gathered.
  - **Logging**—All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged.
4. **Geo IP**—Geo IP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A Geo IP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping IP address to the sources of attack traffic, geographic regions of origin can be determined, giving you the ability to filter traffic to and from specific locations in the world. For Geo IP, you configure the following:
- **Name and Description**
  - **Countries**—Select the check box beside the countries in the Available list and click the > icon to move them to the Selected list. The countries in the Selected list will be included in the policy and action will be taken according to their threat level.
  - **Block Traffic**—Choose what traffic to block from the selected countries. Incoming traffic, Outgoing traffic, or Incoming and Outgoing traffic.
5. The last page is a summary of the items you have configured. Click **OK** to be taken to the Policies page under **Configure > Threat Prevention**, and your policy is listed there.

**NOTE:** When you are using Sky ATP without Policy Enforcer, you must assign the policy to a firewall rule before it can take affect. Navigate to **Configure > Firewall Policy > Policies**. In the Advanced Security column, click an existing item to access the Edit Advanced Security page and select the Threat Prevention Policy from the **Threat Prevention** pulldown list.

## RELATED DOCUMENTATION

[Sky ATP Overview | 22](#)

---

[Sky ATP Realm Overview | 163](#)

---

[Configuring Sky ATP \(No SDSN and No Guided Setup\) Overview | 162](#)

---

[Creating Geo IP Policies | 158](#)

# 7

CHAPTER

## Guided Setup for No Sky ATP (No Selection)

---

Using Guided Setup for No Sky ATP (No Selection) | 132

---

# Using Guided Setup for No Sky ATP (No Selection)

Guided Setup is the most efficient way to complete your initial configuration. Locate Guided Setup from the **Configuration > Guided Setup > Threat Prevention** menu.

You would make no Sky ATP selection to configure SDSN using only custom feeds. Custom feeds are the only threat prevention type available if you make no selection for Sky ATP Configuration Type in the Policy Enforcer Settings page.

- Before you begin the guided setup process, you must enter the IP address and login credentials for the policy enforcer virtual machine on the Policy Enforcer Settings page. If you haven't yet done that, go to **Administration > Policy Enforcer > Settings** and enter the necessary information. See [“Policy Enforcer Settings” on page 70](#) for more information.
- There are some concepts you should understand before you begin the configuration. It is recommended you read about them here in advance. [“Policy Enforcer Configuration Concepts” on page 31](#).

The Guided Setup process offers four steps for configuring threat prevention with custom feeds (No Sky ATP selection). Click **Start Setup** to begin.

1. **Secure Fabric**—Secure Fabric is a collection of network devices (switches, routers, firewalls, and other security devices), used by users or user groups, to which policies for aggregated threat prevention are applied. Once created, secure fabric is located under Devices. For secure fabric, the following is configured:

- **Sites**—A site is a collection of network devices participating in threat prevention. Using quick setup, you can create your own site, but note that a device can only belong to one site and you must remove it from the any other site where it is used to use it elsewhere.

Click **Add Devices** in the Device Name column or in the IP address column to add devices to a site. Using the check boxes in the device list, you should indicate which devices are firewalls or switches.

2. **Policy Enforcement Group**—A policy enforcement group is a grouping of endpoints ready to receive advance threat prevention policies. Create a policy enforcement group by adding endpoints (firewalls and switches) under one common group name and later applying a security policy to that group. For policy enforcement group, the following is configured:

- Once configured, policy enforcement groups are located under **Configure > Shared Objects**. A policy enforcement groups has the following fields:
  - **Name and Description.**
  - **Group Type**—IP Address, Subnet, or Location

- **Endpoint**—IP addresses included in the group
3. **Custom Feeds**— Policy Enforcer uses threat feeds to provide actionable intelligence to policies about various types of threats. These feeds can come from different sources. In this case, the feeds are customized by adding IP addresses, domains, and URLs to your own lists.

The following types of custom threat feeds are available:

- **Dynamic Address**—A dynamic address is a group of IP addresses that can be imported from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. You can then configure security policies to use the dynamic addresses within a security policy.
  - **Whitelist**—An allowlist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the allowlist does not have to be inspected for malware.
  - **Blacklist**—A blocklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.
  - **Infected Host**—Infected hosts are hosts known to be compromised.
4. **Threat Prevention Policy**—A threat prevention policy requires you to create a name for the policy, choose one or more profile types depending on the type of threat prevention this policy provides (infected hosts), and select a log setting. Once configured, you apply policies to policy enforcement groups.
- Once configured, threat prevention policies are located under **Configure > Threat Prevention > Policies**. A policy has the following fields:
    - **Name** and Description.
    - **Profiles**—The type of threat this policy manages:
      - **Infected Hosts**—An infected host profile would provide information on compromised hosts and their associated threat levels. Host information includes IP address, threat level, blocked status, when the threat was seen, command and control hits, and malware detections.
      - **Logging**—All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged.
    - **Group**—Once your policy is created, it is applied to the policy enforcement group.
5. The last page is a summary of the items you have configured using quick setup. Click **OK** to be taken to the Policies page under **Configure > Threat Prevention > Policies** and your policy is listed there.
6. You must update to apply your new or edited policy configuration. Clicking the **Ready to Update** link takes you the Threat Policy Analysis page. See [“Threat Policy Analysis Overview” on page 157](#). From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.

## RELATED DOCUMENTATION

[Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist](#) | 184

---

[Creating Custom Feeds, Infected Host](#) | 189

---

[Policy Enforcer Configuration Concepts](#) | 31

---

[Policy Enforcer Settings](#) | 70

# 8

CHAPTER

## Configuring Sky ATP with SDSN (without Guided Setup)

---

Configuring Sky ATP with SDSN (Without Guided Setup) Overview | **137**

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | **138**

Secure Fabric Overview | **141**

Adding Enforcement Points | **142**

| **144**

Editing or Deleting a Secure Fabric | **146**

Policy Enforcement Groups Overview | **146**

Creating Policy Enforcement Groups | **147**

Threat Prevention Policy Overview | **149**

Creating Threat Prevention Policies | **151**

Threat Policy Analysis Overview | **157**

Geo IP Overview | **158**

Creating Geo IP Policies | **158**

---



# Configuring Sky ATP with SDSN (Without Guided Setup) Overview

This is an outline of the tasks required to configure Sky ATP with SDSN.

**NOTE:** If you prefer to use quick setup, which automatically takes you through the steps listed below, it is located under **Configure>Guided Setup >Sky ATP with PE**.

- A Sky ATP license and account are needed for all threat prevention types (Sky ATP with PE, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium or basic license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to [“Obtaining a Sky ATP License” on page 62](#) for instructions on obtaining a Sky ATP license.
- Before you configure Policy Enforcer, you must enter the IP address and login credentials for the policy enforcer virtual machine. Go to **Administration > Policy Enforcer > Settings**. Once this information is entered, you can begin the setup process. See [“Policy Enforcer Settings” on page 70](#). (Refer to [“Policy Enforcer Installation Overview” on page 41](#) for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)

1. Create one or more Sky ATP realms and enroll SRX Series devices in the appropriate realm. (Enroll devices by clicking **Add Devices** in the list view once the realm is created.)

In the UI, navigate to **Configure>Threat Prevention>Sky ATP Realms**. Click the + icon to add a new Sky ATP realm.

See [“Creating Sky ATP Realms and Enrolling Devices or Associating Sites” on page 138](#) for details.

2. Create sites and add devices to those sites.

In the UI, navigate to **Devices >Secure Fabric**. Click the + icon to create a new site.

See [“Creating Secure Fabric and Sites” on page 144](#) for details.

3. Create a policy enforcement group.

In the UI, navigate to **Configure>Shared Objects>Policy Enforcement Groups**. Click the + icon to create a new policy enforcement group.

See [“Creating Policy Enforcement Groups” on page 147](#) for details.

4. Add the threat prevention policy, including profiles for one or more threat types: C&C server, infected host, malware.

In the UI, navigate to **Configure> Threat Prevention > Policies**. Click the + icon to create a new threat prevention policy.

See [“Creating Threat Prevention Policies” on page 151](#) for details.

## RELATED DOCUMENTATION

[Policy Enforcer Settings | 70](#)

[Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 138](#)

[Creating Secure Fabric and Sites | 144](#)

[Creating Policy Enforcement Groups | 147](#)

[Creating Threat Prevention Policies | 151](#)

[Creating Geo IP Policies | 158](#)

[Policy Enforcer Overview | 17](#)

[Benefits of Policy Enforcer | 20](#)

[Policy Enforcer Components and Dependencies | 26](#)

# Creating Sky ATP Realms and Enrolling Devices or Associating Sites

To access this page, click **Configure>Threat Prevention>Sky ATP Realms**.

You can create Sky ATP realms from the Sky ATP page.

- Understand which type of Sky ATP license you have: free, basic, or premium. The license controls which Sky ATP features are available.
- To configure a Sky ATP realm, you must already have a Sky ATP account with an associated license.
- Ensure that the internet connectivity is available for Policy Enforcer. Without the internet connectivity, you cannot create a realm.

- Decide which region will be covered by the realm you are creating. You must select a region when you configure a realm.
- Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Sky ATP or Policy Enforcer configuration.

To configure a Sky ATP Realm:

1. Select **Configure>Threat Prevention>Sky ATP Realms**.
2. Click the + icon.
3. Complete the initial configuration by using the guidelines in [Table 19 on page 139](#) below.

**Table 19: Fields on the Add Sky ATP Realm Page**

Field	Description
Location	<p>Select a region of the world from the available choices.</p> <p>The following options are available in the Location list:</p> <ul style="list-style-type: none"> <li>• North America</li> <li>• European Region</li> <li>• Canada</li> <li>• Asia Pacific</li> </ul> <p>By default, the North America value appears in the list. To know more about the geographic region, see <a href="#">here</a>.</p>
Username	Enter your e-mail address. Your username for Sky ATP is your e-mail address.
Password	Enter a unique string at least 8 characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character (~!@#\$%^&*()_-={}[] :;<>./?); no spaces are allowed, and you cannot use the same sequence of characters that are in your username.
Realm	<p>Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed.</p> <p><b>NOTE:</b> When you create a custom feed with a realm, the feed is associated at the site level and not at the realm level. If you modify this realm and associate new sites to it, a warning message is shown that there are custom feeds are associated with this realm. Changing the site information will change the custom feed information. You must go and edit the custom feed that was associated with this realm and verify the realm association.</p>

4. Click **Next** and guided setup walks you through the steps for enrolling devices into the realm and associating sites for Policy Enforcer.

The next steps include the following:

5. If you are using Sky ATP with PE and you have no devices in enrolled in the realm, you are asked to select devices in the box on the left and move them to the right to enroll them. All selected devices are automatically enrolled with Sky ATP when you finish guided setup. To disenroll a device, you can edit a realm and move the device back to the left side box.

**NOTE:** Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Sky ATP or Policy Enforcer configuration.

6. Next you select a Site from the list to contain the devices. If there are no sites associated with the realm, click **Create new site**. See [“Creating Secure Fabric and Sites” on page 144](#).

**NOTE:** If you are using Sky ATP without PE, you are not prompted to select a site.

7. Once the devices and site are selected, you use the sidebar to choose a threshold level at which selected administrators are notified via email about infected host events. Click the+ sign if you want to add new administrators to the list.
8. Finally, you select one or more check boxes for event types you want to log.
9. Click **Finish**.

**NOTE:** If you enrolled a device into a realm from within Security Director and you want to disenroll it, you must do that from within Security Director. If you enrolled a device into a realm from within Sky ATP and you want to disenroll it, you must do that from within Sky ATP. You cannot disenroll a device from within Security Directory that was enrolled from within Sky ATP.

## RELATED DOCUMENTATION

[Sky ATP Realm Overview](#) | 163

## Secure Fabric Overview

Secure Fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices), used in policy enforcement groups. When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. This is how threat prevention is aggregated across your secure fabric.

- **Add Enforcement Points**—Click the **Add Enforcement Points** link to add Firewalls, Switches, and/or Connectors. There is a one-to-one mapping between devices with sites. If a device is mapped to a site, you cannot use the same device to map to a different site. The connector can be mapped to multiple sites. To filter by type, click the three vertical dots beside the search field and select the check box for the device type. See [“Creating Secure Fabric and Sites” on page 144](#) for more information.
- **Drag and Drop Enforcement Points**—From the main page, you can select enforcement points and drag them to other sites to include them there. When you drag, the enforcement point is disenrolled from the current site and gets enrolled to the new site where the enforcement point is dropped.

You can either have switches or a connector as enforcement points and not both. However, you can drag a switch and add to a site that already has a switch or SRX Series device.

[Table 20 on page 141](#) shows fields on the Secure Fabric page.

Table 20: Fields on the Secure Fabric Page

Field	Description
Site	Specifies the name of the secure fabric site.
Enforcement Points	<p>Specifies the enforcement points for that particular site, if enforcement points are already added. If not added, click <b>Add Enforcement Points</b> to add Firewalls, Switches, or Connectors as enforcement points.</p> <p>A firewall icon is shown against some of the devices to indicate that they are the perimeter firewalls.</p> <p>For connectors, if you hover over the enforcement point, a tool tip is shown listing the corresponding vSRX devices with IP addresses and descriptions.</p>
Model	Specifies the type of the enforcement point. For example, vSRX, QFX, Connector.
IP	Specifies the IP address of the enforcement point, if the enforcement point is available.

Table 20: Fields on the Secure Fabric Page (*continued*)

Field	Description
SKYATP Enroll Status	<p>Specifies the status of the SkyATP enrollment.</p> <p>The Success status with a warning symbol indicates that the device is enabled for cloud feeds only and there is no support for malware capability and enhanced mode. This field will be blank if the device fails to disenroll SkyATP.</p> <p>If the status is Failed, click <b>Retry</b> to enroll the device with Sky ATP again. You can hover over the Failed status to see the corresponding job details. The device enroll retry option is available only when the status is Failed.</p>
Last Updated	Specifies the date on which the Secure Fabric page was last updated.
Description	Specifies the description that you had entered at the time of creating a secure fabric site.

## RELATED DOCUMENTATION

[Creating Secure Fabric and Sites | 144](#)
[Policy Enforcement Groups Overview | 146](#)
[Threat Prevention Policy Overview | 149](#)

## Adding Enforcement Points

Use the Add Enforcement Points page to assign devices to a site and indicate which devices are perimeter firewalls. To enroll a device with Sky ATP, you must assign one or more perimeter firewalls to each site.

**NOTE:**

- When a connector instance is assigned to a site, that particular connector instance will not be listed as available enforcement point for other sites.
- If you want to enforce an infected host policy within the network, you must assign a switch to the site.
- Assigning a device to the site will cause a change in the device configuration.

To add firewalls, switches, or connectors as an enforcement point:

- 1. Select **Devices>Secure Fabric**.

The Secure Fabric page appears.

- 2. Select the required site for which you want to add enforcement points, and click **Add Enforcement Points**.

The Add Enforcement Points page appears.

- 3. Complete the configuration as shown in [Table 21 on page 143](#).
- 4. Click **OK**.

Table 21: Fields on the Add Enforcement Points Page

Field	Description
Enforcement points	<p>All device types are displayed in the list. To filter by type, click the three vertical dots beside the search field and select the check box for the device type.</p> <p>To include a device, select the check box beside the device in the Unassigned Devices list and click the &gt; icon to move them to the Selected list. The devices in the Selected list will be included in the site.</p> <p>There is a one-to-one mapping between devices and connectors with sites. If a device or a connector is mapped to a site, you cannot use the same device or a connector to map to a different site.</p> <p><b>NOTE:</b> Firewall devices are automatically enrolled with Sky ATP as part of this step. No manual enrollment is required. The only exception is “no selection” mode where Sky ATP is not available and therefore no enrollment takes place. (see <a href="#">“Sky ATP Configuration Type Overview” on page 32</a>)</p> <p>The name of the connector type is shown as a tool tip when you hover over the name.</p>

Table 21: Fields on the Add Enforcement Points Page (*continued*)

Field	Description
Perimeter Firewall	<p>Select the edge firewall devices connecting the network to the internet. These devices will receive the threat feeds. Only firewall devices (SRX and vSRX) that you choose in the Enforcement Points field appear in the Perimeter Firewall field.</p> <p>Among the listed firewall devices, you can choose which firewall device to consider as a perimeter firewall. Only the perimeter devices are enrolled to Sky ATP. If you do not choose any firewall device as a perimeter firewall, all firewall devices listed in this field are enrolled to Sky ATP as perimeter firewalls by default.</p> <p>You can delete devices manually from the field. However, all the firewall devices are still available in the list to include later. To remove firewall devices permanently from list, you must move the firewall devices from the Selected column to the Available column in the Enforcement points field.</p> <p>In any Sky ATP configuration types, if there is a firewall device assigned to a site, it is mandatory to assign one of those devices as a perimeter firewall. If there are no firewall devices assigned to a site, the perimeter firewall list will be empty.</p> <p>When you enroll a connector instance to Policy Enforcer, the connector instance provides few vSRX Series devices. These vSRX devices are discovered by Policy Enforcer in Junos Space. Hover over the connector instances appearing in the Secure Fabric page to view the details of the corresponding vSRX devices. The vSRX Series devices associated with a connector are not shown in the Perimeter Firewall field. However, they are considered as perimeter firewalls.</p> <p><b>NOTE:</b> If a branch SRX Series device is added and selected as a perimeter firewall, system reboots and a warning message is shown before rebooting the system.</p>

## RELATED DOCUMENTATION

[Secure Fabric Overview](#) | 141

[Creating Secure Fabric and Sites](#) | 144

To access this page, click **Devices>Secure Fabric**.

You create sites within your secure fabric from the secure fabric page.

- Plan out your sites in advance. A site is a grouping of network devices, including firewalls and switches, that contribute to threat prevention.
- Keep in mind that when you create a site, you must identify the perimeter firewalls so you can enroll them with Sky ATP.
- If you want to enforce an infected host policy within the network, you must assign a switch to the site.



- Devices *cannot* belong to multiple sites.
- Switches and connectors *cannot* be added to the same site

To create a site within your secure fabric:

1. Select **Devices>Secure Fabric**.
2. Click the + icon.
3. Complete the configuration by using the guidelines in [Table 22 on page 145](#) below.
4. Click **OK**.
5. Create a new site and add an enforcement point to a site.

**Table 22: Fields on the Create Site Page**

Field	Description
Site	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.



**WARNING:** If you add certain SRX Series Devices to your Secure Fabric as enforcement points, you may see a warning that the device(s) must be reconfigured in enhanced mode and require a reboot. Here is a list of SRX models that may require rebooting for enhanced mode after being registered with Policy Enforcer/Sky ATP.

- SRX340
- SRX345
- SRX650
- SRX240h2
- SRX320
- SRX300
- SRX550

## RELATED DOCUMENTATION

[Secure Fabric Overview | 141](#)[Policy Enforcement Groups Overview | 146](#)[Threat Prevention Policy Overview | 149](#)

## Editing or Deleting a Secure Fabric

You can edit or delete a secure fabric from the secure fabric main page.

### Editing or Deleting a Secure Fabric

To edit or delete a secure fabric:

1. Select **Devices > Secure Fabric**.

The secure fabric page appears.

2. Select the secure fabric you want to edit or delete and then right-click.

- Select **Edit** to modify your secure fabric. The secure fabric configuration page appears. Make the changes and click **OK**.
- Select **Delete** to remove your secure fabric. An alert message appears verifying that you want to delete your selection. Click **Yes** to delete your selection.

## RELATED DOCUMENTATION

[Creating Secure Fabric and Sites | 144](#)[Secure Fabric Overview | 141](#)[Creating Policy Enforcement Groups | 147](#)

## Policy Enforcement Groups Overview

A policy enforcement group is a grouping of endpoints to which threat prevention policies are applied. Create a policy enforcement group by adding endpoints (firewalls, switches, subnets, set of end users) under one common group name and later applying a threat prevention policy to that group.

RELATED DOCUMENTATION

<a href="#">Creating Policy Enforcement Groups   147</a>
<a href="#">Threat Prevention Policy Overview   149</a>

# Creating Policy Enforcement Groups

To access this page, click **Configure>Shared Objects>Policy Enforcement Groups**.

You can create policy enforcement groups from the policy enforcement groups page.

- Know what type of endpoints you are including in your policy enforcement group: IP address/subnet, or location.
- Determine what endpoints you will add to the group based on how you will configure threat prevention according to location, users and applications, or threat risk.
- Keep in mind that endpoints *cannot* belong to multiple policy enforcement groups.

To create a policy enforcement group:

1. Select **Configure>Shared Objects>Policy Enforcement Groups**.
2. Click the + icon.
3. Complete the configuration by using the guidelines in the [Table 23 on page 147](#) below.
4. Click **OK**.

Table 23: Fields on the Policy Enforcement Group Page

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Group Type	Select a group type from the available choices. IP Address/Subnet or Location.

Table 23: Fields on the Policy Enforcement Group Page (*continued*)

Field	Description
Connector IPs	<p>This field is available only if the Group Type field is IP Address/Subnet</p> <p>The subnets of all connectors added in the Connector page are dynamically listed in the Available column. If the Group Type is IP Address/Subnet, the subnets within the connector instances that have the threat remediation enabled are only listed.</p> <p>When using Junos Space, Policy Enforcer is able to dynamically discover subnets configured on Juniper switches. Policy Enforcer does not have the same insight with third-party devices. Therefore you can add subnets to your connector configuration and select them here. This allows you to selectively apply policies to those subnets.</p> <p>If you have not configured a connector, you will see only Junos Space subnets discovered by Policy Enforcer. If you have a connector configured, you can see the subnets of a connector in the Available column. Hover over subnets to view the description for these subnets entered during the connector creation. You will not see any description if it is not entered during creating a connector. The description will show “No description available” for subnets that come from Junos Space.</p> <p>The Available and Selected columns have filters listed with connectors or Space. You can choose a connector and filter only the subnets belonging to that particular connector. The result shows the name of a device to which the subnet belongs and also the type of the device.</p> <p>You can also use the search bar to search and filter the result based on subnet, name of the device, or type of the device.</p> <p>Click <b>Refresh Available IPs</b> to refresh the available IP addresses or subnets. If you edit any selected items in the Selected column, the list is refreshed to the initial selected list after the refresh. A progress bar is shown with the refresh progress in percentage.</p> <p>In a scenario where there are no IP addresses or subnets, the refresh will still be successful. A message is displayed showing that the refresh was successful but there are no IP addresses or subnets found.</p>
Additional IP	<p>This field is available only if the Group Type field is IP Address/Subnet</p> <p>Enter an IP address and select the connector type from the list to add to PEG. The IP address must be within the subnet range of the selected connector. Click <b>Add</b> to add the additional IP address to the Selected column of the Connector IPs field.</p> <p>A validation is performed to check if the additional IP address is within the subnet range of the selected connector. If not, an error message is shown to enter the IP address within the subnet range.</p>
Sites	<p>Sites with the threat remediation enabled instances are only listed, if the Group Type is Location. Select the check box beside the sites in the Available list and click the &gt; icon to move them to the Selected list.</p> <p>The endpoints in the Selected list will be included in the policy enforcement group.</p>

You can create a policy enforcement group with subnets from different connectors based on how they have grouped their network segments. For example, If you have Junos Space EX switch with subnets HR: 1.1.1.1/24 and Finance: 2.2.2.2/24, ClearPass connector with subnets HR: 1.1.1.1/24 and Marketing: 2.2.2.2/24, Cisco ISE with subnets HR: 1.1.1.1/24 and Finance: 2.2.2.2/24. You can create a single policy enforcement group and name it as HR by choosing the following subnets: Junos Space EX HR: 1.1.1.1/24, ClearPass connector subnet HR: 1.1.1.1/24, and Cisco ISE connector subnet HR: 1.1.1.1/24.

## RELATED DOCUMENTATION

[Policy Enforcement Groups Overview | 146](#)

[Using Guided Setup for Sky ATP with SDSN | 124](#)

# Threat Prevention Policy Overview

Threat prevention policies provide protection and monitoring for selected threat profiles, including command and control servers, infected hosts, and malware. Using feeds from Sky ATP and optional custom feeds that you configure, ingress and egress traffic is monitored for suspicious content and behavior. Based on a threat score, detected threats are evaluated and action may be taken once a verdict is reached.

Once policies are configured, the following fields are available on the Security Director main page to provide an overview of each policy.

**Table 24: Threat Prevention Policy Fields**

Field	Description
Name	The user-created name for the policy.
Profile: C&C Server	Threat score settings overview if selected for the policy. (Otherwise this field is empty.) For example:  <b>Block: 8-10</b>  <b>Monitor: 5-7</b>  <b>Permit: 1-4</b>
Profile: Infected Host	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)
Profile: Malware HTTP	Threat score settings overview if selected for the policy. (Otherwise this is empty.)

Table 24: Threat Prevention Policy Fields (*continued*)

Field	Description
Profile: Malware SMTP	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)
Status	<p>This displays the status of the policy. This status is a clickable link you can use to change the policy status. When you first create a policy and assign it to a group, this field reads <b>View Analysis</b>. Read <a href="#">“Threat Policy Analysis Overview” on page 157</a> for more information on this field.</p> <p>If the status is Update Failed, click <b>Retry</b> to perform the rule analysis again. You can click the Update Failed status to see the corresponding job details. The rule analysis retry option is available only when the status is Update Failed.</p> <p><b>NOTE:</b> If the policy has been updated after it has already been pushed to the endpoint, the status here is <b>Update</b> with a warning icon to notify you the policy has been changed but not pushed.</p>
Policy Enforcement Group	This is the group to which the policy is assigned.
Log	This field displays the log setting for the policy.
Description	The user-created description for the policy.

## Benefits of Threat Prevention Policy

- Enables you to define and enforce policies for controlling specific applications and embedded social networking widgets.
- Reduces the need for manual updates and automatically applies policies and enforcement rules, driving down the costs of managing network security.
- Leverages the network for multiple enforcement points across the infrastructure. Enables you to stop threats closer to infection points and to prevent threats from spreading, which greatly improves the efficacy of security operations.

### RELATED DOCUMENTATION

---

[Creating Threat Prevention Policies | 151](#)

---

[Policy Enforcement Groups Overview | 146](#)

---

[Creating Geo IP Policies | 158](#)

---

[Policy Enforcer Overview | 17](#)

---

[Benefits of Policy Enforcer | 20](#)

---

[Policy Enforcer Components and Dependencies | 26](#)

---

[Sky ATP Overview | 22](#)

---

## Creating Threat Prevention Policies

To access this page, select **Configure>Threat Prevention > Policy**.

You can create threat prevention policies from the policy page.

**NOTE:** If you are creating policies for the first time, you are given the option of setting up Policy Enforcer with Sky ATP or configuring Sky ATP alone. Clicking either button takes you to quick setup for your selection. See [“Comparing the SDSN and non-SDSN Configuration Steps” on page 38](#) for a configuration comparison.

- Determine the type of profile you will use for this policy; command & control server, infected hosts, malware. You can select one or more threat profiles in a policy. Note that you configure Geo IP policies separately. See [“Creating Geo IP Policies” on page 158](#).
- Determine what action to take if a threat is found.
- Know what policy enforcement group you will add to this policy. To apply the policy, you must assign one or more policy enforcement groups. See the instructions for assigning groups to policies at the bottom of this page.
- Once policies are configured with one more groups assigned, you can save a policy in draft form or update it. Policies changes do not go live until they have been updated.
- If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. See the instructions at the bottom of this page.
- If you delete a threat prevention policy that is assigned to a policy enforcement group, a status screen appears displaying the progress of the deletion and the affected configuration items.

To create a threat prevention policy:

1. Select **Configure>Threat Prevention > Policy**.

2. Click the + icon.

The Create Threat Prevention Policy page appears.

3. Complete the configuration by using the guidelines in the [Table 25 on page 152](#), [Table 26 on page 152](#), [Table 27 on page 153](#), [Table 28 on page 153](#), and [Table 29 on page 155](#) below.

4. Click **OK**.

**Table 25: Fields on the Threat Prevention Policy Page**

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Log Setting (Policy setting for all profiles)	Select the log setting for the policy. You can log all traffic, log only blocked traffic, or log no traffic.

[Table 26 on page 152](#) shows the management of command and control server threat in a policy.

**Table 26: C&C Server Profile Management**

Field	Description
<b>Command and Control Server</b>	Select and choose settings for command and control servers. A C&C is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. Botnets can be used to gather sensitive information, such as account numbers or credit card information, or to participate in a distributed denial-of-service (DDoS) attack.
<i>Include C&amp; C profile in policy</i>	Select the check box to include management for this threat type in the policy.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. Refer to the monitoring pages in the UI to investigate, located under <b>Monitor &gt; Threat Management</b> .



Table 26: C&C Server Profile Management (*continued*)

Field	Description
Actions	<p>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Close connection and do not send a message <ul style="list-style-type: none"> <li>• Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.</li> <li>• Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.</li> </ul> </li> </ul>

Table 27 on page 153 shows the management of infected host threat in a policy.

Table 27: Infected Host Profile Management

Field	Description
<b>Infected Host</b>	Infected hosts are systems for which there is a high confidence that attackers have gained unauthorized access. Infected hosts data feeds are listed with the IP address or IP subnet of the host, along with a threat score.
<i>Include infected host profile in policy</i>	<p>Select the check box to include management for this threat type in the policy.</p> <p><b>NOTE:</b> If you want to enforce an infected host policy <i>within</i> the network, you must include a switch in the site.</p>
Actions	<p>You have following options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Quarantine—In the field provided, enter a VLAN to which quarantined files are sent. (Note that the fallback option is to block and drop the connection silently.)</li> </ul>

Table 28 on page 153 shows the management of malware threat in a policy.

Table 28: Malware Threat Profile Management

Field	Description
<b>Malware</b> (HTTP file download, SMTP File attachment, and IMAP attachments)	Malware is files that are downloaded by hosts or received as email attachments and found to be suspicious based on known signatures, URLs. or other heuristics.

Table 28: Malware Threat Profile Management (*continued*)

Field	Description
<i>Include malware profile in policy</i>	Select the check box to include management for this threat type in the policy.
HTTP file download	Turn this feature on to scan files downloaded over HTTP and then select a file scanning device profile. The device profile is configured using Sky ATP.
Scan HTTPS	Turn this feature to scan encrypted files downloaded over HTTPS.
Device Profile	Select a Sky ATP device profile. This is configured through Sky ATP. Sky ATP profiles let you define which files to send to the cloud for inspection. You can group types of files to be scanned together under a common name and create multiple profiles based on the content you want scanned.
Actions	<p>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Close connection and do not send a message <ul style="list-style-type: none"> <li>• Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.</li> <li>• Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.</li> </ul> </li> </ul>
SMTP File Attachments	Turn this feature on to inspect files received as email attachments (over SMTP only).
Scan SMTPS	<p>Enable this option to configure reverse proxy for SMTP.</p> <p>The reverse proxy does not prohibit server certificates. It forwards the actual server certificate or chain as is to the client without modifying it.</p>
Device Profile	<p>If you do not click the <b>Change</b> button to select a device profile for SMTP scanning, the device profile selected for HTTP will be used by default.</p> <p>Select <b>Change</b> to use a different device profile for SMTP.</p> <p>Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.</p>
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP and SMTP. (Note: There is no monitoring setting for malware.)

Table 28: Malware Threat Profile Management (*continued*)

Field	Description
Actions	Actions for SMTP File Attachments include: Quarantine, Deliver malicious messages with warning headers added, and Permit. This actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
IMAP Attachments	Turn this feature on to select a a file scanning device profile and threat score ranges to apply to IMAP e-mails.
Scan IMAPS	Enable this option to configure reverse proxy for IMAP e-mails.
Device Profile	<p>If you do not click the <b>Change</b> button to select a device profile for IMAP scanning, the device profile selected for HTTP will be used by default.</p> <p>Select <b>Change</b> to use a different device profile for IMAP.</p> <p>Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.</p>
Actions	Actions for IMAP Attachments include: Block, Deliver malicious messages with warning headers added, and Permit. This actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP, SMTP, and IMAP. (Note: There is no monitoring setting for malware.)

[Table 29 on page 155](#) shows the management of DDoS threat in a policy

Table 29: DDoS Threat Profile Management

Field	Description
<i>Include DDoS Profile in Policy</i>	<p>Enable this option to include the management of Distributed denial-of-service (DDoS) protection that enables the MX router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.</p> <p>When you create a threat policy for the DDoS profile, it is not pushed to the device because the policy is not yet assigned to any device. Assign the policy to the policy enforcement group. Because the policy is created for the MX router, rule analysis is not initiated when a policy is assigned to the policy enforcement group (PEG).</p>

Table 29: DDoS Threat Profile Management (*continued*)

Field	Description
Actions	<p>Select the following actions from the list for the DDoS profile:</p> <ul style="list-style-type: none"> <li>• <b>Block</b>—Use this option to block the DDoS attack.</li> <li>• <b>Rate Limit Value</b>—Use this option to limit the bandwidth on the flow route. You can express the rate limit value in Kbps, Mbps, or Gbps units. The rate limit range is 10Kbps to 100Gbps.</li> <li>• <b>Forward to</b>—Use this option to configure the routing next hop to forward the packets for scrubbing.</li> </ul>
Scrubbing Site	Specify a routing instance to which packets are forwarded in the <i>as-number:community-value</i> format, where each value is a decimal number. For example, 65001:100.

Once you have a threat prevention policy, you assign one or more groups to it:

1. In the threat prevention policy main page (located under **Configure > Threat Prevention > Policy**), find the appropriate policy.
2. In the Groups column, click the **Assign to Groups** link that appears here when there are no policy enforcement groups assigned or click the group name that appears in this column to edit the existing list of assigned groups. You can also select the check box beside a policy and click the **Assign to Groups** button at the top of the page. See [“Policy Enforcement Groups Overview” on page 146](#).
3. In the Assign to Groups page, select the check box beside a group in the Available list and click the > icon to move it to the Selected list. The groups in the Selected list will be assigned to the policy.
4. Click **OK**.
5. Once one or more policy enforcement groups have been assigned, a **Ready to Update** link appears in the Status column. You must update to apply your new or edited policy configuration. Clicking the Ready to Update link takes you the Threat Policy Analysis page. See [“Threat Policy Analysis Overview” on page 157](#). From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.
6. If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. Navigate to **Configure > Firewall Policy > Policies**. In the Advanced Security column, click an item to access the Edit Advanced Security page and select the threat prevention policy from the **Threat Prevention** pulldown list.

## RELATED DOCUMENTATION

---

[Comparing the SDSN and non-SDSN Configuration Steps | 38](#)


---

[Creating Policy Enforcement Groups | 147](#)


---

[Threat Policy Analysis Overview | 157](#)


---

[Creating Geo IP Policies | 158](#)


---

[Threat Prevention Policy Overview | 149](#)


---

[Policy Enforcer Overview | 17](#)


---

[Benefits of Policy Enforcer | 20](#)


---

[Policy Enforcer Components and Dependencies | 26](#)


---

[Sky ATP Overview | 22](#)


---

## Threat Policy Analysis Overview

To access this page, click **Configure>Threat Prevention > Policy** and click the **Ready to Update** link in the Status column.

You can update policy changes from this page. Policies must be updated before they can go live.

**NOTE:** If the policy has been updated after it has already been pushed to the endpoint, the status here is **Update** with a warning icon to notify you the policy has been changed but not pushed.

Use the threat policy analysis page to view your pending policy changes in chronological order. Click the **View Analysis** link to view the changes. In the Action section, you can select to Update now, Update later, or Save the changes without updating. If you select to update later, you can schedule a time to update.

By clicking on the policy links, you can update only the policies you select and choose not to update others.

### RELATED DOCUMENTATION

---

[Threat Prevention Policy Overview | 149](#)


---

[Creating Threat Prevention Policies | 151](#)


---

# Geo IP Overview

Geo IP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A Geo IP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping IP address to the sources of attack traffic, geographic regions of origin can be determined, giving you the ability to filter traffic to and from specific locations in the world.

## RELATED DOCUMENTATION

---

[Creating Geo IP Policies | 158](#)

---

[Threat Prevention Policy Overview | 149](#)

---

[Sky ATP Realm Overview | 163](#)

## Creating Geo IP Policies

To access this page, click **Configure>Shared Objects>Geo IP**.

You can create Geo IP policies from the Geo IP policies page.

- You must have a Sky ATP account to receive Geo IP feeds. Make sure you configure the necessary steps for Sky ATP before creating a Geo IP policy.
- Geo IP filtering is a useful tool when you are experiencing certain types of attacks, such as DDOS from specific geographical locations.
- If you are using Sky ATP without Policy Enforcer, you must select your Geo IP policy as the source and/or destination of a firewall rule to apply it.

To create a Geo IP policy:

1. Select **Configure>Shared Objects>Geo IP**.
2. Click the + icon.
3. Complete the configuration by using the guidelines in [Table 30 on page 159](#) below.
4. Click **OK**.

Table 30: Fields on the Geo IP Policy Page

Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Countries	Select the check box beside the countries in the Available list and click the > icon to move them to the Selected list. The countries in the Selected list will be included in the policy and action will be taken according to their threat level.
Block Traffic	Choose what traffic to block from the selected countries. Incoming traffic, Outgoing traffic, or Incoming and Outgoing traffic. (Policy Enforcer only)
Log Setting	Choose to log all traffic or only blocked traffic. (Policy Enforcer only)

Once you have a Geo IP policy, you assign it to one more groups (Policy Enforcer only):

1. In the Group column, click the **Assign to Groups** link that appears here when there are no groups assigned or click the group name that appears in this column to edit the existing list of assigned groups.
2. In the Assign to Groups page, select the check box beside a group in the Available list and click the > icon to move it to the Selected list. The groups in the Selected list will be assigned to the policy.
3. Click **OK**.
4. Once one or more groups have been assigned, a **Ready to Update** link appears in the Status column. You must update to apply your new or edited policy configuration. Clicking the Ready to Update link takes you the Threat Policy Analysis page. See [“Threat Policy Analysis Overview” on page 157](#). From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.
5. If you are using Sky ATP without Policy Enforcer, you must select your Geo IP policy as the source and/or destination of a firewall rule. Navigate to **Configure > Firewall Policy > Policies**.

## RELATED DOCUMENTATION

[Creating Policy Enforcement Groups | 147](#)

[Creating Threat Prevention Policies | 151](#)

[Threat Policy Analysis Overview | 157](#)

Geo IP Overview | 158

Configuring Cloud Feeds Only | 176



# 9

CHAPTER

## Configuring Sky ATP (without Guided Setup)

---

Configuring Sky ATP (No SDSN and No Guided Setup) Overview | **162**

Sky ATP Realm Overview | **163**

Creating Sky ATP Realms and Enrolling Devices or Associating Sites | **164**

Threat Prevention Policy Overview | **166**

Creating Threat Prevention Policies | **169**

---

# Configuring Sky ATP (No SDSN and No Guided Setup)

## Overview

This is an outline of the configuration tasks you must complete to configure Sky ATP mode without SDSN mode.

**NOTE:** Configuring Policy Enforcer (SDSN mode) is required if you want to work on the SDSN architecture from within Security Director.

If you prefer to use guided setup, which automatically takes you through the steps listed below, it is located under **Configure>Guided Setup >Sky ATP**.

- A Sky ATP license and account are needed for all threat prevention types (Sky ATP with PE, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to [“Obtaining a Sky ATP License” on page 62](#) for instructions on obtaining a Sky ATP premium license.
  - Before you configure Sky ATP you must enter the IP address and login credentials for the policy enforcer virtual machine. Go to **Administration > Policy Enforcer > Settings**. Once this information is entered, you can begin the setup process. See [“Policy Enforcer Settings” on page 70](#). (Refer to [“Policy Enforcer Installation Overview” on page 41](#) for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)
1. Create one or more Sky ATP realms and enroll SRX Series devices in the appropriate realm. (Enroll devices by clicking **Add Devices** in the list view once the realm is created.)  
  
In the UI, navigate to **Configure>Threat Prevention>Sky ATP Realms**. Click the + icon to add a new Sky ATP realm.  
  
See [“Creating Sky ATP Realms and Enrolling Devices or Associating Sites” on page 138](#) for details.
  2. Create a threat prevention policy, including profiles for one or more threat types: C&C server, infected host, or malware.  
  
In the UI, navigate to **Configure>Threat Prevention >Policy**. Click the + icon to create a new threat prevention policy.  
  
See [“Creating Threat Prevention Policies” on page 151](#) for details.
  3. You must assign a threat prevention policy to a firewall rule before it can take affect.

In the UI, navigate to **Configure > Firewall Policy > Policies**. In the Advanced Security column, click an item to access the Edit Advanced Security page and select the threat prevention policy from the **Threat Prevention** pulldown list.

RELATED DOCUMENTATION

<a href="#">Creating Sky ATP Realms and Enrolling Devices or Associating Sites   138</a>
<a href="#">Creating Threat Prevention Policies   151</a>
<a href="#">Creating Geo IP Policies   158</a>

# Sky ATP Realm Overview

A security realm is a group identifier for an organization used to restrict access to Web applications. You must create at least one security realm to login into Sky ATP. Once you create a realm, you can enroll SRX Series devices into the realm. You can also give more users (administrators) permission to access the realm.

If you have multiple security realms, note that each SRX Series device can only be bound to one realm, and users cannot travel between realms.

[Table 31 on page 163](#) provides the guidelines on using the fields on the Sky ATP Realm page.

Table 31: Fields on the Sky ATP Realm Page

Field	Description
Realm	Specifies the name of a realm.
Sites	Specifies the site name associated to the realm.
Location	Specifies the region of the realm.
Devices	Specifies the perimeter firewall devices that are enrolled to Sky ATP.
Enrollment Status	Specifies the enrollment status of the realm.

RELATED DOCUMENTATION

<a href="#">Creating Sky ATP Realms and Enrolling Devices or Associating Sites   138</a>
--

## Creating Sky ATP Realms and Enrolling Devices or Associating Sites

To access this page, click **Configure>Threat Prevention>Sky ATP Realms**.

You can create Sky ATP realms from the Sky ATP page.

- Understand which type of Sky ATP license you have: free, basic, or premium. The license controls which Sky ATP features are available.
- To configure a Sky ATP realm, you must already have a Sky ATP account with an associated license.
- Ensure that the internet connectivity is available for Policy Enforcer. Without the internet connectivity, you cannot create a realm.
- Decide which region will be covered by the realm you are creating. You must select a region when you configure a realm.
- Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Sky ATP or Policy Enforcer configuration.

To configure a Sky ATP Realm:

1. Select **Configure>Threat Prevention>Sky ATP Realms**.
2. Click the + icon.
3. Complete the initial configuration by using the guidelines in [Table 19 on page 139](#) below.

Table 32: Fields on the Add Sky ATP Realm Page

Field	Description
Location	<p>Select a region of the world from the available choices.</p> <p>The following options are available in the Location list:</p> <ul style="list-style-type: none"> <li>• North America</li> <li>• European Region</li> <li>• Canada</li> <li>• Asia Pacific</li> </ul> <p>By default, the North America value appears in the list. To know more about the geographic region, see <a href="#">here</a>.</p>
Username	Enter your e-mail address. Your username for Sky ATP is your e-mail address.
Password	Enter a unique string at least 8 characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character (~!@\$%^&*()_+={}[] ;:<>./?); no spaces are allowed, and you cannot use the same sequence of characters that are in your username.
Realm	<p>Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed.</p> <p><b>NOTE:</b> When you create a custom feed with a realm, the feed is associated at the site level and not at the realm level. If you modify this realm and associate new sites to it, a warning message is shown that there are custom feeds are associated with this realm. Changing the site information will change the custom feed information. You must go and edit the custom feed that was associated with this realm and verify the realm association.</p>

- Click **Next** and guided setup walks you through the steps for enrolling devices into the realm and associating sites for Policy Enforcer.

The next steps include the following:

- If you are using Sky ATP with PE and you have no devices in enrolled in the realm, you are asked to select devices in the box on the left and move them to the right to enroll them. All selected devices are automatically enrolled with Sky ATP when you finish guided setup. To disenroll a device, you can edit a realm and move the device back to the left side box.

**NOTE:** Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Sky ATP or Policy Enforcer configuration.

6. Next you select a Site from the list to contain the devices. If there are no sites associated with the realm, click **Create new site**. See [“Creating Secure Fabric and Sites” on page 144](#).

**NOTE:** If you are using Sky ATP without PE, you are not prompted to select a site.

7. Once the devices and site are selected, you use the sidebar to choose a threshold level at which selected administrators are notified via email about infected host events. Click the+ sign if you want to add new administrators to the list.
8. Finally, you select one or more check boxes for event types you want to log.
9. Click **Finish**.

**NOTE:** If you enrolled a device into a realm from within Security Director and you want to disenroll it, you must do that from within Security Director. If you enrolled a device into a realm from within Sky ATP and you want to disenroll it, you must do that from within Sky ATP. You cannot disenroll a device from within Security Directory that was enrolled from within Sky ATP.

## RELATED DOCUMENTATION

[Sky ATP Realm Overview](#) | 163

[Using Guided Setup for Sky ATP](#) | 128

[Creating Secure Fabric and Sites](#) | 144

# Threat Prevention Policy Overview

Threat prevention policies provide protection and monitoring for selected threat profiles, including command and control servers, infected hosts, and malware. Using feeds from Sky ATP and optional custom feeds that you configure, ingress and egress traffic is monitored for suspicious content and behavior. Based on a threat score, detected threats are evaluated and action may be taken once a verdict is reached.

Once policies are configured, the following fields are available on the Security Director main page to provide an overview of each policy.

Table 33: Threat Prevention Policy Fields

Field	Description
Name	The user-created name for the policy.
Profile: C&C Server	Threat score settings overview if selected for the policy. (Otherwise this field is empty.) For example:  <b>Block: 8-10</b>  <b>Monitor: 5-7</b>  <b>Permit: 1-4</b>
Profile: Infected Host	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)
Profile: Malware HTTP	Threat score settings overview if selected for the policy. (Otherwise this is empty.)
Profile: Malware SMTP	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)
Status	<p>This displays the status of the policy. This status is a clickable link you can use to change the policy status. When you first create a policy and assign it to a group, this field reads <b>View Analysis</b>. Read <a href="#">“Threat Policy Analysis Overview” on page 157</a> for more information on this field.</p> <p>If the status is Update Failed, click <b>Retry</b> to perform the rule analysis again. You can click the Update Failed status to see the corresponding job details. The rule analysis retry option is available only when the status is Update Failed.</p> <p><b>NOTE:</b> If the policy has been updated after it has already been pushed to the endpoint, the status here is <b>Update</b> with a warning icon to notify you the policy has been changed but not pushed.</p>
Policy Enforcement Group	This is the group to which the policy is assigned.
Log	This field displays the log setting for the policy.
Description	The user-created description for the policy.

## Benefits of Threat Prevention Policy

- Enables you to define and enforce policies for controlling specific applications and embedded social networking widgets.
- Reduces the need for manual updates and automatically applies policies and enforcement rules, driving down the costs of managing network security.
- Leverages the network for multiple enforcement points across the infrastructure. Enables you to stop threats closer to infection points and to prevent threats from spreading, which greatly improves the efficacy of security operations.

### RELATED DOCUMENTATION

---

[Creating Threat Prevention Policies | 151](#)

---

[Policy Enforcement Groups Overview | 146](#)

---

[Creating Geo IP Policies | 158](#)

---

[Policy Enforcer Overview | 17](#)

---

[Benefits of Policy Enforcer | 20](#)

---

[Policy Enforcer Components and Dependencies | 26](#)

---

[Sky ATP Overview | 22](#)



# Creating Threat Prevention Policies

To access this page, select **Configure>Threat Prevention > Policy**.

You can create threat prevention policies from the policy page.

**NOTE:** If you are creating policies for the first time, you are given the option of setting up Policy Enforcer with Sky ATP or configuring Sky ATP alone. Clicking either button takes you to quick setup for your selection. See [“Comparing the SDSN and non-SDSN Configuration Steps” on page 38](#) for a configuration comparison.

- Determine the type of profile you will use for this policy; command & control server, infected hosts, malware. You can select one or more threat profiles in a policy. Note that you configure Geo IP policies separately. See [“Creating Geo IP Policies” on page 158](#).
- Determine what action to take if a threat is found.
- Know what policy enforcement group you will add to this policy. To apply the policy, you must assign one or more policy enforcement groups. See the instructions for assigning groups to policies at the bottom of this page.
- Once policies are configured with one more groups assigned, you can save a policy in draft form or update it. Policies changes do not go live until they have been updated.
- If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. See the instructions at the bottom of this page.
- If you delete a threat prevention policy that is assigned to a policy enforcement group, a status screen appears displaying the progress of the deletion and the affected configuration items.

To create a threat prevention policy:

1. Select **Configure>Threat Prevention > Policy**.
2. Click the + icon.

The Create Threat Prevention Policy page appears.

3. Complete the configuration by using the guidelines in the [Table 25 on page 152](#), [Table 26 on page 152](#), [Table 27 on page 153](#), [Table 28 on page 153](#), and [Table 29 on page 155](#) below.
4. Click **OK**.

Table 34: Fields on the Threat Prevention Policy Page

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Log Setting (Policy setting for all profiles)	Select the log setting for the policy. You can log all traffic, log only blocked traffic, or log no traffic.

Table 26 on page 152 shows the management of command and control server threat in a policy.

Table 35: C&amp;C Server Profile Management

Field	Description
<b>Command and Control Server</b>	Select and choose settings for command and control servers. A C&C is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. Botnets can be used to gather sensitive information, such as account numbers or credit card information, or to participate in a distributed denial-of-service (DDoS) attack.
<i>Include C&amp; C profile in policy</i>	Select the check box to include management for this threat type in the policy.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. Refer to the monitoring pages in the UI to investigate, located under <b>Monitor &gt; Threat Management</b> .
Actions	<p>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Close connection and do not send a message <ul style="list-style-type: none"> <li>• Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.</li> <li>• Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.</li> </ul> </li> </ul>

Table 27 on page 153 shows the management of infected host threat in a policy.

Table 36: Infected Host Profile Management

Field	Description
<b>Infected Host</b>	Infected hosts are systems for which there is a high confidence that attackers have gained unauthorized access. Infected hosts data feeds are listed with the IP address or IP subnet of the host, along with a threat score.
<i>Include infected host profile in policy</i>	Select the check box to include management for this threat type in the policy.  <b>NOTE:</b> If you want to enforce an infected host policy <i>within</i> the network, you must include a switch in the site.
Actions	You have following options: <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Quarantine—In the field provided, enter a VLAN to which quarantined files are sent. (Note that the fallback option is to block and drop the connection silently.)</li> </ul>

[Table 28 on page 153](#) shows the management of malware threat in a policy.

Table 37: Malware Threat Profile Management

Field	Description
<b>Malware</b> (HTTP file download, SMTP File attachment, and IMAP attachments)	Malware is files that are downloaded by hosts or received as email attachments and found to be suspicious based on known signatures, URLs. or other heuristics.
<i>Include malware profile in policy</i>	Select the check box to include management for this threat type in the policy.
HTTP file download	Turn this feature on to scan files downloaded over HTTP and then select a file scanning device profile. The device profile is configured using Sky ATP.
Scan HTTPS	Turn this feature to scan encrypted files downloaded over HTTPS.
Device Profile	Select a Sky ATP device profile. This is configured through Sky ATP. Sky ATP profiles let you define which files to send to the cloud for inspection. You can group types of files to be scanned together under a common name and create multiple profiles based on the content you want scanned.

Table 37: Malware Threat Profile Management (*continued*)

Field	Description
Actions	<p>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Close connection and do not send a message <ul style="list-style-type: none"> <li>• Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.</li> <li>• Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.</li> </ul> </li> </ul>
SMTP File Attachments	Turn this feature on to inspect files received as email attachments (over SMTP only).
Scan SMTPS	<p>Enable this option to configure reverse proxy for SMTP.</p> <p>The reverse proxy does not prohibit server certificates. It forwards the actual server certificate or chain as is to the client without modifying it.</p>
Device Profile	<p>If you do not click the <b>Change</b> button to select a device profile for SMTP scanning, the device profile selected for HTTP will be used by default.</p> <p>Select <b>Change</b> to use a different device profile for SMTP.</p> <p>Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.</p>
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP and SMTP. (Note: There is no monitoring setting for malware.)
Actions	Actions for SMTP File Attachments include: Quarantine, Deliver malicious messages with warning headers added, and Permit. This actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
IMAP Attachments	Turn this feature on to select a a file scanning device profile and threat score ranges to apply to IMAP e-mails.
Scan IMAPS	Enable this option to configure reverse proxy for IMAP e-mails.

Table 37: Malware Threat Profile Management (*continued*)

Field	Description
Device Profile	<p>If you do not click the <b>Change</b> button to select a device profile for IMAP scanning, the device profile selected for HTTP will be used by default.</p> <p>Select <b>Change</b> to use a different device profile for IMAP.</p> <p>Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.</p>
Actions	Actions for IMAP Attachments include: Block, Deliver malicious messages with warning headers added, and Permit. These actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP, SMTP, and IMAP. (Note: There is no monitoring setting for malware.)

[Table 29 on page 155](#) shows the management of DDoS threat in a policy

Table 38: DDoS Threat Profile Management

Field	Description
<i>Include DDoS Profile in Policy</i>	<p>Enable this option to include the management of Distributed denial-of-service (DDoS) protection that enables the MX router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.</p> <p>When you create a threat policy for the DDoS profile, it is not pushed to the device because the policy is not yet assigned to any device. Assign the policy to the policy enforcement group. Because the policy is created for the MX router, rule analysis is not initiated when a policy is assigned to the policy enforcement group (PEG).</p>
Actions	<p>Select the following actions from the list for the DDoS profile:</p> <ul style="list-style-type: none"> <li>• <b>Block</b>—Use this option to block the DDoS attack.</li> <li>• <b>Rate Limit Value</b>—Use this option to limit the bandwidth on the flow route. You can express the rate limit value in Kbps, Mbps, or Gbps units. The rate limit range is 10Kbps to 100Gbps.</li> <li>• <b>Forward to</b>—Use this option to configure the routing next hop to forward the packets for scrubbing.</li> </ul>
Scrubbing Site	Specify a routing instance to which packets are forwarded in the <i>as-number:community-value</i> format, where each value is a decimal number. For example, 65001:100.

Once you have a threat prevention policy, you assign one or more groups to it:

1. In the threat prevention policy main page (located under **Configure>Threat Prevention > Policy**), find the appropriate policy.
2. In the Groups column, click the **Assign to Groups** link that appears here when there are no policy enforcement groups assigned or click the group name that appears in this column to edit the existing list of assigned groups. You can also select the check box beside a policy and click the **Assign to Groups** button at the top of the page. See [“Policy Enforcement Groups Overview” on page 146](#) .
3. In the Assign to Groups page, select the check box beside a group in the Available list and click the > icon to move it to the Selected list. The groups in the Selected list will be assigned to the policy.
4. Click **OK**.
5. Once one or more policy enforcement groups have been assigned, a **Ready to Update** link appears in the Status column. You must update to apply your new or edited policy configuration. Clicking the Ready to Update link takes you the Threat Policy Analysis page. See [“Threat Policy Analysis Overview” on page 157](#). From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.
6. If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. Navigate to **Configure > Firewall Policy > Policies**. In the Advanced Security column, click an item to access the Edit Advanced Security page and select the threat prevention policy from the **Threat Prevention** pulldown list.

## RELATED DOCUMENTATION

[Comparing the SDSN and non-SDSN Configuration Steps | 38](#)

[Creating Policy Enforcement Groups | 147](#)

[Threat Policy Analysis Overview | 157](#)

[Creating Geo IP Policies | 158](#)

[Threat Prevention Policy Overview | 149](#)

[Policy Enforcer Overview | 17](#)

[Benefits of Policy Enforcer | 20](#)

[Policy Enforcer Components and Dependencies | 26](#)

[Sky ATP Overview | 22](#)

# 10

CHAPTER

## Configuring Cloud Feeds Only

---

Configuring Cloud Feeds Only | **176**

---

# Configuring Cloud Feeds Only

This is an outline of the configuration tasks you must complete to configure Cloud feeds only threat prevention.

**NOTE:** Since devices are not enrolled to Sky ATP in Cloud feed only mode, there is no information to display under Monitor > Threat Prevention, and therefore those screens are unavailable.

- A Sky ATP license and account are needed for the following (Sky ATP with SDSN, Sky ATP, and Cloud feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to [“Obtaining a Sky ATP License” on page 62](#) for instructions on obtaining a Sky ATP premium license.
- Before you configure Cloud Feeds you must enter the IP address and login credentials for the policy enforcer virtual machine. Go to **Administration > Policy Enforcer > Settings**. Once this information is entered, you can begin the setup process. See [“Policy Enforcer Settings” on page 70](#). (Refer to [“Deploying and Configuring the Policy Enforcer with OVA files” on page 42](#) for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)

To configure Security Director for Cloud feed only threat prevention, do the following:

**NOTE:** Cloud feed only configuration is similar to Sky ATP (without SDSN) configuration. The only differences being that devices do not have to be enrolled to Sky ATP and the only threat prevention types available are command and control server and Geo IP.

1. Create one or more Sky ATP realms and add devices to the realm. (Note that devices do not have to be enrolled to Sky ATP for Cloud Feed only mode.)

In the UI, navigate to **Configure>Threat Prevention>Sky ATP Realms**. Click the + icon to add a new Sky ATP realm.

See [“Creating Sky ATP Realms and Enrolling Devices or Associating Sites” on page 138](#) for details.

2. Create sites and add devices to those sites.

In the UI, navigate to **Devices >Secure Fabric**. Click the + icon to create a new site.

See [“Creating Secure Fabric and Sites” on page 144](#) for details.



3. Create a policy enforcement group.

In the UI, navigate to **Configure>Shared Objects>Policy Enforcement Groups**. Click the + icon to create a new policy enforcement group.

See [“Creating Policy Enforcement Groups” on page 147](#) for details.

4. Create a threat prevention policy for Command and Control server, Geo IP, or Infected hosts.

In the UI, navigate to **Configure>Threat Prevention >Policy**. Click the + icon to create a new threat prevention policy.

See [“Creating Threat Prevention Policies” on page 151](#) for details.

5. Configure Geo IP settings for inclusion in a firewall policy. See [“Creating Geo IP Policies” on page 158](#).

You must select your Geo IP policy as the source and/or destination of a firewall rule before it can take effect. Navigate to **Configure > Firewall Policy > Policies**.

.

## RELATED DOCUMENTATION

---

[Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 138](#)

---

[Creating Geo IP Policies | 158](#)

---

[Creating Threat Prevention Policies | 151](#)

---

[Policy Enforcer Settings | 70](#)

# 11

CHAPTER

## Configuring No Sky ATP (No Selection) (without Guided Setup)

---

Secure Fabric Overview | **179**

| **180**

Creating Policy Enforcement Groups | **182**

Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist | **184**

Creating Custom Feeds, Infected Host | **189**

Threat Prevention Policy Overview | **193**

Creating Threat Prevention Policies | **195**

---

# Secure Fabric Overview

Secure Fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices), used in policy enforcement groups. When threat prevention policies are applied to policy enforcement groups, the system automatically discovers to which sites those groups belong. This is how threat prevention is aggregated across your secure fabric.

- **Add Enforcement Points**—Click the **Add Enforcement Points** link to add Firewalls, Switches, and/or Connectors. There is a one-to-one mapping between devices with sites. If a device is mapped to a site, you cannot use the same device to map to a different site. The connector can be mapped to multiple sites. To filter by type, click the three vertical dots beside the search field and select the check box for the device type. See [“Creating Secure Fabric and Sites” on page 144](#) for more information.
- **Drag and Drop Enforcement Points**—From the main page, you can select enforcement points and drag them to other sites to include them there. When you drag, the enforcement point is disenrolled from the current site and gets enrolled to the new site where the enforcement point is dropped.

You can either have switches or a connector as enforcement points and not both. However, you can drag a switch and add to a site that already has a switch or SRX Series device.

[Table 20 on page 141](#) shows fields on the Secure Fabric page.

Table 39: Fields on the Secure Fabric Page

Field	Description
Site	Specifies the name of the secure fabric site.
Enforcement Points	<p>Specifies the enforcement points for that particular site, if enforcement points are already added. If not added, click <b>Add Enforcement Points</b> to add Firewalls, Switches, or Connectors as enforcement points.</p> <p>A firewall icon is shown against some of the devices to indicate that they are the perimeter firewalls.</p> <p>For connectors, if you hover over the enforcement point, a tool tip is shown listing the corresponding vSRX devices with IP addresses and descriptions.</p>
Model	Specifies the type of the enforcement point. For example, vSRX, QFX, Connector.
IP	Specifies the IP address of the enforcement point, if the enforcement point is available.

Table 39: Fields on the Secure Fabric Page (*continued*)

Field	Description
SKYATP Enroll Status	<p>Specifies the status of the SkyATP enrollment.</p> <p>The Success status with a warning symbol indicates that the device is enabled for cloud feeds only and there is no support for malware capability and enhanced mode. This field will be blank if the device fails to disenroll SkyATP.</p> <p>If the status is Failed, click <b>Retry</b> to enroll the device with Sky ATP again. You can hover over the Failed status to see the corresponding job details. The device enroll retry option is available only when the status is Failed.</p>
Last Updated	Specifies the date on which the Secure Fabric page was last updated.
Description	Specifies the description that you had entered at the time of creating a secure fabric site.

## RELATED DOCUMENTATION

[Creating Secure Fabric and Sites | 144](#)

[Policy Enforcement Groups Overview | 146](#)

[Threat Prevention Policy Overview | 149](#)

To access this page, click **Devices>Secure Fabric**.

You create sites within your secure fabric from the secure fabric page.

- Plan out your sites in advance. A site is a grouping of network devices, including firewalls and switches, that contribute to threat prevention.
- Keep in mind that when you create a site, you must identify the perimeter firewalls so you can enroll them with Sky ATP.
- If you want to enforce an infected host policy within the network, you must assign a switch to the site.
- Devices *cannot* belong to multiple sites.
- Switches and connectors *cannot* be added to the same site

To create a site within your secure fabric:

1. Select **Devices>Secure Fabric**.
2. Click the + icon.
3. Complete the configuration by using the guidelines in [Table 22 on page 145](#) below.

4. Click **OK**.
5. Create a new site and add an enforcement point to a site.

**Table 40: Fields on the Create Site Page**

Field	Description
Site	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.



**WARNING:** If you add certain SRX Series Devices to your Secure Fabric as enforcement points, you may see a warning that the device(s) must be reconfigured in enhanced mode and require a reboot. Here is a list of SRX models that may require rebooting for enhanced mode after being registered with Policy Enforcer/Sky ATP.

- SRX340
- SRX345
- SRX650
- SRX240h2
- SRX320
- SRX300
- SRX550

## RELATED DOCUMENTATION

[Secure Fabric Overview | 141](#)

[Policy Enforcement Groups Overview | 146](#)

[Threat Prevention Policy Overview | 149](#)

# Creating Policy Enforcement Groups

To access this page, click **Configure>Shared Objects>Policy Enforcement Groups**.

You can create policy enforcement groups from the policy enforcement groups page.

- Know what type of endpoints you are including in your policy enforcement group: IP address/subnet, or location.
- Determine what endpoints you will add to the group based on how you will configure threat prevention according to location, users and applications, or threat risk.
- Keep in mind that endpoints *cannot* belong to multiple policy enforcement groups.

To create a policy enforcement group:

1. Select **Configure>Shared Objects>Policy Enforcement Groups**.
2. Click the + icon.
3. Complete the configuration by using the guidelines in the [Table 23 on page 147](#) below.
4. Click **OK**.

**Table 41: Fields on the Policy Enforcement Group Page**

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Group Type	Select a group type from the available choices. IP Address/Subnet or Location.

Table 41: Fields on the Policy Enforcement Group Page (*continued*)

Field	Description
Connector IPs	<p>This field is available only if the Group Type field is IP Address/Subnet</p> <p>The subnets of all connectors added in the Connector page are dynamically listed in the Available column. If the Group Type is IP Address/Subnet, the subnets within the connector instances that have the threat remediation enabled are only listed.</p> <p>When using Junos Space, Policy Enforcer is able to dynamically discover subnets configured on Juniper switches. Policy Enforcer does not have the same insight with third-party devices. Therefore you can add subnets to your connector configuration and select them here. This allows you to selectively apply policies to those subnets.</p> <p>If you have not configured a connector, you will see only Junos Space subnets discovered by Policy Enforcer. If you have a connector configured, you can see the subnets of a connector in the Available column. Hover over subnets to view the description for these subnets entered during the connector creation. You will not see any description if it is not entered during creating a connector. The description will show “No description available” for subnets that come from Junos Space.</p> <p>The Available and Selected columns have filters listed with connectors or Space. You can choose a connector and filter only the subnets belonging to that particular connector. The result shows the name of a device to which the subnet belongs and also the type of the device.</p> <p>You can also use the search bar to search and filter the result based on subnet, name of the device, or type of the device.</p> <p>Click <b>Refresh Available IPs</b> to refresh the available IP addresses or subnets. If you edit any selected items in the Selected column, the list is refreshed to the initial selected list after the refresh. A progress bar is shown with the refresh progress in percentage.</p> <p>In a scenario where there are no IP addresses or subnets, the refresh will still be successful. A message is displayed showing that the refresh was successful but there are no IP addresses or subnets found.</p>
Additional IP	<p>This field is available only if the Group Type field is IP Address/Subnet</p> <p>Enter an IP address and select the connector type from the list to add to PEG. The IP address must be within the subnet range of the selected connector. Click <b>Add</b> to add the additional IP address to the Selected column of the Connector IPs field.</p> <p>A validation is performed to check if the additional IP address is within the subnet range of the selected connector. If not, an error message is shown to enter the IP address within the subnet range.</p>
Sites	<p>Sites with the threat remediation enabled instances are only listed, if the Group Type is Location. Select the check box beside the sites in the Available list and click the &gt; icon to move them to the Selected list.</p> <p>The endpoints in the Selected list will be included in the policy enforcement group.</p>

You can create a policy enforcement group with subnets from different connectors based on how they have grouped their network segments. For example, If you have Junos Space EX switch with subnets HR: 1.1.1.1/24 and Finance: 2.2.2.2/24, ClearPass connector with subnets HR: 1.1.1.1/24 and Marketing: 2.2.2.2/24, Cisco ISE with subnets HR: 1.1.1.1/24 and Finance: 2.2.2.2/24. You can create a single policy enforcement group and name it as HR by choosing the following subnets: Junos Space EX HR: 1.1.1.1/24, ClearPass connector subnet HR: 1.1.1.1/24, and Cisco ISE connector subnet HR: 1.1.1.1/24.

## RELATED DOCUMENTATION

[Policy Enforcement Groups Overview | 146](#)

[Using Guided Setup for Sky ATP with SDSN | 124](#)

# Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist

To access this page, click **Configure>Threat Prevention>Custom Feeds**.

You can create custom feeds from the custom feeds page.

- Know what type of feed you are configuring and have all the necessary information on hand. Local feeds are created on your local system and uploaded from there.
- To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show Dynamic Addresses.
- For creating an Infected Host custom feed, see [“Creating Custom Feeds, Infected Host” on page 189](#).  
For creating a DDoS custom feed, see [“Creating Custom Feeds, DDoS” on page 220](#).

To create local file and remote file custom feeds:

1. Select **Configure>Threat Prevention>Custom Feeds**.
2. Select one of the following feed types.



Table 42: Custom Feed Categories

Feed Category	Definition
Dynamic Address	<p>A dynamic address entry provides dynamic IP address information to security policies. A dynamic address is a group of IP addresses, not just a single IP prefix, that can be imported from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. You can then configure security policies to use the dynamic addresses within a security policy.</p> <p>You can use custom feeds while configuring the firewall policy. For information on how to create dynamic addresses, see: <a href="#">Creating Dynamic Address Groups</a>.</p> <p><b>NOTE:</b> You can create multiple custom feeds for all types of feed categories.</p>
Allowlist	<p>An allowlist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the allowlist does not have to be inspected for malware.</p>
Blocklist	<p>A blocklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.</p>
Infected Host	<p>Infected hosts are hosts known to be compromised. Enter host IP addresses manually or upload a text file with the IP addresses of infected hosts. See <a href="#">“Creating Custom Feeds, Infected Host” on page 189</a> for configuration details.</p>
DDoS	<p>Using DDoS threat feed, policy Enforcer blocks source IP addresses in the feed, rate limit the traffic from the source IP addresses, and takes BGP Flowspec action to blackhole or redirect the traffic to scrubbing centers. See <a href="#">“Creating Custom Feeds, DDoS” on page 220</a> and <a href="#">“Creating Threat Prevention Policies” on page 151</a>.</p>

**NOTE:**

- The Remote Download Status field shows the status of downloading feeds from a remote file server to Policy Enforcer. This field will be blank if the locally created custom feeds.

The following statuses are shown under different scenarios:

- Pending—Status is shown as pending until Policy Enforcer downloads the new feeds from the remote file server.
- Success—Status is shown as success when Policy Enforcer downloads the feeds successfully.
- Failed—Status is shown as failed when downloading the feeds fails.
- The Days to Become Inactive field shows the number of days within which the custom feed is going to expire or become inactive. You must specify the number of days for each custom feed to be active in the Time to Live (TTL) Settings page. Whenever you make any update to a feed type in the TTL Settings page, number of days to expire is counted from that date. See [“Configuring TTL Settings for Custom Feeds” on page 223](#).

Once the Days to Become Inactive field is zero, the respective feed will become inactive and cannot be used. You must update the feed again to make it active.

3. Click **Create** and select one of the following:

- **Feeds with local files**—This is data you enter manually into the provided fields or upload from a text file on your location machine. See [Table 43 on page 187](#) for details.
- **Feeds with remote file server**—This is a data feed from a remote server. Configure communication with the remote server using instructions in [Table 44 on page 188](#).

4. Complete the configuration by using the guidelines in [Table 43 on page 187](#) or [Table 44 on page 188](#).

5. Click **OK**. Your entry is added to custom list displayed at the bottom of the page.

**NOTE:** To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show Dynamic Addresses.

If there is a firewall policy rule created using the dynamic address, you cannot delete the same dynamic address from the Custom Feeds page. You must first delete the firewall policy rule and then, delete the dynamic address from the Custom Feeds page.

Use the fields in [Table 43 on page 187](#) to add custom feeds.

Table 43: Fields on the Custom Feeds Page, Feeds with Local Files

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description for your custom feed; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Feed Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• IP, Subnet and Range—Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</li> <li>• URL and Domain—Enter the URL using the following format: http://yourfeed.com/abc and Domain using the following format: http://yourfeed.com. Wildcards and protocols are not valid entries.</li> </ul> <p><b>NOTE:</b> For Dynamic Address, you can only select IP, Subnet, and Range. For Blocklists and Allowlist, all feed types are available for selection.</p>
Sites	<p>Select the required sites from the list to associate them with the dynamic address or allowlists and blocklists feeds.</p> <p>In the default mode (no Sky ATP), only sites are listed because of no Sky ATP. The same site can be shared across dynamic address, allowlists, and blocklists feeds.</p>
Realms	<p>Select the required realms from the list, if you are in Cloud feeds only, Sky ATP, or Sky ATP with SDSN mode.</p> <p>Associate these realms with dynamic address or allowlists and blocklists feeds. The same realm can be shared across dynamic address, allowlists and blocklists feeds.</p> <p>When you are creating a Sky ATP realm, if you do not assign any sites to it, those realms are not listed here. Only realms with sites associated are listed here.</p>

Table 43: Fields on the Custom Feeds Page, Feeds with Local Files (*continued*)

Field	Description
Custom List	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Click <b>Upload File</b> to upload a text file with an IP address list. Click the <b>Add</b> button to include the address list in your custom list.</li> </ul> <p>Note that the file must contain only one item per line (no commas or semi colons). All items are validated before being added to the custom list.</p> <p>The file must not contain more than 500 entries. An error message is shown if you try to upload a file containing more than 500 IP addresses. Use the Feeds with remote file server option to upload a file containing more than 500 IP addresses.</p> <ul style="list-style-type: none"> <li>Manually enter your item in the space provided in the Custom List section. To add more items, click + to add more spaces.</li> </ul>

Table 44: Fields on the Custom Feeds Page, Feeds with Remote File Server

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description for your custom feed; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Feed Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>IP, Subnet and Range—Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</li> <li>URL and Domain—Enter the URL using the following format: http://yourfeed.com/abc and Domain using the following format: http://yourfeed.com. Wildcards and protocols are not valid entries.</li> </ul> <p><b>NOTE:</b> For Dynamic Address, you can only enter IP, Subnet, and Range. For Blocklists and Allowlist, all feed types are available for selection.</p>
Type of Server URL	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>http</li> <li>https</li> </ul>
Server File URL	Enter the URL for the remote file server.

Table 44: Fields on the Custom Feeds Page, Feeds with Remote File Server (*continued*)

Field	Description
Certificate Upload	<p>Click <b>Browse</b> and select the CA certificate to upload.</p> <p>If you do not upload a certificate for https server URL, a warning message is shown that a certificate is not uploaded and to whether proceed further or not. Click <b>Yes</b> to proceed further without uploading a certificate or <b>No</b> to go back and upload the certificate.</p>
Username	<p>Enter the credentials for the remote file server.</p> <p>This is not a mandatory field. You can still proceed to create a custom feed without entering the username.</p>
Password	<p>Enter the credentials for the remote file server.</p> <p>This is a mandatory field, if you have provided the username.</p>
Update Interval	<p>Select how often updates are retrieved from the remote files server: Hourly, Daily, Weekly, Monthly, Never</p>

## RELATED DOCUMENTATION

[Example: Creating a Dynamic Address Custom Feed and Firewall Policy | 215](#)

[Creating Custom Feeds, Infected Host | 189](#)

[Custom Feed Sources Overview | 209](#)

[Sky ATP Realm Overview | 163](#)

# Creating Custom Feeds, Infected Host

To access this page, click **Configure>Threat Prevention>Custom Feeds**.

- Note that infected hosts are hosts known to be compromised. For an infected host custom feed, enter host IP addresses manually or upload a text file with the IP addresses of infected hosts.
- If you create a custom infected hosts feed, it will override the SKY ATP infected hosts feed.
- To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show custom feed types, including infected hosts.

- Note that when Sky ATP only mode is selected as the Threat Prevention Type, the infected host custom feed is not available.
- For creating other custom feed types, see [“Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist” on page 184](#).



**WARNING:** When you have no Sky ATP Configuration Type selected (No selection), Sky ATP realms are disabled. Because site selection is usually done from the Sky ATP realm page, you must select sites from the Custom Feed - Infected Hosts page when in “No selection” mode. The custom feeds are then downloaded to the devices in the chosen sites. This is the only time site selection is available in the Custom Feeds - Infected Hosts page.

To create local file and remote file custom feeds:

1. Select **Configure>Threat Prevention>Custom Feeds**.
2. Select the **Infected Host** tab.

**NOTE:** When Sky ATP only is selected as the Threat Prevention Type, the infected host custom feed is not available.

3. Click **Create** and select one of the following:
  - **Feeds with local files**—This is data you enter manually into the provided fields or upload from a text file on your location machine. See [Table 43 on page 187](#) for details.
  - **Feeds with remote file server**—This is a data feed from a remote server. Configure communication with the remote server using instructions in [Table 44 on page 188](#).
4. Complete the configuration by using the guidelines in [Table 43 on page 187](#) or [Table 44 on page 188](#).
5. Click **OK**. Your entry is added to custom list displayed at the bottom of the page.

**NOTE:** To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show Infected Hosts, Dynamic Addresses, Allowlist and Blocklists.

Use the fields in [Table 43 on page 187](#) to add custom feeds.

Table 45: Fields on the Custom Feeds Page, Feeds with Local Files

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
Description	Enter a description for your custom feed; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.
Sites	<p>Select the required sites from the list to associate them with the infected feeds.</p> <p>In the default mode (no Sky ATP), only sites are listed because of no Sky ATP. You cannot share the same site across the same feed type. However, you can share a site across different feed types.</p>
Realms	<p>Select the required realms from the list, if you are in Cloud feeds only, or SDSN with Sky ATP only mode and associate them with dynamic address or allowlists and blocklists feeds.</p> <p>You cannot share the same realm across the same feed type. However, you can share a realm across different feed types.</p> <p>When you are creating a Sky ATP realm, if you do not assign any sites it, those realms are not listed here. Only realms with sites associated are listed here.</p>
Custom List	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Click <b>Upload File</b> to upload a text file with an IP address list. The uploading file must have the string <i>add</i> at the beginning, followed by the IP addresses. If you want to delete certain IP addresses, enter the string <i>delete</i> followed by the IP addresses to delete.</li> </ul> <p>Click the <b>Add</b> button to include the address list in your custom list.</p> <p>Note that the file must contain only one item per line (no commas or semi colons). All items are validated before being added to the custom list.</p> <ul style="list-style-type: none"> <li>Manually enter your item in the space provided in the Custom List section. To add more items, click <b>+</b> to add more spaces.</li> </ul> <p>For syntax, enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</p>

Table 46: Fields on the Custom Feeds Page, Feeds with Remote File Server

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
Description	Enter a description for your custom feed; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.

Table 46: Fields on the Custom Feeds Page, Feeds with Remote File Server (continued)

Field	Description
Type of Server URL	Select one of the following: <ul style="list-style-type: none"> <li>• http</li> <li>• https</li> </ul>
Server File URL	Enter the URL for the remote file server.
Certificate Upload	Click <b>Browse</b> and select the CA certificate to upload.  If you do not upload a certificate for https server URL, a warning message is shown that a certificate is not uploaded and to whether proceed further or not. Click <b>Yes</b> to proceed further without uploading a certificate or <b>No</b> to go back and upload the certificate.
Username	Enter the credentials for the remote file server.
Password	Enter the credentials for the remote file server.
Update Interval	Select how often updates are retrieved from the remote files server: Hourly, Daily, Weekly, Monthly, Never

You can create only a single infected host. If you want to create one more infected host, you must first delete the existing feed and create a new one.

If you try to disenroll a site in an infected host, a warning message is shown to resolve all the current infected hosts from the respective endpoints within a site. To resolve the infected hosts, log-in to Sky ATP UI, resolve the hosts, and then unassign sites from Policy Enforcer. Ensure that you always resolve the infected hosts before unassigning sites. Once you unassign sites, you cannot resolve the hosts.

## RELATED DOCUMENTATION

[Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist](#) | 184

[Custom Feed Sources Overview](#) | 209

[Sky ATP Realm Overview](#) | 163



# Threat Prevention Policy Overview

Threat prevention policies provide protection and monitoring for selected threat profiles, including command and control servers, infected hosts, and malware. Using feeds from Sky ATP and optional custom feeds that you configure, ingress and egress traffic is monitored for suspicious content and behavior. Based on a threat score, detected threats are evaluated and action may be taken once a verdict is reached.

Once policies are configured, the following fields are available on the Security Director main page to provide an overview of each policy.

**Table 47: Threat Prevention Policy Fields**

Field	Description
Name	The user-created name for the policy.
Profile: C&C Server	Threat score settings overview if selected for the policy. (Otherwise this field is empty.) For example:  <b>Block: 8-10</b>  <b>Monitor: 5-7</b>  <b>Permit: 1-4</b>
Profile: Infected Host	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)
Profile: Malware HTTP	Threat score settings overview if selected for the policy. (Otherwise this is empty.)
Profile: Malware SMTP	Threat score settings overview if selected for the policy. (Otherwise this field is empty.)

Table 47: Threat Prevention Policy Fields (continued)

Field	Description
Status	<p>This displays the status of the policy. This status is a clickable link you can use to change the policy status. When you first create a policy and assign it to a group, this field reads <b>View Analysis</b>. Read <a href="#">“Threat Policy Analysis Overview” on page 157</a> for more information on this field.</p> <p>If the status is Update Failed, click <b>Retry</b> to perform the rule analysis again. You can click the Update Failed status to see the corresponding job details. The rule analysis retry option is available only when the status is Update Failed.</p> <p><b>NOTE:</b> If the policy has been updated after it has already been pushed to the endpoint, the status here is <b>Update</b> with a warning icon to notify you the policy has been changed but not pushed.</p>
Policy Enforcement Group	This is the group to which the policy is assigned.
Log	This field displays the log setting for the policy.
Description	The user-created description for the policy.

## Benefits of Threat Prevention Policy

- Enables you to define and enforce policies for controlling specific applications and embedded social networking widgets.
- Reduces the need for manual updates and automatically applies policies and enforcement rules, driving down the costs of managing network security.
- Leverages the network for multiple enforcement points across the infrastructure. Enables you to stop threats closer to infection points and to prevent threats from spreading, which greatly improves the efficacy of security operations.

### RELATED DOCUMENTATION

[Creating Threat Prevention Policies | 151](#)

[Policy Enforcement Groups Overview | 146](#)

---

[Creating Geo IP Policies | 158](#)

---

[Policy Enforcer Overview | 17](#)

---

[Benefits of Policy Enforcer | 20](#)

---

[Policy Enforcer Components and Dependencies | 26](#)

---

[Sky ATP Overview | 22](#)

---

## Creating Threat Prevention Policies

To access this page, select **Configure>Threat Prevention > Policy**.

You can create threat prevention policies from the policy page.

**NOTE:** If you are creating policies for the first time, you are given the option of setting up Policy Enforcer with Sky ATP or configuring Sky ATP alone. Clicking either button takes you to quick setup for your selection. See [“Comparing the SDSN and non-SDSN Configuration Steps” on page 38](#) for a configuration comparison.

- Determine the type of profile you will use for this policy; command & control server, infected hosts, malware. You can select one or more threat profiles in a policy. Note that you configure Geo IP policies separately. See [“Creating Geo IP Policies” on page 158](#).
- Determine what action to take if a threat is found.
- Know what policy enforcement group you will add to this policy. To apply the policy, you must assign one or more policy enforcement groups. See the instructions for assigning groups to policies at the bottom of this page.
- Once policies are configured with one more groups assigned, you can save a policy in draft form or update it. Policies changes do not go live until they have been updated.
- If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. See the instructions at the bottom of this page.
- If you delete a threat prevention policy that is assigned to a policy enforcement group, a status screen appears displaying the progress of the deletion and the affected configuration items.

To create a threat prevention policy:

1. Select **Configure>Threat Prevention > Policy**.
2. Click the + icon.

The Create Threat Prevention Policy page appears.

3. Complete the configuration by using the guidelines in the [Table 25 on page 152](#), [Table 26 on page 152](#), [Table 27 on page 153](#), [Table 28 on page 153](#), and [Table 29 on page 155](#) below.
4. Click **OK**.

**Table 48: Fields on the Threat Prevention Policy Page**

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Log Setting (Policy setting for all profiles)	Select the log setting for the policy. You can log all traffic, log only blocked traffic, or log no traffic.

[Table 26 on page 152](#) shows the management of command and control server threat in a policy.

**Table 49: C&C Server Profile Management**

Field	Description
<b>Command and Control Server</b>	Select and choose settings for command and control servers. A C&C is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. Botnets can be used to gather sensitive information, such as account numbers or credit card information, or to participate in a distributed denial-of-service (DDoS) attack.
<i>Include C&amp; C profile in policy</i>	Select the check box to include management for this threat type in the policy.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. Refer to the monitoring pages in the UI to investigate, located under <b>Monitor &gt; Threat Management</b> .

Table 49: C&C Server Profile Management (*continued*)

Field	Description
Actions	<p>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Close connection and do not send a message <ul style="list-style-type: none"> <li>• Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.</li> <li>• Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.</li> </ul> </li> </ul>

Table 27 on page 153 shows the management of infected host threat in a policy.

Table 50: Infected Host Profile Management

Field	Description
<b>Infected Host</b>	Infected hosts are systems for which there is a high confidence that attackers have gained unauthorized access. Infected hosts data feeds are listed with the IP address or IP subnet of the host, along with a threat score.
<i>Include infected host profile in policy</i>	<p>Select the check box to include management for this threat type in the policy.</p> <p><b>NOTE:</b> If you want to enforce an infected host policy <i>within</i> the network, you must include a switch in the site.</p>
Actions	<p>You have following options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Quarantine—In the field provided, enter a VLAN to which quarantined files are sent. (Note that the fallback option is to block and drop the connection silently.)</li> </ul>

Table 28 on page 153 shows the management of malware threat in a policy.

Table 51: Malware Threat Profile Management

Field	Description
<b>Malware</b> (HTTP file download, SMTP File attachment, and IMAP attachments)	Malware is files that are downloaded by hosts or received as email attachments and found to be suspicious based on known signatures, URLs. or other heuristics.

Table 51: Malware Threat Profile Management (*continued*)

Field	Description
<i>Include malware profile in policy</i>	Select the check box to include management for this threat type in the policy.
HTTP file download	Turn this feature on to scan files downloaded over HTTP and then select a file scanning device profile. The device profile is configured using Sky ATP.
Scan HTTPS	Turn this feature to scan encrypted files downloaded over HTTPS.
Device Profile	Select a Sky ATP device profile. This is configured through Sky ATP. Sky ATP profiles let you define which files to send to the cloud for inspection. You can group types of files to be scanned together under a common name and create multiple profiles based on the content you want scanned.
Actions	<p>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</p> <ul style="list-style-type: none"> <li>• Drop connection silently (This is the default and recommended setting.)</li> <li>• Close connection and do not send a message <ul style="list-style-type: none"> <li>• Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.</li> <li>• Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.</li> </ul> </li> </ul>
SMTP File Attachments	Turn this feature on to inspect files received as email attachments (over SMTP only).
Scan SMTPS	<p>Enable this option to configure reverse proxy for SMTP.</p> <p>The reverse proxy does not prohibit server certificates. It forwards the actual server certificate or chain as is to the client without modifying it.</p>
Device Profile	<p>If you do not click the <b>Change</b> button to select a device profile for SMTP scanning, the device profile selected for HTTP will be used by default.</p> <p>Select <b>Change</b> to use a different device profile for SMTP.</p> <p>Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.</p>
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP and SMTP. (Note: There is no monitoring setting for malware.)

Table 51: Malware Threat Profile Management (*continued*)

Field	Description
Actions	Actions for SMTP File Attachments include: Quarantine, Deliver malicious messages with warning headers added, and Permit. This actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
IMAP Attachments	Turn this feature on to select a a file scanning device profile and threat score ranges to apply to IMAP e-mails.
Scan IMAPS	Enable this option to configure reverse proxy for IMAP e-mails.
Device Profile	<p>If you do not click the <b>Change</b> button to select a device profile for IMAP scanning, the device profile selected for HTTP will be used by default.</p> <p>Select <b>Change</b> to use a different device profile for IMAP.</p> <p>Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.</p>
Actions	Actions for IMAP Attachments include: Block, Deliver malicious messages with warning headers added, and Permit. This actions are set in Sky ATP. Refer to the Sky ATP documentation for information.
Threat Score	Use the slider to change the action to be taken based on the threat score. Threat scores are assigned using several criteria. This threat score applies to all malware, HTTP, SMTP, and IMAP. (Note: There is no monitoring setting for malware.)

[Table 29 on page 155](#) shows the management of DDoS threat in a policy

Table 52: DDoS Threat Profile Management

Field	Description
<i>Include DDoS Profile in Policy</i>	<p>Enable this option to include the management of Distributed denial-of-service (DDoS) protection that enables the MX router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.</p> <p>When you create a threat policy for the DDoS profile, it is not pushed to the device because the policy is not yet assigned to any device. Assign the policy to the policy enforcement group. Because the policy is created for the MX router, rule analysis is not initiated when a policy is assigned to the policy enforcement group (PEG).</p>

Table 52: DDoS Threat Profile Management (*continued*)

Field	Description
Actions	<p>Select the following actions from the list for the DDoS profile:</p> <ul style="list-style-type: none"> <li>• <b>Block</b>—Use this option to block the DDoS attack.</li> <li>• <b>Rate Limit Value</b>—Use this option to limit the bandwidth on the flow route. You can express the rate limit value in Kbps, Mbps, or Gbps units. The rate limit range is 10Kbps to 100Gbps.</li> <li>• <b>Forward to</b>—Use this option to configure the routing next hop to forward the packets for scrubbing.</li> </ul>
Scrubbing Site	Specify a routing instance to which packets are forwarded in the <i>as-number:community-value</i> format, where each value is a decimal number. For example, 65001:100.

Once you have a threat prevention policy, you assign one or more groups to it:

1. In the threat prevention policy main page (located under **Configure > Threat Prevention > Policy**), find the appropriate policy.
2. In the Groups column, click the **Assign to Groups** link that appears here when there are no policy enforcement groups assigned or click the group name that appears in this column to edit the existing list of assigned groups. You can also select the check box beside a policy and click the **Assign to Groups** button at the top of the page. See [“Policy Enforcement Groups Overview” on page 146](#).
3. In the Assign to Groups page, select the check box beside a group in the Available list and click the > icon to move it to the Selected list. The groups in the Selected list will be assigned to the policy.
4. Click **OK**.
5. Once one or more policy enforcement groups have been assigned, a **Ready to Update** link appears in the Status column. You must update to apply your new or edited policy configuration. Clicking the Ready to Update link takes you the Threat Policy Analysis page. See [“Threat Policy Analysis Overview” on page 157](#). From there you can view your changes and choose to Update now, Update later, or Save them in draft form without updating.
6. If you are using Sky ATP without Policy Enforcer, you must assign your threat prevention policy to a firewall rule for it to take affect. Navigate to **Configure > Firewall Policy > Policies**. In the Advanced Security column, click an item to access the Edit Advanced Security page and select the threat prevention policy from the **Threat Prevention** pulldown list.

## RELATED DOCUMENTATION



Comparing the SDSN and non-SDSN Configuration Steps	38
Creating Policy Enforcement Groups	147
Threat Policy Analysis Overview	157
Creating Geo IP Policies	158
Threat Prevention Policy Overview	149
Policy Enforcer Overview	17
Benefits of Policy Enforcer	20
Policy Enforcer Components and Dependencies	26
Sky ATP Overview	22

# 12

CHAPTER

## Threat Prevention - Configure

---

[Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 204](#)

[Sky ATP Realm Overview | 206](#)

[Modifying Sky ATP Realm | 207](#)

[Custom Feed Sources Overview | 209](#)

[Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist | 210](#)

[Example: Creating a Dynamic Address Custom Feed and Firewall Policy | 215](#)

[Creating Custom Feeds, Infected Host | 217](#)

[Creating Custom Feeds, DDoS | 220](#)

[Configuring TTL Settings for Custom Feeds | 223](#)

[Sky ATP Email Management Overview | 224](#)

[Sky ATP Email Management: SMTP Settings | 226](#)

[Sky ATP Email Management: Allowlist and Blocklists | 229](#)

[Email Management: Configure IMAP | 230](#)

[Sky ATP Malware Management Overview | 233](#)

[File Inspection Profiles Overview | 233](#)

Creating File Inspection Profiles | **235**

Creating Allowlist and Blocklists | **236**

Implementing Threat Policy on VMWare NSX | **238**

---

# Creating Sky ATP Realms and Enrolling Devices or Associating Sites

To access this page, click **Configure>Threat Prevention>Sky ATP Realms**.

You can create Sky ATP realms from the Sky ATP page.

- Understand which type of Sky ATP license you have: free, basic, or premium. The license controls which Sky ATP features are available.
- To configure a Sky ATP realm, you must already have a Sky ATP account with an associated license.
- Ensure that the internet connectivity is available for Policy Enforcer. Without the internet connectivity, you cannot create a realm.
- Decide which region will be covered by the realm you are creating. You must select a region when you configure a realm.
- Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Sky ATP or Policy Enforcer configuration.

To configure a Sky ATP Realm:

1. Select **Configure>Threat Prevention>Sky ATP Realms**.
2. Click the + icon.
3. Complete the initial configuration by using the guidelines in [Table 19 on page 139](#) below.

**Table 53: Fields on the Add Sky ATP Realm Page**

Field	Description
Location	<p>Select a region of the world from the available choices.</p> <p>The following options are available in the Location list:</p> <ul style="list-style-type: none"> <li>• North America</li> <li>• European Region</li> <li>• Canada</li> <li>• Asia Pacific</li> </ul> <p>By default, the North America value appears in the list. To know more about the geographic region, see <a href="#">here</a>.</p>
Username	Enter your e-mail address. Your username for Sky ATP is your e-mail address.

Table 53: Fields on the Add Sky ATP Realm Page (*continued*)

Field	Description
Password	Enter a unique string at least 8 characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character (~!@#\$%^&*()_+={}[] ;:<>./?); no spaces are allowed, and you cannot use the same sequence of characters that are in your username.
Realm	<p>Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed.</p> <p><b>NOTE:</b> When you create a custom feed with a realm, the feed is associated at the site level and not at the realm level. If you modify this realm and associate new sites to it, a warning message is shown that there are custom feeds are associated with this realm. Changing the site information will change the custom feed information. You must go and edit the custom feed that was associated with this realm and verify the realm association.</p>

- Click **Next** and guided setup walks you through the steps for enrolling devices into the realm and associating sites for Policy Enforcer.

The next steps include the following:

- If you are using Sky ATP with PE and you have no devices in enrolled in the realm, you are asked to select devices in the box on the left and move them to the right to enroll them. All selected devices are automatically enrolled with Sky ATP when you finish guided setup. To disenroll a device, you can edit a realm and move the device back to the left side box.

**NOTE:** Note that adding a device to a realm results in one or more commit operations occurring on the device to apply the Sky ATP or Policy Enforcer configuration.

- Next you select a Site from the list to contain the devices. If there are no sites associated with the realm, click **Create new site**. See [“Creating Secure Fabric and Sites” on page 144](#).

**NOTE:** If you are using Sky ATP without PE, you are not prompted to select a site.

- Once the devices and site are selected, you use the sidebar to choose a threshold level at which selected administrators are notified via email about infected host events. Click the+ sign if you want to add new administrators to the list.

- 8. Finally, you select one or more check boxes for event types you want to log.
- 9. Click **Finish**.

**NOTE:** If you enrolled a device into a realm from within Security Director and you want to disenroll it, you must do that from within Security Director. If you enrolled a device into a realm from within Sky ATP and you want to disenroll it, you must do that from within Sky ATP. You cannot disenroll a device from within Security Directory that was enrolled from within Sky ATP.

RELATED DOCUMENTATION

<a href="#">Sky ATP Realm Overview   163</a>
<a href="#">Using Guided Setup for Sky ATP   128</a>
<a href="#">Creating Secure Fabric and Sites   144</a>

# Sky ATP Realm Overview

A security realm is a group identifier for an organization used to restrict access to Web applications. You must create at least one security realm to login into Sky ATP. Once you create a realm, you can enroll SRX Series devices into the realm. You can also give more users (administrators) permission to access the realm.

If you have multiple security realms, note that each SRX Series device can only be bound to one realm, and users cannot travel between realms.

[Table 31 on page 163](#) provides the guidelines on using the fields on the Sky ATP Realm page.

Table 54: Fields on the Sky ATP Realm Page

Field	Description
Realm	Specifies the name of a realm.
Sites	Specifies the site name associated to the realm.
Location	Specifies the region of the realm.
Devices	Specifies the perimeter firewall devices that are enrolled to Sky ATP.

Table 54: Fields on the Sky ATP Realm Page (*continued*)

Field	Description
Enrollment Status	Specifies the enrollment status of the realm.

## RELATED DOCUMENTATION

[Creating Sky ATP Realms and Enrolling Devices or Associating Sites | 138](#)

[Using Guided Setup for Sky ATP | 128](#)

[skyConfiguring Sky ATP \(No SDSN and No Guided Setup\) Overview | 162](#)

## Modifying Sky ATP Realm

Use the Modify Sky ATP Realm page to modify the site information and global configuration information of an existing Sky ATP realm. You can also view devices from the realm that are not managed by Security Director.

In the Global Configuration section, you can add trusted proxy server IP addresses to Sky ATP. When there is a proxy server between users on the network and a firewall, the firewall might see the proxy server IP address as the source of an HTTP or HTTPS request instead of the actual address of the user making the request.

With this in mind, X-Forwarded-For (XFF) is a standard header added to packets by a proxy server that includes the real IP address of the client making the request. Therefore, if you add trusted proxy servers IP addresses to the list in Sky ATP, by matching this list with the IP addresses in the HTTP header (X-Forwarded-For field) for requests sent from the SRX Series devices, Sky ATP can determine the originating IP address.

**NOTE:** X-Forwarded-For (XFF) only applies to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header.

To modify a Sky ATP realm:

1. Select **Configure** > **Threat Prevention** > **Sky ATP Realms**.

The Sky ATP Realms page appears.

2. Select the realm and click the pencil icon to modify the configuration.

The Modify Sky ATP Realm page appears.

3. Complete the configuration by using the guidelines in [Table 55 on page 208](#).

4. Click **Finish** to complete the configuration or **Cancel** to discard the changes.

**NOTE:** Assigning a site to the realm will cause a change in the device configuration in the associated devices.

**Table 55: Fields on the Modify Sky ATP Realm page**

Field	Description
<i>Site</i>	
Site	Select a site to enroll into the realm. If there are no sites associated with the realm, click <b>Create new site</b> .
Unmanaged Devices	Lists all devices from the realm that are not managed in Security Director. You must manually discover them.
<i>Global Configuration</i>	
Threat Level Threshold	Select a threshold level to block the infected hosts and to send an e-mail to the selected administrators notifying about the infected host events.
Logging	Enable logging for the Malware or the Host Status event.
Proxy Servers	Click the add icon (+) to enter the IPv4 address of the proxy server, in the Server IP column.  You can also edit the existing IP address or delete them.



## RELATED DOCUMENTATION

# Custom Feed Sources Overview

Policy Enforcer uses threat feeds to provide actionable intelligence to policies about various types of threats. These feeds can come from different sources, such as Sky ATP, and from lists that you can customize by adding IP addresses, domains, and URLs.

**NOTE:** Sky ATP feeds and custom feeds are mutually exclusive. You can only have one source for allowlist, blocklist, and infected host feeds.

The following types of custom threat feeds are available:

- A dynamic address is a group of IP addresses that can be imported from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. You can then configure security policies to use the dynamic addresses within a security policy.
- An allowlist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the allowlist does not have to be inspected for malware.
- A blocklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.
- Infected hosts are hosts known to be compromised.

For threat management policies to use these feeds, you must enter configuration information for each feed type.

## Benefits of Custom Feed Sources

- Provides relevant and timely intelligence that you can use to create enforcement policies. Enables you to customize threat feeds specific to your industry or organization.
- Provides flexible mechanisms to synchronize threat information to:
  - Configure Policy Enforcer to poll from local file and remote file custom feeds.
  - Push threat feeds to Policy Enforcer using the Threat Feed API .

## RELATED DOCUMENTATION

---

[Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist | 184](#)


---

[Creating Custom Feeds, Infected Host | 189](#)


---

[Example: Creating a Dynamic Address Custom Feed and Firewall Policy | 215](#)


---

## Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist

To access this page, click **Configure>Threat Prevention>Custom Feeds**.

You can create custom feeds from the custom feeds page.

- Know what type of feed you are configuring and have all the necessary information on hand. Local feeds are created on your local system and uploaded from there.
- To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show Dynamic Addresses.
- For creating an Infected Host custom feed, see [“Creating Custom Feeds, Infected Host” on page 189](#).  
For creating a DDoS custom feed, see [“Creating Custom Feeds, DDoS” on page 220](#).

To create local file and remote file custom feeds:

1. Select **Configure>Threat Prevention>Custom Feeds**.
2. Select one of the following feed types.

**Table 56: Custom Feed Categories**

Feed Category	Definition
Dynamic Address	<p>A dynamic address entry provides dynamic IP address information to security policies. A dynamic address is a group of IP addresses, not just a single IP prefix, that can be imported from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. You can then configure security policies to use the dynamic addresses within a security policy.</p> <p>You can use custom feeds while configuring the firewall policy. For information on how to create dynamic addresses, see: <a href="#">Creating Dynamic Address Groups</a>.</p> <p><b>NOTE:</b> You can create multiple custom feeds for all types of feed categories.</p>

Table 56: Custom Feed Categories (*continued*)

Feed Category	Definition
Allowlist	An allowlist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the allowlist does not have to be inspected for malware.
Blocklist	A blocklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.
Infected Host	Infected hosts are hosts known to be compromised. Enter host IP addresses manually or upload a text file with the IP addresses of infected hosts. See <a href="#">“Creating Custom Feeds, Infected Host” on page 189</a> for configuration details.
DDoS	Using DDoS threat feed, policy Enforcer blocks source IP addresses in the feed, rate limit the traffic from the source IP addresses, and takes BGP Flowspec action to blackhole or redirect the traffic to scrubbing centers. See <a href="#">“Creating Custom Feeds, DDoS” on page 220</a> and <a href="#">“Creating Threat Prevention Policies” on page 151</a> .

**NOTE:**

- The Remote Download Status field shows the status of downloading feeds from a remote file server to Policy Enforcer. This field will be blank if the locally created custom feeds.

The following statuses are shown under different scenarios:

- Pending—Status is shown as pending until Policy Enforcer downloads the new feeds from the remote file server.
- Success—Status is shown as success when Policy Enforcer downloads the feeds successfully.
- Failed—Status is shown as failed when downloading the feeds fails.
- The Days to Become Inactive field shows the number of days within which the custom feed is going to expire or become inactive. You must specify the number of days for each custom feed to be active in the Time to Live (TTL) Settings page. Whenever you make any update to a feed type in the TTL Settings page, number of days to expire is counted from that date. See [“Configuring TTL Settings for Custom Feeds” on page 223](#).

Once the Days to Become Inactive field is zero, the respective feed will become inactive and cannot be used. You must update the feed again to make it active.

3. Click **Create** and select one of the following:
  - **Feeds with local files**—This is data you enter manually into the provided fields or upload from a text file on your location machine. See [Table 43 on page 187](#) for details.
  - **Feeds with remote file server**—This is a data feed from a remote server. Configure communication with the remote server using instructions in [Table 44 on page 188](#).
4. Complete the configuration by using the guidelines in [Table 43 on page 187](#) or [Table 44 on page 188](#).
5. Click **OK**. Your entry is added to custom list displayed at the bottom of the page.

**NOTE:** To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show Dynamic Addresses.

If there is a firewall policy rule created using the dynamic address, you cannot delete the same dynamic address from the Custom Feeds page. You must first delete the firewall policy rule and then , delete the dynamic address from the Custom Feeds page.

Use the fields in [Table 43 on page 187](#) to add custom feeds.

**Table 57: Fields on the Custom Feeds Page, Feeds with Local Files**

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description for your custom feed; maximum length is 64 characters. You should make this description as useful as possible for all administrators.
Feed Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>IP, Subnet and Range</b>—Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</li> <li>• <b>URL and Domain</b>—Enter the URL using the following format: http://yourfeed.com/abc and Domain using the following format: http://yourfeed.com. Wildcards and protocols are not valid entries.</li> </ul> <p><b>NOTE:</b> For Dynamic Address, you can only select IP, Subnet, and Range. For Blocklists and Allowlist, all feed types are available for selection.</p>

Table 57: Fields on the Custom Feeds Page, Feeds with Local Files (*continued*)

Field	Description
Sites	<p>Select the required sites from the list to associate them with the dynamic address or allowlists and blocklists feeds.</p> <p>In the default mode (no Sky ATP), only sites are listed because of no Sky ATP. The same site can be shared across dynamic address, allowlists, and blocklists feeds.</p>
Realms	<p>Select the required realms from the list, if you are in Cloud feeds only, Sky ATP, or Sky ATP with SDSN mode.</p> <p>Associate these realms with dynamic address or allowlists and blocklists feeds. The same realm can be shared across dynamic address, allowlists and blocklists feeds.</p> <p>When you are creating a Sky ATP realm, if you do not assign any sites to it, those realms are not listed here. Only realms with sites associated are listed here.</p>
Custom List	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Click <b>Upload File</b> to upload a text file with an IP address list. Click the <b>Add</b> button to include the address list in your custom list.</li> </ul> <p>Note that the file must contain only one item per line (no commas or semi colons). All items are validated before being added to the custom list.</p> <p>The file must not contain more than 500 entries. An error message is shown if you try to upload a file containing more than 500 IP addresses. Use the Feeds with remote file server option to upload a file containing more than 500 IP addresses.</p> <ul style="list-style-type: none"> <li>Manually enter your item in the space provided in the Custom List section. To add more items, click + to add more spaces.</li> </ul>

Table 58: Fields on the Custom Feeds Page, Feeds with Remote File Server

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include only dashes and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description for your custom feed; maximum length is 64 characters. You should make this description as useful as possible for all administrators.

Table 58: Fields on the Custom Feeds Page, Feeds with Remote File Server (*continued*)

Field	Description
Feed Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• IP, Subnet and Range—Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</li> <li>• URL and Domain—Enter the URL using the following format: http://yourfeed.com/abc and Domain using the following format: http://yourfeed.com. Wildcards and protocols are not valid entries.</li> </ul> <p><b>NOTE:</b> For Dynamic Address, you can only enter IP, Subnet, and Range. For Blocklists and Allowlist, all feed types are available for selection.</p>
Type of Server URL	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• http</li> <li>• https</li> </ul>
Server File URL	Enter the URL for the remote file server.
Certificate Upload	<p>Click <b>Browse</b> and select the CA certificate to upload.</p> <p>If you do not upload a certificate for https server URL, a warning message is shown that a certificate is not uploaded and to whether proceed further or not. Click <b>Yes</b> to proceed further without uploading a certificate or <b>No</b> to go back and upload the certificate.</p>
Username	<p>Enter the credentials for the remote file server.</p> <p>This is not a mandatory field. You can still proceed to create a custom feed without entering the username.</p>
Password	<p>Enter the credentials for the remote file server.</p> <p>This is a mandatory field, if you have provided the username.</p>
Update Interval	Select how often updates are retrieved from the remote files server: Hourly, Daily, Weekly, Monthly, Never

## RELATED DOCUMENTATION

[Example: Creating a Dynamic Address Custom Feed and Firewall Policy | 215](#)
[Creating Custom Feeds, Infected Host | 189](#)

## Example: Creating a Dynamic Address Custom Feed and Firewall Policy

As stated earlier, dynamic addresses provide dynamic IP address information to security policies. A dynamic address entry (DAE) is a group of IP addresses, not just a single IP prefix, that can be entered manually or imported from external sources. The DAE feature allows feed-based IP objects to be used in security policies to either deny or allow traffic based on either source or destination IP criteria. For example, a DAE may contain IP addresses for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. When the DAE is updated, the changes automatically become part of the security policy. There is no need to manually update the policy; no configuration commit action is required.

This topic steps you through a simple example of creating a DAE and associating it with a policy. For complete information in creating firewall policies in Security Director, see [Creating Firewall Policies](#). This example is based on Security Director 17.1R1.

1. Click **Configure>Threat Prevention>Custom Feeds**.
2. Click the Dynamic Address tab if it is not already selected, and click **Create > Feeds with local files**.
3. Enter **DAE\_example1** as the name.
4. Click the plus sign (+) to add individual entries to the custom list.
5. Add the following IP addresses. See the online help for information on supported formats.
  - 192.0.2.0
  - 192.0.2.1/10
  - 198.51.100.0-198.51.100.5
6. Make sure all entries in the custom list are unchecked and click **OK**.

**NOTE:** If you have an entry selected, an error message will prompt you to uncheck the item prior to clicking OK.

7. Click **Configure > Firewall Policies > Policies**.

**NOTE:** This example uses simplistic rules to show how to associate a DAE with an allowlist firewall policy. When creating your own firewall policy, you will have to configure the rules that meet your company's requirements.

8. Click the plus sign (+) to create a new firewall policy.

9. Enter **dynamic\_address\_test** as the name.

10. Select **All Logging Enabled** from the Profile pull-down menu.

11. Select **Device Policy** as the Type and select a device from the Device pull-down menu.

12. Click **OK**.

After a few seconds, the **dynamic\_address\_test** policy appears in the list.

13. Click **Add Rule** next to the **dynamic\_address\_test** policy to start the rule wizard.

14. Enter **dynamic\_rule** as the name and click **Next**.

15. In the Source window, select **untrust** from the Zone pulldown menu and click **Select** under the Address(es) field.

16. In the Source Address window, select the **Include Specific** radio button.

17. Select **DAE\_example1** in the left table and click the right arrow to move it to the right table. Then click **Next**.

The Source window reappears and **DAE\_example1** appears in the address(es) field.

18. In the Destination window, select **trust** from the Zone pulldown menu and click **Next**.

19. In the Advanced Security window, select **permit** from the Rule Action pulldown menu and click **Next**.

20. In the Rule Options window, click **Next** to use the default settings.

21. Click **Select** in the Address(es) section and click the **Include Specifics** radio button.



22. In the Rule Analysis window, select the **Analyze the new rule to suggest a placement to avoid anomalies** checkbox and click **Next**.

After a few seconds, an analysis of your rule appears, including where it should be placed, etc.

23. Click **Finish** and then **OK** to exit the wizard.

24. In the resulting page, click **Save** (located near the top of the window.)

25. Check the checkbox for the **dynamic\_rule** policy and click **Publish**.

When you publish rules, the process takes into account the priority and precedence values set on the policy and the order of rules on the device.

## Creating Custom Feeds, Infected Host

To access this page, click **Configure>Threat Prevention>Custom Feeds**.

- Note that infected hosts are hosts known to be compromised. For an infected host custom feed, enter host IP addresses manually or upload a text file with the IP addresses of infected hosts.
- If you create a custom infected hosts feed, it will override the SKY ATP infected hosts feed.
- To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show custom feed types, including infected hosts.
- Note that when Sky ATP only mode is selected as the Threat Prevention Type, the infected host custom feed is not available.
- For creating other custom feed types, see [“Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist”](#) on page 184.



**WARNING:** When you have no Sky ATP Configuration Type selected (No selection), Sky ATP realms are disabled. Because site selection is usually done from the Sky ATP realm page, you must select sites from the Custom Feed - Infected Hosts page when in “No selection” mode. The custom feeds are then downloaded to the devices in the chosen sites. This is the only time site selection is available in the Custom Feeds - Infected Hosts page.

To create local file and remote file custom feeds:

1. Select **Configure>Threat Prevention>Custom Feeds**.
2. Select the **Infected Host** tab.

**NOTE:** When Sky ATP only is selected as the Threat Prevention Type, the infected host custom feed is not available.

3. Click **Create** and select one of the following:
  - **Feeds with local files**—This is data you enter manually into the provided fields or upload from a text file on your location machine. See [Table 43 on page 187](#) for details.
  - **Feeds with remote file server**—This is a data feed from a remote server. Configure communication with the remote server using instructions in [Table 44 on page 188](#).
4. Complete the configuration by using the guidelines in [Table 43 on page 187](#) or [Table 44 on page 188](#).
5. Click **OK**. Your entry is added to custom list displayed at the bottom of the page.

**NOTE:** To use a custom feed, apply it to the source or destination address in a firewall rule. In the firewall rule, you can filter addresses to show Infected Hosts, Dynamic Addresses, Allowlist and Blocklists.

Use the fields in [Table 43 on page 187](#) to add custom feeds.

**Table 59: Fields on the Custom Feeds Page, Feeds with Local Files**

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
Description	Enter a description for your custom feed; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.
Sites	Select the required sites from the list to associate them with the infected feeds.  In the default mode (no Sky ATP), only sites are listed because of no Sky ATP. You cannot share the same site across the same feed type. However, you can share a site across different feed types.

Table 59: Fields on the Custom Feeds Page, Feeds with Local Files (*continued*)

Field	Description
Realms	<p>Select the required realms from the list, if you are in Cloud feeds only, or SDSN with Sky ATP only mode and associate them with dynamic address or allowlists and blocklists feeds.</p> <p>You cannot share the same realm across the same feed type. However, you can share a realm across different feed types.</p> <p>When you are creating a Sky ATP realm, if you do not assign any sites it, those realms are not listed here. Only realms with sites associated are listed here.</p>
Custom List	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Click <b>Upload File</b> to upload a text file with an IP address list. The uploading file must have the string <i>add</i> at the beginning, followed by the IP addresses. If you want to delete certain IP addresses, enter the string <i>delete</i> followed by the IP addresses to delete.</li> </ul> <p>Click the <b>Add</b> button to include the address list in your custom list.</p> <p>Note that the file must contain only one item per line (no commas or semi colons). All items are validated before being added to the custom list.</p> <ul style="list-style-type: none"> <li>Manually enter your item in the space provided in the Custom List section. To add more items, click <b>+</b> to add more spaces.</li> </ul> <p>For syntax, enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</p>

Table 60: Fields on the Custom Feeds Page, Feeds with Remote File Server

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
Description	Enter a description for your custom feed; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.
Type of Server URL	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>http</li> <li>https</li> </ul>
Server File URL	Enter the URL for the remote file server.

Table 60: Fields on the Custom Feeds Page, Feeds with Remote File Server (*continued*)

Field	Description
Certificate Upload	Click <b>Browse</b> and select the CA certificate to upload.  If you do not upload a certificate for https server URL, a warning message is shown that a certificate is not uploaded and to whether proceed further or not. Click <b>Yes</b> to proceed further without uploading a certificate or <b>No</b> to go back and upload the certificate.
Username	Enter the credentials for the remote file server.
Password	Enter the credentials for the remote file server.
Update Interval	Select how often updates are retrieved from the remote files server: Hourly, Daily, Weekly, Monthly, Never

You can create only a single infected host. If you want to create one more infected host, you must first delete the existing feed and create a new one.

If you try to disenroll a site in an infected host, a warning message is shown to resolve all the current infected hosts from the respective endpoints within a site. To resolve the infected hosts, log-in to Sky ATP UI, resolve the hosts, and then unassign sites from Policy Enforcer. Ensure that you always resolve the infected hosts before unassigning sites. Once you unassign sites, you cannot resolve the hosts.

## RELATED DOCUMENTATION

[Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist | 184](#)

[Custom Feed Sources Overview | 209](#)

[Sky ATP Realm Overview | 163](#)

# Creating Custom Feeds, DDoS

To access this page, select **Configure > Threat Prevention > Custom Feeds**.

To create local file and remote file custom feeds:

1. Select **Configure > Threat Prevention > Custom Feeds**.
2. Select the **DDoS** tab.

**NOTE:** When Sky ATP only is selected as the Threat Prevention Type, the DDoS custom feed is not available.

3. Click the Create icon and select one of the following options:

- Feeds with local files—Enter the data manually into the provided fields or upload from a text file on your location machine. Complete the configuration as per the guidelines provided in [Table 61 on page 221](#).
- Feeds with remote file server—Feeds are fetched from a remote server. Complete the configuration as per the guidelines provided in [Table 62 on page 222](#).

4. Click **OK**.

DDoS feed is updated. You can create only one DDoS feed, but add any number of IP addresses to the custom list.

**Table 61: Fields on the Feeds with Local File Page**

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum.
Description	Enter a description for your custom feed; maximum length is 1,024 characters. You must make this description as useful as possible for all administrators.
Sites	<p>Select the required sites from the list to associate them with the DDoS feeds.</p> <p>In the default mode (no Sky ATP), only sites are listed because of no Sky ATP. You cannot share the same site across the same feed. However, you can share a site across different feed types.</p>
Realms	<p>Select the required realms from the list, if you are in Cloud feeds only, or SDSN with Sky ATP only mode and associate them with dynamic address or allowlists and blocklists feeds.</p> <p>You cannot share the same realm across the same feed type. However, you can share a realm across different feed types.</p> <p>When you are creating a Sky ATP realm, if you do not assign any sites it, those realms are not listed here. Only realms with sites associated are listed here.</p>

Table 61: Fields on the Feeds with Local File Page (*continued*)

Field	Description
Custom List	<p>Add all the target IP addresses that are supposed to be blocked. You can add only IP addresses and not IP subnets.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Click <b>Upload File</b> to upload a text file with an IP address list. The uploading file must have the string <i>add</i> at the beginning, followed by the IP addresses. If you want to delete certain IP addresses, enter the string <i>delete</i> followed by the IP addresses to delete.</li> </ul> <p>Click the <b>Add</b> button to include the address list in your custom list.</p> <p>The file must contain only one item per line (no commas or semi colons). All items are validated before being added to the custom list.</p> <ul style="list-style-type: none"> <li>Manually enter your item in the space provided in the Custom List section. To add more items, click the add icon (+) to add more IP addresses.</li> </ul>

Table 62: Fields on the Feeds with Remote File Server Page

Field	Description
Name	Enter a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 32-character maximum.
Description	Enter a description for your custom feed; maximum length is 1,024 characters. You must make this description as useful as possible for all administrators.
Feed Type	<p>Select one of the following feed types for the DDoS feed category.</p> <ul style="list-style-type: none"> <li>IP, Subnet and Range—Enter an IPV4 address in standard four octet format.</li> </ul>
Types of Server URL	<p>Select one of the following type to access the remove file server:</p> <ul style="list-style-type: none"> <li>http</li> <li>https</li> </ul>
Server File URL	Enter the URL for the remote file server.
Certificate Upload	<p>Click <b>Browse</b> and select the CA certificate to upload.</p> <p>If you do not upload a certificate for https server URL, a warning message is shown that a certificate is not uploaded and to whether proceed further or not. Click <b>Yes</b> to proceed further without uploading a certificate or <b>No</b> to go back and upload the certificate.</p>
Username	Enter the username for the remote file server.
Password	Enter the password for the remote file server.

Table 62: Fields on the Feeds with Remote File Server Page (*continued*)

Field	Description
Update Interval	Select how often updates are retrieved from the remote files server: Hourly, Daily, Weekly, Monthly, Never.

## RELATED DOCUMENTATION

[Custom Feed Sources Overview | 209](#)
[Creating Threat Prevention Policies | 151](#)

## Configuring TTL Settings for Custom Feeds

To access this page, click **Configure>Threat Prevention>Custom Feeds**.

Use the Time to Live (TTL) Settings page to specify the number of days for the custom feed to be active.

In the Sky ATP with SDSN, Clouds feed only, and No Sky ATP modes, you can configure the TTL settings for dynamic address, allowlist, blocklist, infected host, and DDoS feed types. In the Sky ATP mode, you can configure TTL settings for only dynamic address, allowlist, and blocklist feed types.

**NOTE:** When you configure a TTL setting for a particular feed type, the configuration is applicable for all the custom feeds belonging to that particular feed type. For example, if you set TTL for Allowlist feed type to 45 days, then all Allowlist feeds will have the same configuration.

To configure TTL Settings:

1. Select **Configure>Threat Prevention>Custom Feeds**.

2. Select the **TTL Settings** tab.

The Time To live Settings page appears.

3. Complete the configuration by using the guidelines in [Table 63 on page 224](#).

4. Click **Update**.

The TTL settings are updated and a success message is shown that the TTL Settings are updated successfully. Click **Reset** to reset the settings to the last known stable configuration.

At the beginning of the TTL Settings page, the last updated TTL settings information is shown. This message is refreshed whenever you update a new TTL setting.

**Table 63: Fields on the TTL Settings Page**

Option	Description
Specify Manually	Select this option to specify the number of days for the required custom feed type to be active.
Never Expire	Select this option if you do not want any custom feed type to be inactive or expire.
Expires in (days)	<p>This field is available only if you select the Specify Manually option.</p> <p>Specify the number of days for the required custom feed to be active. The available range is 1 to 365 days.</p> <p>The number of days that you configure in this field appears in the Days to Become Inactive field on each custom feed page. If you make any changes to this field, the same information is refreshed in the Days to Become Inactive field and the timer is adjusted to the updated value.</p>

## RELATED DOCUMENTATION

[Custom Feed Sources Overview | 209](#)

[Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist | 184](#)

[Creating Custom Feeds, Infected Host | 189](#)

[Creating Custom Feeds, DDoS | 220](#)

# Sky ATP Email Management Overview

With Email Management, enrolled devices transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Sky ATP assigns the file a threat score between 0-10 with 10 being the most malicious.

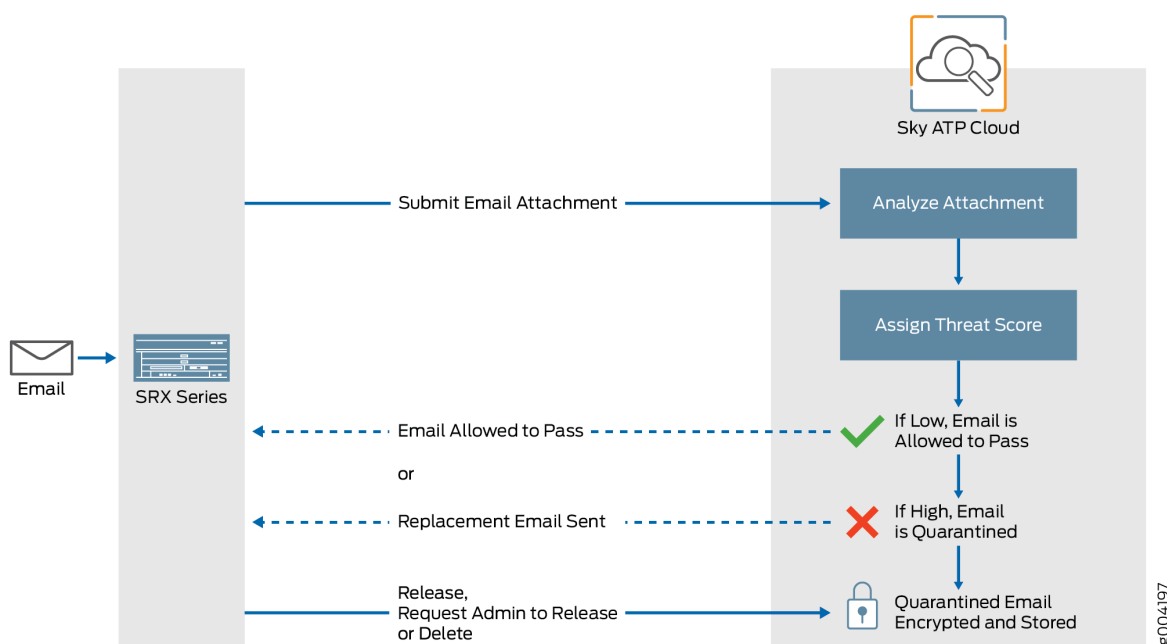


**NOTE:** If an email contains no attachments, it is allowed to pass without any analysis.

Configure one of the following actions when an email attachment is determined to be malicious:

- **Quarantine Malicious Messages**—If you select to quarantine emails with attachments found to be malicious, those emails are stored in the cloud in an encrypted form and a replacement email is sent to the intended recipient. That replacement email informs the recipient of the quarantined message and provides a link to the Sky ATP quarantine portal where the email can be previewed. The recipient can then choose to release the email by clicking a Release button (or request that the administrator release it) or Delete the email.
- **Deliver malicious messages with warning headers added**—When you select this option, headers are added to emails that most mail servers recognize and filter into Spam or Junk folders.
- **Permit**—You can select to permit the email and the recipient receives it intact.

**Figure 56: Email Management Overview**



### Quarantine Release

If the recipient selects to release a quarantined email, it is allowed to pass through the SRX series with a header message that prevents it from being quarantined again, but the attachments are placed in a password-protected ZIP file. The password required to open the ZIP file is also included as a separate

attachment. The administrator is notified when the recipient takes an action on the email (either to release or delete it).

If you configure Sky ATP to have the recipient send a request to the administrator to release the email, the recipient previews the email in the Sky ATP quarantine portal and can select to Delete the email or Request to Release. The recipient receives a message when the administrator takes action (either to release or delete the email.)

### Blocklist and Allowlist

Emails are checked against administrator-configured blocklists and allowlists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches the allowlist, that email is allowed through without any scanning. If an email matches the blocklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

### RELATED DOCUMENTATION

[Sky ATP Email Management: SMTP Settings | 226](#)

[Sky ATP Email Management: Allowlist and Blocklists | 229](#)

## Sky ATP Email Management: SMTP Settings

Use the this page to inspect and manage email attachments sent over SMTP.

- Read the “[Sky ATP Email Management Overview](#)” on [page 224](#) topic.
  - Decide how malicious emails are handled: quarantined, delivered with headers, or permitted.
1. Select **Configure > Threat Prevention > Sky ATP Email Management** and choose the **SMTP Settings** tab.
  2. Select a Sky ATP Realm and click the pencil icon to configure email management settings for that realm.
  3. Based on your selections, configuration options will vary. See the tables below.

Table 64: Configure Quarantine Malicious Messages

Setting	Guideline
Action to take	Quarantine malicious messages (the default)—When you select to quarantine malicious email messages, in place of the original email, intended recipients receive a custom email you configure with information on the quarantining. Both the original email and the attachment are stored in the cloud in an encrypted format.
Release option	<ul style="list-style-type: none"> <li>Recipients can release email—This option provides recipients with a link to the Sky ATP quarantine portal where they can preview the email. From the portal, recipients can select to <b>Release</b> the email or <b>Delete</b> it. Either action causes a message to be sent to the administrator.  <b>NOTE:</b> If a quarantined email has multiple recipients, any individual recipient can release the email from the portal and all recipients will receive it. Similarly, if one recipient deletes the email from the portal, it is deleted for all recipients.</li> <li>Recipients can request administrator to release email—This option also provides recipients with a link to the Sky ATP quarantine portal where they can preview the email. From the portal, recipients can select to <b>Request to Release</b> the email or <b>Delete</b> it. Either choice causes a message to be sent to the administrator. When the administrator takes action on the email, a message is sent to the recipient.  <b>NOTE:</b> When a quarantined email is released, it is allowed to pass through the SRX series with a header message that prevents it from being quarantined again, but the attachment is placed inside a password-protected zip file with a text file containing the password that the recipient must use to open the file.</li> </ul>
<i>Email Notifications for End Users</i>	
Learn More Link URL	If you have a corporate web site with further information for users, enter that URL here. If you leave this field blank, this option will not appear to the end user.
Subject	When an email is quarantined, the recipient receives a custom message informing them of their quarantined email. For this custom message, enter a subject indicating a suspicious email sent to them has been quarantined, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.

Table 64: Configure Quarantine Malicious Messages (*continued*)

Setting	Guideline
Custom Link Text	Enter custom text for the Sky ATP quarantine portal link where recipients can preview quarantined emails and take action on them.
Buttons	<ul style="list-style-type: none"> <li>• Click <b>Preview</b> to view the custom message that will be sent to a recipient when an email is quarantined. Then click <b>Save</b>.</li> <li>• Click <b>Reset</b> to clear all fields without saving.</li> <li>• Click <b>Save</b> if you are satisfied with the configuration.</li> </ul>

Table 65: Configure Deliver with Warning Headers

Setting	Guideline
Action to take	Deliver malicious messages with warning headers added—When you select to deliver a suspicious email with warning headers, you can add headers to emails that most mail servers will recognize and filter into spam or junk folders.
SMTP Headers	<ul style="list-style-type: none"> <li>• X-Distribution (Bulk, Spam)—Use this header for messages that are sent to a large distribution list and are most likely spam. You can also select “Do not add this header.”</li> <li>• X-Spam-Flag—This is a common header added to incoming emails that are possibly spam and should be redirected into spam or junk folders. You can also select “Do not add this header.”</li> <li>• Subject Prefix—You can prepend headers with information for the recipient, such as “Possible Spam.”</li> </ul>
Buttons	<ul style="list-style-type: none"> <li>• Click <b>Reset</b> to clear all fields without saving.</li> <li>• Click <b>OK</b> if you are satisfied with the configuration.</li> </ul>

Table 66: Permit

Setting	Guideline
Action to take	Permit—You can select to permit the message and no further configuration is required.

### Administrators Who Receive Notifications

To send notifications to administrators when emails are quarantined or released from quarantine:

1. Click the + sign to add an administrator.
2. Enter the administrator's email address.
3. Select the **Quarantine Notification** check box to receive those notifications.
4. Select the **Release Notifications** check box to receive those notifications.
5. Click **OK**.

### RELATED DOCUMENTATION

[Sky ATP Email Management Overview | 224](#)

[Sky ATP Email Management: Allowlist and Blocklists | 229](#)

## Sky ATP Email Management: Allowlist and Blocklists

Access this page from **Configure > Threat Prevention > Sky ATP Email Management** and choose either the **Whitelist** or **Blacklist** tab.

Use custom blocklists and allowlists to filter email attachments.

- Read the [“Sky ATP Email Management Overview” on page 224](#) topic.
- Compile a list of known malicious email addresses or domains to add to your blocklist. If an email matches the blocklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment, blocked and a replacement email is sent. If an email matches the allowlist, that email is allowed through without any scanning.
- It is worth noting that attackers can easily fake the “From” email address of an email, making blocklists a less effective way to stop malicious emails.

The procedure for adding addresses to blocklists and allowlists is the same, although the results are very different. Be sure you are adding the entry to the correct list.

1. Select **Configure > Threat Prevention > Sky ATP Email Management** and choose either the **Whitelist** or **Blacklist** tab..
2. Select a Sky ATP realm and click the + sign to add a new entry.
3. In the Email Sender field, enter the full address in the format **name@domain.com** or wildcard the name to permit or block all emails from a specific domain. For example, **\*@domain.com**.
4. Click **OK**.

#### RELATED DOCUMENTATION

[Sky ATP Email Management Overview | 224](#)

[Sky ATP Email Management: SMTP Settings | 226](#)

## Email Management: Configure IMAP

To access this page, navigate to **Configure > Threat Prevention > Sky ATP Email Management**.

Use the Sky ATP Email Management page to configure email management for IMAP. With email management for IMAP, enrolled SRX Series devices transparently submit suspicious emails to Sky ATP for inspection and blocking.

### Before You Begin

- Read the [“Sky ATP Email Management Overview” on page 224](#) topic.
- Decide how malicious emails are handled. For IMAP, the available options are to block or permit email. Unlike SMTP, there is no quarantine option for IMAP and no method for previewing a blocked email.

To configure IMAP:

1. Select **Configure > Threat Prevention > Sky ATP Email Management** and choose the **IMAP Settings** tab.
2. Select a Sky ATP Realm and click the pencil icon to configure email management settings for that realm.

3. Complete the configuration as per the guidelines given in [Table 67 on page 231](#).

Based on your selections, configuration options will vary.

**Table 67: Configure Block Malicious Messages**

Setting	Guideline
Action to take	<ul style="list-style-type: none"> <li>Permit download of attachments—Allow email attachments, either from all IMAP servers or specific IMAP servers, through to their destination.  <b>NOTE:</b> In Permit mode, block and allowlists are not checked. Emails from blocklisted addresses are not sent to the cloud for scanning. They are allowed through to the client.</li> <li>Block download of attachments—Block email attachments, either from all IMAP servers or specific IMAP servers, from reaching their destination.  <b>NOTE:</b> In Block mode, block and allowlists are checked. Emails from blocklisted addresses are blocked. Emails from allowlisted addresses are allowed through to the client.</li> </ul> <p>Recipients can send a request to an administrator to release the email. Enter the email address to which recipients should send a release request.</p> <p><b>NOTE:</b> If a blocked email has multiple recipients, any individual recipient can request to release the email and all recipients will receive it.</p> <p>When you select to block email attachments, in place of the original email, intended recipients receive a custom email you configure with information on the block action. Both the original email and the attachment are stored in the cloud in an encrypted format.</p>
IMAP Server	<ul style="list-style-type: none"> <li>All IMAP Servers—The permitting or blocking of email attachments applies to all IMAP servers.</li> <li>Specific IMAP Server—The permitting or blocking of email attachments applies only to IMAP servers with hostnames that you add to a list. A configuration section to add the IMAP server name appears when you select this option.</li> </ul> <p>When you add IMAP servers to the list, it is sent to the SRX Series device to filter emails sent to Sky ATP for scanning. For emails that are sent for scanning, if the returned score is above the set policy threshold on the SRX, then the email is blocked.</p>
IMAP Servers	<p>Select the <b>Specific IMAP Server</b> option above and click the + sign to add IMAP server hostnames to the list.</p> <p><b>NOTE:</b> You must use the IMAP server hostname and not the IP address.</p>

Table 67: Configure Block Malicious Messages (*continued*)

Setting	Guideline
<i>Email Notifications for End Users</i>	
Learn More Link URL	If you have a corporate web site with further information for users, enter that URL here. If you leave this field blank, this option will not appear to the end user.
Subject	When an email is blocked, the recipient receives a custom message informing them of their blocked email. For this custom message, enter a subject indicating a suspicious email sent to them has been blocked, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.
Custom Link Text	Enter custom text for the Sky ATP quarantine portal link where recipients can preview blocked emails and take action on them.
Buttons	<ul style="list-style-type: none"> <li>• Click <b>Preview</b> to view the custom message that will be sent to a recipient when an email is blocked. Then click <b>Save</b>.</li> <li>• Click <b>Reset</b> to clear all fields without saving.</li> <li>• Click <b>Save</b> if you are satisfied with the configuration.</li> </ul>

### Administrators Who Receive Notifications

To send notifications to administrators when emails are blocked or released from quarantine:

1. Click the + sign to add an administrator.
2. Enter the email address of the administrator and click **OK**.
3. Once the administrator is created, you can uncheck or check which notification types the administrator will receive.
  - Block Notifications—If you enable this option, a notification is sent when an email is blocked.
  - Unblock Notifications—If you enable this option, a notification is sent when a user releases a blocked email.

### RELATED DOCUMENTATION



# Sky ATP Malware Management Overview

Malware management includes profiles you can create to group file types together for scanning. It also lets you configure customized allowlists and blocklists.

- File inspection profiles let you define which files to send to the cloud for inspection. By grouping similar file types together to be scanned (such as .tar, .exe, and .java) under a common name, you can create multiple profiles based on the content you want scanned. Then enter the profile names on eligible SRX Series devices to apply them.
- Use the allowlist and blocklist pages to configure custom trusted and untrusted URLs and IPs. Content downloaded from locations on the allowlist is trusted and does not have to be inspected for malware. Hosts cannot download content from locations on the blocklist because those locations are untrusted.

## RELATED DOCUMENTATION

[Creating File Inspection Profiles | 235](#)

[Creating Allowlist and Blocklists | 236](#)

## File Inspection Profiles Overview

File Inspection profiles let you define which files to send to the cloud for inspection. You can group types of files to be scanned together (such as .tar, .exe, and .java) under a common name and create multiple profiles based on the content you want scanned. Then enter the profile names on eligible devices to apply them.

Table 68: File Category Contents

Category	Description
Archive	Archive files
Configuration	Configuration files
Document	All document types except PDFs
Executable	Executable binaries
Java	Java applications, archives, and libraries

Table 68: File Category Contents (*continued*)

Category	Description
Library	Dynamic and static libraries and kernel modules
Mobile	Mobile formats
OS package	OS-specific update applications
PDF	PDF, e-mail, and MBOX files
Rich Application	Installable Internet Applications such as Adobe Flash, JavaFX, Microsoft Silverlight
Script	Scripting files

You can also define the maximum file size requirement per each category to send to the cloud. If a file falls outside of the maximum file size limit the file is automatically downloaded to the client system.

**NOTE:** Once the profile is created, use the `set services advanced-anti-malware policy CLI` command to associate it with the Sky ATP profile.

**NOTE:** If you are using the free model of Sky ATP, you are limited to only the executable file category.

## RELATED DOCUMENTATION

[Creating File Inspection Profiles | 235](#)

[Sky ATP Malware Management Overview | 233](#)

[File Scanning Limits | 269](#)

# Creating File Inspection Profiles

Access this page from **Configure > Threat Prevention > Sky ATP Malware Management** and choose the **File Inspection Profiles** tab.

- Read the [“File Inspection Profiles Overview” on page 233](#) topic.
- Read the [“File Scanning Limits” on page 269](#) topic.
- Note that if you are using the free version of Sky ATP, only executable files are scanned.

To configure file inspection profiles:

1. From the **File Inspection Profiles** tab, click the + sign.
2. Enter a name for the profile. (You can create multiple profiles for file inspection.)
3. Select a **Sky ATP Realm**.
4. Select the file types to include using the check boxes. You can also define the maximum file size requirement per each category to send to the cloud. If a file falls outside of the maximum file size limit, the file is automatically downloaded to the client system. See [Table 69 on page 235](#) for the list of file types for each category.
5. Click **OK**.

**Table 69: File Category Contents**

Category	Description
Active media	Flash and Silverlight applications
Archive	Archive files
Code	Source code
Config	Configuration files
Document	All document types except PDFs
Emerging threat	A special category that includes known threat source file types
Executable	Executable binaries

Table 69: File Category Contents (*continued*)

Category	Description
Java	Java applications, archives, and libraries
Library	Dynamic and static libraries and kernel modules
Media	Audio video formats
OS package	OS-specific update applications
Script	Scripting files
Portable document	PDF, e-mail, and MBOX files

**NOTE:** Once the profile is created, use the `set services advanced-anti-malware policy CLI` command to associate it with the Sky ATP profile.

#### RELATED DOCUMENTATION

[File Inspection Profiles Overview | 233](#)

[Sky ATP Malware Management Overview | 233](#)

[File Scanning Limits | 269](#)

## Creating Allowlist and Blocklists

Access this page from **Configure > Threat Prevention > Sky ATP Malware Management** and choose the **Whitelist** or **Blacklist** tab.

- Decide on the type of location you intend to define: URL or IP.
- Review current list entries to ensure the item you are adding does not already exist.
- Review syntax requirements for entries in [Table 70 on page 237](#).

To configure allowlists and blocklists:

1. From the **Whitelist** or **Blacklist** tab, click the + sign.
2. Select a **Sky ATP Realm**.
3. Click the + sign.
4. Enter an IP address or a URL. Continue to click the + sign to add more entries. See [Table 70 on page 237](#) for syntax requirements.
5. Click **OK**.

**Table 70: Whitelist and Block Syntax**

Setting	Guideline
IP	Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.
URL	Enter the URL using the following format: juniper.net. Wildcards and protocols are not valid entries. The system automatically adds a wildcard to the beginning and end of URLs. Therefore juniper.net also matches a.juniper.net, a.b.juniper.net, and a.juniper.net/abc. If you explicitly enter a.juniper.net, it matches b.a.juniper.net, but not c.juniper.net. You can enter a specific path. If you enter juniper.net/abc, it matches x.juniper.net/abc, but not x.juniper.net/123.

To edit an existing allowlist or blocklist entry, select the check box next to the entry you want to edit and click the pencil icon.

Sky ATP periodically polls for new and updated content and automatically downloads it to your SRX Series device. There is no need to manually push your allowlist or blocklist files.

RELATED DOCUMENTATION

<a href="#">Sky ATP Malware Management Overview   233</a>
<a href="#">Creating File Inspection Profiles   235</a>

# Implementing Threat Policy on VMWare NSX

## IN THIS SECTION

- VMWare NSX Integration with Policy Enforcer and Sky ATP Overview | 238
- Before You Begin | 241
- Configuring VMware NSX with Policy Enforcer | 244
- Example: Creating a Firewall Rule in VMWare vCenter Server Using SDSN\_BLOCK Tag | 246

## VMWare NSX Integration with Policy Enforcer and Sky ATP Overview

Juniper Networks Sky Advanced Threat Prevention (Sky ATP) identifies the infected virtual machines (VMs) running on VMWare NSX and tags these VMs as infected. This is based on a malware file exchange from the infected VMs and/or based on the Command and Control communication with known botnet sites on the internet.

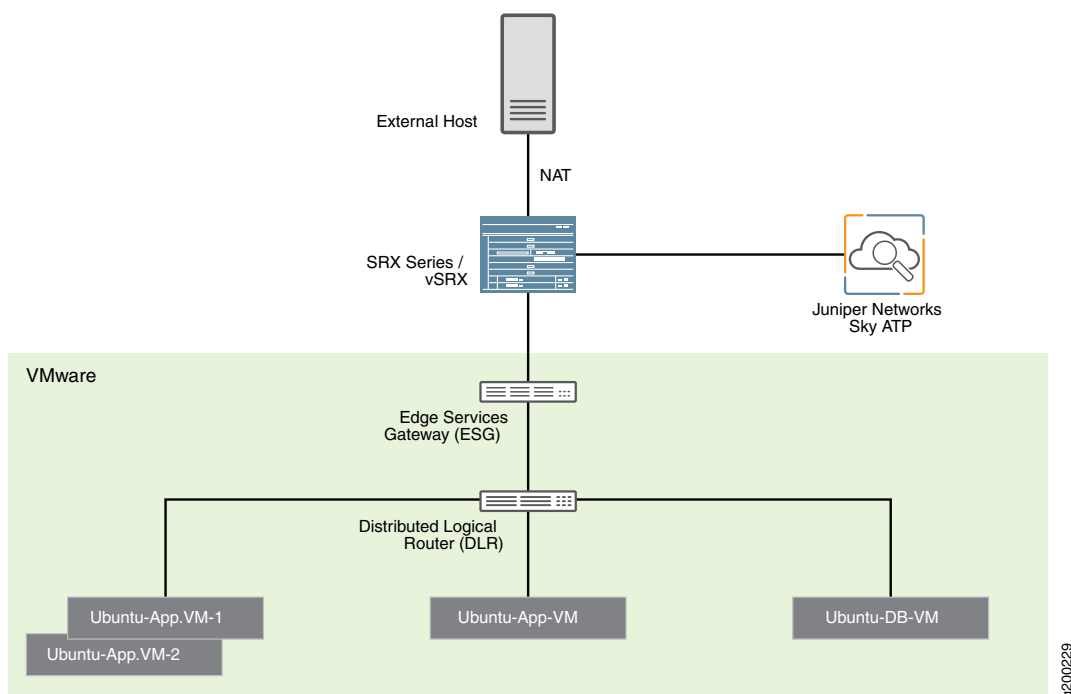
Based on this identification of infected or compromised hosts, you can take one of the following actions:

- Enable additional security features such as Layer-7 Application Firewall and Intrusion Prevention (IPS) leveraging vSRX
- Enforce Layer-2 to Layer-4 controls using NSX Distributed Firewall
- Leverage NSX integration with Host-Based security vendors (<https://www.vmware.com/products/nsx/technology-partners.html>) to take host-based security actions such as running antivirus or anti malware features on the infected VMs.

Policy Enforcer provides a set of Connector APIs for the third-party adaptors. The NSX Connector integrates with the Policy Enforcer using these APIs to enable enforcement of the infected hosts policy on Secure Fabric. For NSX connectors, the NSX Manager, its associated vCenter, and an edge firewall form the Secure Fabric.

The following topology shows how NSX Manager and the edge firewall create a Secure Fabric to use with Policy Enforcer.

Figure 57: Topology of NSX Integration with Policy Enforcer



Within the NSX Manager, the virtual machines (VM) connect to logical networks, shown as green and yellow colour logical networks, as shown in [Figure 57 on page 239](#). The logical switches connect to each other using a Distributed Logical Router(DLR). To form the Secure Fabric, configure the edge service gateway (ESG) to point to SRX Series devices or vSRX as the gateway for the networks hosted on NSX. This is implemented by establishing IBGP session between ESG and vSRX or SRX Series device. This ensures that all the north-south traffic passes through the vSRX edge firewall. The vSRX edge gateway is enrolled with Sky ATP for the traffic inspection.

If NAT services are required, it must be configured on the vSRX and not on the ESG. Configure NAT services using the following CLI commands.

```
set security nat source rule-set trust-to-untrust from zone trust
```

```
set security nat source rule-set trust-to-untrust to zone untrust
```

```
set security nat source rule-set trust-to-untrust rule snat-rule match source-address 0.0.0.0/0
```

```
set security nat source rule-set trust-to-untrust rule snat-rule then source-nat interface
```

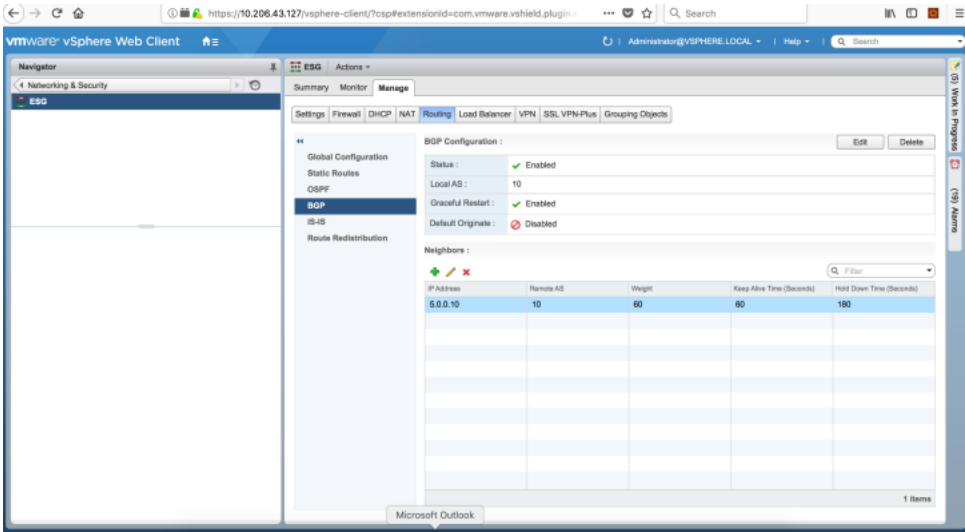
To establish a BGP session, use the following configuration commands:

```
set routing-options autonomous-system 10
```

```
set protocols bgp group nsx neighbor 5.0.0.2 peer-as 10
```

You can view the BGP configuration in VMWare vCenter Server, as shown in [Figure 58 on page 240](#).

**Figure 58: VMWare vCenter BGP Configuration**



**NOTE:** You can register the NSX Manager with Security Director only when the Policy Enforcer is configured. The NSX micro service is bundled with the Policy Enforcer VM. However, the NSX micro service is packaged as a standalone rpm, so that the NSX micro service upgrade and patches can be performed independent of the Policy Enforcer VM.

## Implementation of Infected Hosts Policy Overview

The vSRX or SRX Series devices running as an edge firewall is enrolled to send all the suspected traffic to Sky ATP.

The following steps explain the high-level workflow:

- If an infection is detected, Sky ATP notifies the Policy Enforcer about the infected IP addresses
- If the infected IP address belongs to Secure Fabric associated with the NSX domain, Policy Enforcer calls the NSX plugin APIs to notify the NSX Connector about the list of infected IP addresses
- NSX service will then retrieve the VM corresponding to the IP addresses sent and then calls the NSX API to tag to an appropriate VM with a security tag, SDSN\_BLOCK.

You can then create a policy to block the infected hosts using the SDSN\_BLOCK tag by creating VMWare Distributed Firewall (DFW) rules. The block policy consists of two rules for ingress block and egress block. The ingress block rule applies to any traffic originating from a security group composed of VMs tagged



with a block tag to any destination. Similarly, the egress block rule applies to any traffic destined to security group composed of VMs tagged with block tag from any source.

The creation of security groups associated with the SDSN\_BLOCK tag, creation of ingress and egress block rules, and the action to take on the matching packets must be configured by the VMWare administrators. The NSX Connector will simply apply the SDSN\_BLOCK tag on the infected VM.

## Registering NSX Micro Service as Policy Enforcer Connector Instance Overview

The integration of each NSX manager discovered in Security Director with Policy Enforcer is triggered automatically.

The automatic registration of a connector instance involves the following steps:

1. Discovering the NSX Manager in Security Director. This triggers an auto creation of the Policy Enforcer connector instance.
2. Secure Fabric is created to manage the discovered NSX Manager.
3. Creation of threat prevention policy requires the knowledge of Sky ATP realm and the edge firewall device. These are taken as inputs from the user.

## Before You Begin

### IN THIS SECTION

- [Infected Hosts Workflow in VMware vCenter Server | 241](#)

Before you begin to configure NSX with Policy Enforcer, configure the infected hosts workflow in VMWare vCenter Server.

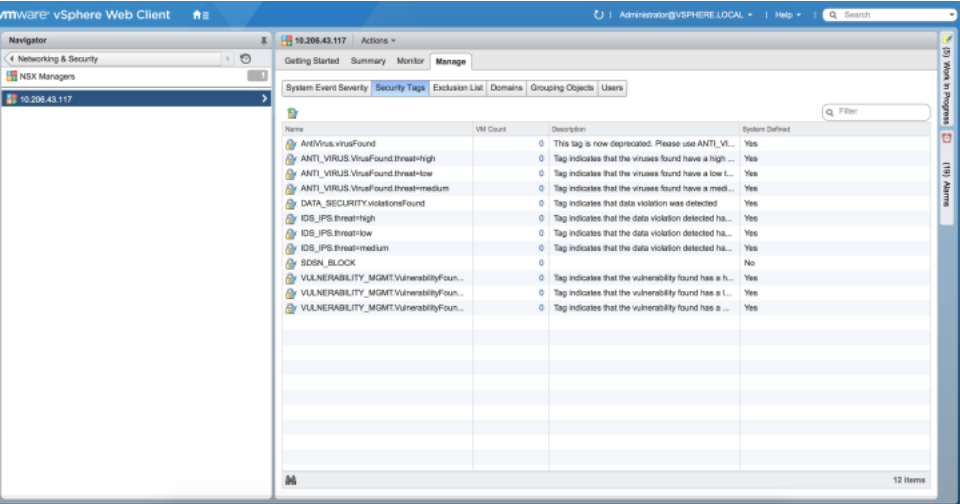
### Infected Hosts Workflow in VMware vCenter Server

To block the infected hosts:

1. Log in to the vSphere Web Client through the VMware vCenter Server.
2. From the vSphere Web Client, click **Networking & Security** and then click **NSX Managers**.

Under the Manage section, click **Security Tags** column head and create SDSN\_BLOCK security tag for NSX, as shown in [Figure 59 on page 242](#).

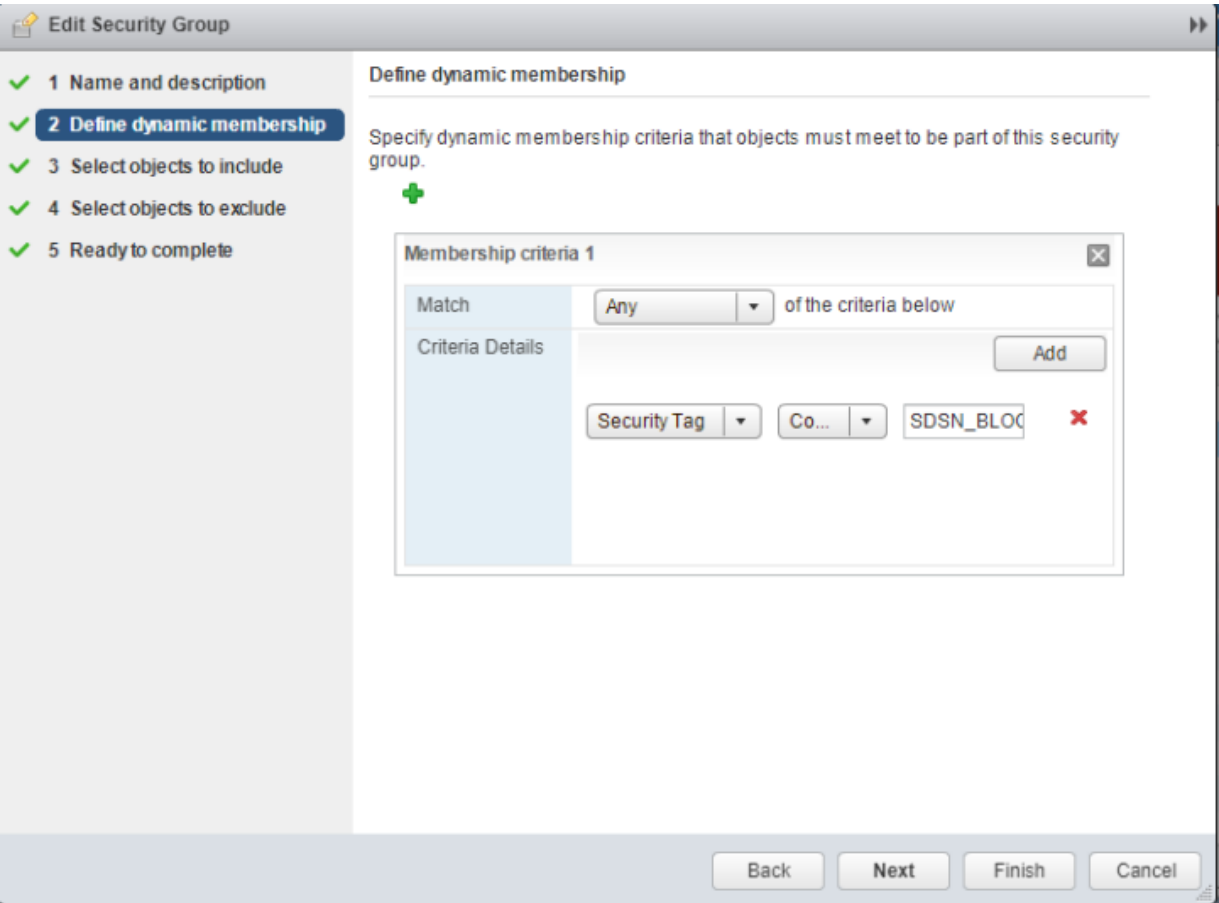
Figure 59: SDSN\_BLOCK Security Tag



The feed for the infected hosts will be triggered by Sky ATP down to Policy Enforcer. When there is a trigger, the SDSN\_BLOCK tag is attached to the VM. Click on the VM Count column to see the VM details attached to the tag.

3. Select **Networking & Security** and then click **Service Composer**.  
The Service Composer page appears. From the Service Composer, click the **Security Groups** tab. The security administrator can create the security group based on the security tag.
4. Click the **New Security Group** icon to create a new security group.
5. Enter a name and description for the security group and then click **Next**.
6. On the Define dynamic membership page, define the criteria that an object must meet for it to be added to the security group you are creating.  
In the Criteria Details row, select **Security Tag** from the list and provide the SDSN\_BLOCK tag name, as shown in [Figure 60 on page 243](#).

Figure 60: Define Dynamic Membership Page



Click **Next**.

- 7. In the Ready to Complete page, verify the parameters and click **Finish**.

In the Service Composer page, under the Security Groups tab, you can see that the security group has been created and the VM with the security tag is assigned to the security group.

## Configuring VMware NSX with Policy Enforcer

The following steps explain configuring VMWare NSX with Policy Enforcer:

1. Add the NSX Manager to the Security Director database, as shown in [Figure 61 on page 244](#). To know more about adding a NSX Manager, see *Adding the NSX Manager*.

Figure 61: Adding NSX Manager Page

Add NSX Manager ⓘ

1 NSX Manager 2 Service Manager Registration 3 vCenter Server

Name \* ⓘ NSX-134

Host \* ⓘ

Port \* ⓘ 443

Username \* ⓘ admin

Password \* ⓘ

Description ⓘ

SSL Certificate ⓘ

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number: 1727846944 (0x66fce5d8)  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: CN=SR, RTO=SA, L=Policy Admin

Accept SSL Certificate \* ⓘ ☒

Cancel Next

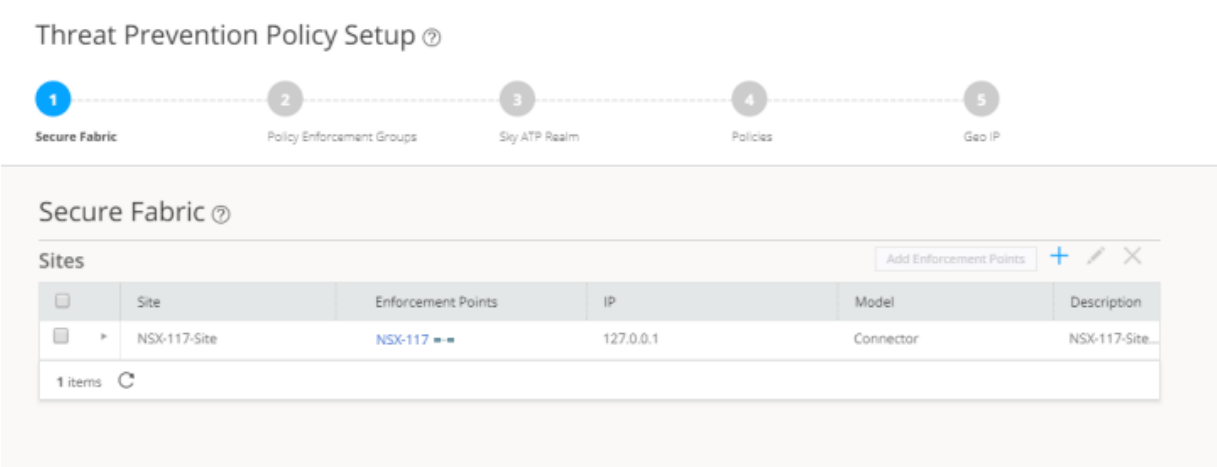
2. After discovering the NSX Manager in Security Director, use the Guided Setup workflow to configure the following parameters:
  - Secure Fabric
  - Policy Enforcement Group (PEG)
  - Sky ATP Realm
  - Threat policies for the following threat types:
    - Command and Control (C&C) Server
    - Infected Hosts
    - Malware
3. Select **Configuration > Guided Setup > Threat Prevention**.

The Threat Prevention Policy Setup page appears.

4. Click **Stat Setup**.

The Threat Prevention Policy Setup page appears, as shown in [Figure 62 on page 245](#). Some of the resources are already configured as you discover the NSX Manager.

**Figure 62: Guided Setup Page**



5. In the Secure Fabric page, the site is already created. For that site, one enforcement point is also added.

To create a secure fabric site in Policy Enforcer for NSX based environment, you require two parts : NSX Manager and edge firewall. In the Add Enforcement Points page, add vSRX, as shown in the topology, as a edge firewall. Select the vSRX device listed under the Available column and move it to the Selected column. You now have two enforcement points within the Secure Fabric.

Click **Next**.

6. In the Policy Enforcement Groups page, the policy enforcement group is already created based on the Location Group Type. The location points to the Secure Fabric site created for NSX.

Click. **Next**.

7. In the Sky ATP Realm page, associate the Secure Fabric with a Sky ATP realm.

If the Sky ATP realm is already created, click **Assign Sites** in the Sites Assigned column and chose the Secure Fabric site. The Sky ATP realm and Secure Fabric are now associated.

Click. **Next**.

8. In the Policies page, create a threat prevention policy by choosing the profile types depending on the type of threat prevention this policy provides (C&C Server, Infected Host, Malware) and an action for

the profile. The DDoS profile is not supported by the NSX Connector. Once configured, you apply policies to PEGs.

Click **Assign groups** in the Policy Enforcement Group column to associate the policy enforcement group with the policy.

Security Director takes the snapshot of the firewall by performing the rule analysis and threat remediation rules are pushed into the edge firewall.

Click **Finish**.

**NOTE:** The GeolP feeds are not used with the NSX Connectors.

9. The last page is a summary of the items you have configured using quick setup. Click **OK** to be taken to the Policies page under Configure > Threat Prevention > Policies and your policy is listed there.

## Example: Creating a Firewall Rule in VMWare vCenter Server Using SDSN\_BLOCK Tag

The following example shows the firewall rule creation using the SDSN\_BLOCK security tag:

1. Log in to the vSphere Web Client through the VMware vCenter Server.
2. Select **Networking & Security** and then click **Service Composer**.  
The Service Composer page appears.
3. Select **Security Policies** tab in the Service Composer page.  
Create a security policy to block the traffic coming from the infected hosts.
4. Select the **Create Security Policy** icon.  
The New Security Policy page appears.
5. Enter a name and description for the security policy, and click **Next**.
6. Select the **Firewall Rules** option from the left pane.  
The Firewall Rules page appears.
7. Select the New Firewall Rule icon (+) to create a new firewall rule.

The New Firewall Rule page appears.

8. Enter the name of the firewall rule.
  9. In the Action field, select the **Block** option.
  10. In the Source field, click **Change** and select the security group.
  11. In the Destination field, click **Change** and select the security group to add as Any.
- Click **Ok**. [Figure 63 on page 248](#) shows a sample firewall rule configuration.

Figure 63: New Firewall Rule Page

**New Firewall Rule**

Name:

Description/Comments:

Action: ☐ Allow ☒ Block ☐ Reject

Source: Policy's Security Groups [Change...](#)  
☐ Negate source

Destination: Any [Change...](#)  
☐ Negate destination

**i** Either source or destination selection (or both) must be "Policy's Security Groups". Current selection will apply to "Outgoing" traffic from the security groups where this policy gets applied to specified Destination.

Service: Any [Change...](#)

State: ☒ Enabled ☐ Disabled

Log: ☐ Log ☒ Do not log

**OK** **Cancel**

12. Click **Finish**.

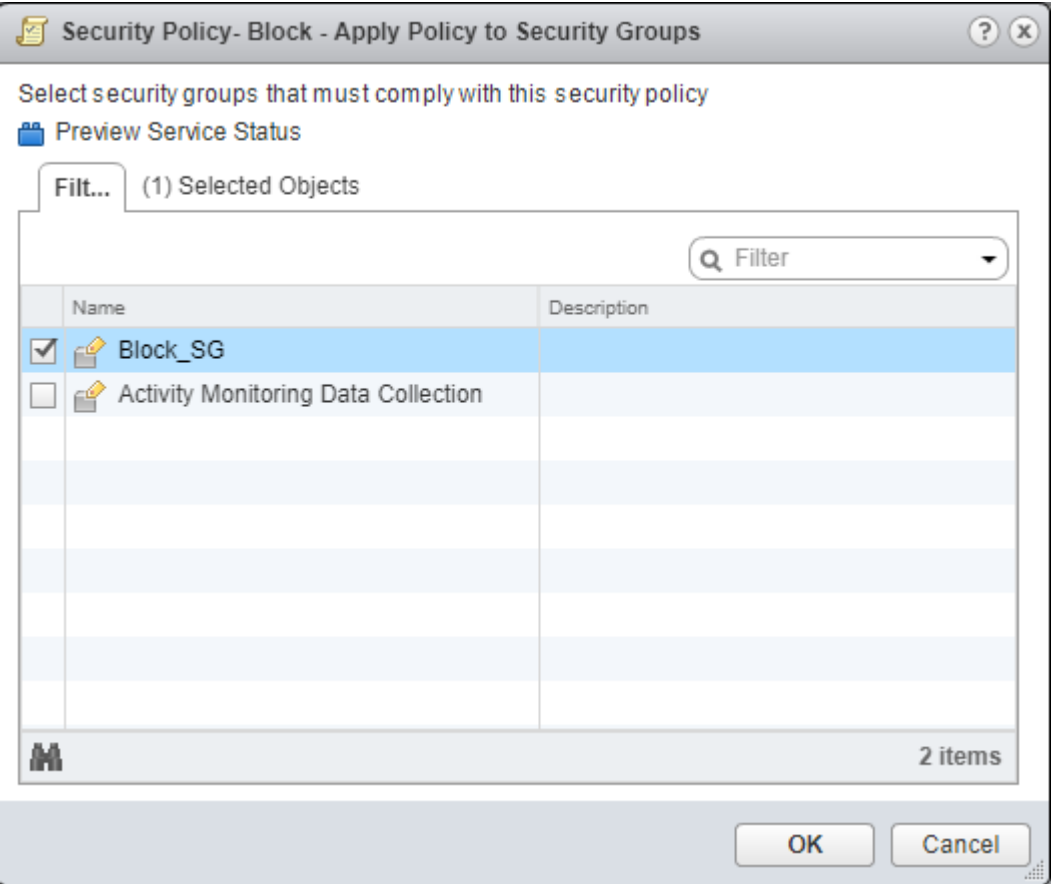
A new policy is created. You can apply this policy to the security group.

13. In the Security Policies page, right-click on the policy name and select **Apply Policy**.

The Apply Policy to Security Groups page appears, as shown in [Figure 64 on page 249](#).



Figure 64: Apply Policy to SG Page



14. Select the security group that you have created and assign to a policy.
- Security administrator is now able to block the traffic coming from the infected hosts.

# 13

CHAPTER

## Threat Prevention- Monitor

---

[Policy Enforcer Dashboard Widgets | 252](#)

[Infected Hosts Overview | 253](#)

[Infected Host Details | 254](#)

[Command and Control Servers Overview | 256](#)

[Command and Control Server Details | 257](#)

[HTTP File Download Overview | 259](#)

[HTTP File Download Details | 260](#)

[SMTP Quarantine Overview | 262](#)

[Email Attachments Scanning Overview | 264](#)

[Email Attachments Scanning Details | 265](#)

[IMAP Block Overview | 267](#)

[File Scanning Limits | 269](#)

[All Hosts Status Details | 270](#)

[DDoS Feeds Status Details | 272](#)

---

# Policy Enforcer Dashboard Widgets

Policy enforcer adds widgets to the dashboard that provide a summary of all gathered information on compromised content and hosts. Drag and drop widgets to add them to your dashboard. Mouse over a widget to refresh, remove, or edit the contents.

In addition, you can use the dashboard to:

- Navigate to the File Scanning page from the Top Scanned Files and Top Infected Files widgets by clicking the **More Details** link.
- Navigate to the Hosts page from the Top Compromised Hosts widget by clicking the **More Details** link.
- Navigate to the Command and Control Servers page from the C&C Server Malware Source Location widget.

**NOTE:** C&C and GeoIP filtering feeds are only available with the Cloud Feed or Premium license.

Available dashboard widgets are as follows:

**Table 71: Sky ATP Dashboard Widgets**

Widget	Definition
Top Malware Identified	A list of the top malware found based on the number of times the malware is detected over a period of time. Use the arrow to filter by different time frames.
Top Compromised Hosts	A list of the top compromised hosts based on their associated threat level and blocked status.
Top Infected File Types	A graph of the top infected file types by file extension. Examples: exe, pdf, ini, zip. Use the arrows to filter by threat level and time frame.
Top Infected File Categories	A graph of the top infected file categories. Examples: executables, archived files, libraries. Use the arrows to filter by threat level and time frame.
Top Scanned File Types	A graph of the top file types scanned for malware. Examples: exe, pdf, ini, zip. Use the arrows to filter by different time frames.
Top Scanned File Categories	A graph of the top file categories scanned for malware. Examples: executables, archived files, libraries. Use the arrows to filter by different time frames.

Table 71: Sky ATP Dashboard Widgets (*continued*)

Widget	Definition
C&C Server and Malware Source	A color-coded map displaying the location of Command and Control servers or other malware sources. Click a location on the map to view the number of detected sources.

## RELATED DOCUMENTATION

[Infected Hosts Overview | 253](#)
[Command and Control Servers Overview | 256](#)
[HTTP File Download Overview | 259](#)
[SMTP Quarantine Overview | 262](#)

## Infected Hosts Overview

Access this page from **Monitor > Threat Prevention > Hosts**.

The hosts page lists compromised hosts and their associated threat levels. From here, you can monitor and mitigate malware detections on a per host basis.

**NOTE:** You must select a Sky ATP realm from the available pulldown.

Compromised hosts are systems for which there is a high confidence that attackers have gained unauthorized access. When a host is compromised, the attacker can do several things to the computer, such as:

- Send junk or spam e-mail to attack other systems or distribute illegal software.
- Collect personal information, such as passwords and account numbers.

Compromised hosts are listed as secure intelligence data feeds (also called information sources.) The data feed lists the IP address or IP subnet of the host along with a threat level; for example, 130.131.132.133 and threat level 5. Once threats are identified, you can create threat prevention policies to take enforcement actions on the inbound and outbound traffic on these infected hosts.

**Export Data**—Click the Export button to download compromised host data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

## RELATED DOCUMENTATION

[Infected Host Details | 254](#)[HTTP File Download Overview | 259](#)[HTTP File Download Details | 260](#)[Email Attachments Scanning Overview | 264](#)[Email Attachments Scanning Details | 265](#)[File Scanning Limits | 269](#)

## Infected Host Details

Access this page by clicking on the host IP from the **Hosts** page.

Use the host details page to view in-depth information about current threats to a specific host by time frame. From here you can change the investigation status and the blocked status of the host.

The information provided on the host details page is as follows:

**Table 72: Threat Level Definitions**

Threat Level	Definition
0	Clean; no action is required.
1–3	Low threat level. Recommendation: Disable this host.
4–6	Medium threat level. Recommendation: Disable this host.
7–10	High threat level. Host has been automatically blocked.

- **Host Status**—Displays the current state by threat level, which could be any of the levels described in the table above.
- **Investigation Status**—The following states of investigation are available: Open, In progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.
- **Policy override for this host**—The following options are available: Use configured policy (not included in infected hosts feed), Always include host in infected hosts feed, Never include host in infected hosts feed.

**NOTE:** The blocked status changes in relation to the investigation state. For example, when a host changes from an open status (Open or In Progress) to one of the resolved statuses, the blocked status is changed to allowed and the threat level is brought down to 0. Also, when the investigation status is changed to resolved, an event is added to the log at the bottom of the page.

- Host threat level graph—This is a color-coded graphical representation of threats to this host displayed by time frame. You can change the time frame, and you can slide the graph backward or forward to zoom in or out on certain times. When you zoom in, you can view individual days within a month.
- Expand time-frame to separate events—Use this check box to stretch a period of time and see the events spread out individually.
- Past threats—The date and status of past threats to this host are listed here. The time frame set previously also applies to this list. The description for each event provides details about the threat and the action taken at the time.

#### RELATED DOCUMENTATION

---

[Infected Hosts Overview](#) | 253

---

[HTTP File Download Overview](#) | 259

---

[HTTP File Download Details](#) | 260

---

[File Scanning Limits](#) | 269

---

[Policy Enforcer Dashboard Widgets](#) | 252

# Command and Control Servers Overview

Access this page from the **Monitor** menu.

**NOTE:** C&C and Geo IP filtering feeds are only available with a Sky ATP premium license.

**NOTE:** When managing Sky ATP with Security Director, you must select a Sky ATP realm from the available pulldown.

The C&C servers page lists information on servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them. Botnets can be used to gather sensitive information, such as account numbers or credit card information, or to participate in a distributed denial-of-service (DDoS) attack.

When a host on your network tries to initiate contact with a possible C&C server on the Internet, the SRX Series device can intercept the traffic and perform an enforcement action based on real-time intelligence feed information that identifies the C&C server IP address and URL.

- **Export Data**—Click the **Export** button to download C&C data to a CSV file. You are prompted to narrow the data download to a selected time-frame.
- **Report False Positives**—Click the **FP/FN** button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.

The following information is available on this page.

**Table 73: Command & Control Server Data Fields**

Field	Definition
C&C Server	The IP address of the suspected command and control server.
C&C Threat Level	The threat level of the C&C server as determined by an analysis of actions and behaviors.
Hits	The number of times the C&C server has attempted to contact hosts on your network.



Table 73: Command & Control Server Data Fields (*continued*)

Field	Definition
C&C Country	The country where the C&C server is located.
Last Seen	The date and time of the most recent C&C server hit.
Protocol	The protocol (TCP or UDP) the C&C server used to attempt communication.
Client Host	The IP address of the host the C&C server attempted to communicate with.
Action	The action taken on the communication (permitted or blocked).

## RELATED DOCUMENTATION

[Command and Control Server Details | 257](#)

[HTTP File Download Overview | 259](#)

[Email Attachments Scanning Overview | 264](#)

[Email Attachments Scanning Details | 265](#)

[File Scanning Limits | 269](#)

# Command and Control Server Details

Access this page by clicking the **External Server IP** from the **Command and Control Servers** page.

Use Command and Control Server Details page to view analysis information and a threat summary for the C&C server. The following information is displayed for each server.

- Total Hits
- Threat Summary (Threat level, Location, Category, Time last seen)
- Ports and protocols used

You can filter this information by clicking on the time-frame links: 1 day, 1 week, 1 month, Custom (select your own time-frame). You can also expand the time-frame to separate events using the slider.

## Hosts That have Contacted This C&C Server

This is a list of hosts that have contacted the server. The information provided in this section is as follows:

Table 74: Command &amp; Control Server Contacted Host Data

Field	Definition
Client Host	The name of the host in contact with the command and control server.
Client IP Address	The IP address of the host in contact with the command and control server. (Click through to the Host Details page for this host IP.)
C&C Threat Level	The threat level of the C&C server as determined by an analysis of actions and behaviors.
Action	The action taken on the communication (permitted or blocked).
Protocol	The protocol (TCP or UDP) the C&C server used to attempt communication.
Port	The port the C&C server used to attempt communication.
Device Name	The name of the device in contact with the command and control server.
Date Seen	The date and time of the most recent C&C server hit.
Username	The name of the host user in contact with the command and control server.

### Associated Domains

This is a list of domains the destination IP addresses in the C&C server events resolved to.

### Signatures

This is a list of command and control indicators that were detected.

### RELATED DOCUMENTATION

[Command and Control Servers Overview | 256](#)

[Infected Hosts Overview | 253](#)

[HTTP File Download Overview | 259](#)

[Policy Enforcer Dashboard Widgets | 252](#)

# HTTP File Download Overview

Access this page from the **Monitor** menu.

A record is kept of all file metadata sent to the cloud for inspection. These are files downloaded by hosts and found to be suspicious based on known signatures or URLs. From the main page, click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.

**NOTE:** When managing Sky ATP with Security Director, you must select a Sky ATP realm from the available pulldown.

**Export Data**—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

The following information is available on this page.

**Table 75: HTTP Scanning Data Fields**

Field	Definition
File Signature	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file signature can also contain information that ensures the original data stored in the file remains intact and has not been modified.
Threat Level	The threat score.  <b>NOTE:</b> Click the three vertical dots at the top of the column to filter the information on the page by threat level.
Filename	The name of the file, including the extension.  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.
Last Submitted	The time and date of the most recent scan of this file.
URL	The URL from which the file originated.  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.
Malware	The name of file and the type of threat if the verdict is positive for malware. Examples: Trojan, Application, Adware. If the file is not malware, the verdict is "clean."  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.

Table 75: HTTP Scanning Data Fields (*continued*)

Field	Definition
Category	The type of file. Examples: PDF, executable, document.  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.

## RELATED DOCUMENTATION

[HTTP File Download Details | 260](#)
[SMTP Quarantine Overview | 262](#)
[Email Attachments Scanning Overview | 264](#)
[File Scanning Limits | 269](#)

## HTTP File Download Details

To access this page, navigate to **Monitor > Threat Prevention > HTTP File Download**. Click on the **File Signature** to go to the File Scanning Details page.

Use this page to view analysis information and malware behavior summaries for the downloaded file. This page is divided into several sections:

**Report False Positives**—Click the **Report False Positive** button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.

**Printable View**—Click this link to organize the information into a print-ready format.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the threat category and the action taken.
- **Top Indicators**—In this box, you will find the malware name, the signature it matches, and the IP address/URL from which the file originated.
- **Prevalence**—This box provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

## File Summary

Table 76: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.
Category	The type of file. Examples: PDF, executable, document.
File Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Sky ATP determines the name of the malware.
Malware Type	If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, Sky ATP determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

In the Network Activity section, you can view information in the following tabs:

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Sky ATP sandbox.
- **Contacted IPs**—If available, lists all IPs that were contacted while executing the file, along with the destination IP's country, ASN, and reputation. The reputation field is based on Juniper IP intelligence data destination.
- **DNS Activity**— This tab lists DNS activity while executing the file, including reverse lookup to find the domain name of externally contacted servers. This tab also provides the known reputation of the destination servers.

## HTTP Downloads

This is a list of hosts that have downloaded the suspicious file. Click the **IP address** to be taken to the Host Details page for this host. Click the **Device Serial number** to be taken to the Devices page. From there you can view device versions and version numbers for the Sky ATP configuration, including profile, allowlist, and blocklist versions. You can also view the malware detection connection type for the device: telemetry, submission, or C&C event.

### RELATED DOCUMENTATION

[HTTP File Download Details | 260](#)[SMTP Quarantine Overview | 262](#)[Email Attachments Scanning Overview | 264](#)[File Scanning Limits | 269](#)[Policy Enforcer Dashboard Widgets | 252](#)

## SMTP Quarantine Overview

Access this page from the **Monitor** menu.

The SMTP quarantine monitor page lists quarantined emails with their threat score and other details including sender and recipient. You can also take action on quarantined emails here, including releasing them and adding them to the blocklist.

The following information is available from the Summary View:

**Table 77: Blocked Email Summary View**

Field	Description
Time Range	Use the slider to narrow or increase the time-frame within the selected the time parameter in the top right: 12 hrs, 24 hrs, 7 days or custom.
Total Email Scanned	This lists the total number of emails scanned during the chosen time-frame and then categorizes them into blocked, quarantined, released, and permitted emails.

Table 77: Blocked Email Summary View (*continued*)

Field	Description
Malicious Email Count	This is a graphical representation of emails, organized by time, with lines for blocked emails, quarantined and not released emails, and quarantined and released emails.
Emails Scanned	This is a graphical representation of emails, organized by time, with lines for total emails, and emails with one or more attachments.
Email Classification	This is another graphical view of classified emails, organized by percentage of blocked emails, quarantined and not released emails, and quarantined and released emails.

The following information is available from the Detail View:

Table 78: Blocked Email Detail View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the <b>Read This</b> link to go to the Sky ATP quarantine portal and preview the email.
Date	The date the email was received.
Malicious Attachment	Click on the attachment name to go to the Sky ATP file scanning page where you can view details about the attachment.
Size	The size of the attachment in kilobytes.
Threat Score	The threat score of the attachment, 0-10, with 10 being the most malicious.
Threat Name	The type of threat found in the attachment, for example, worm or trojan.
Action	The action taken, including the date and the person (recipient or administrator) who took the action.

Using the available buttons on the Details page, you can take the following actions on blocked emails:

- Add domain to blocklist

- Add sender to blocklist
- Release

## RELATED DOCUMENTATION

[HTTP File Download Overview | 259](#)

[HTTP File Download Details | 260](#)

[Email Attachments Scanning Overview | 264](#)

# Email Attachments Scanning Overview

Access this page from the **Monitor** menu.

A record is kept of all file metadata sent to the cloud for inspection. These are files downloaded by hosts and found to be suspicious based on known signatures. From the main page, click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.

**NOTE:** You must select a Sky ATP realm from the available pulldown.

**Export Data**—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

The following information is available on this page.

**Table 79: Email Attachments Scanning Data Fields**

Field	Definition
File Signature	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file signature can also contain information that ensures the original data stored in the file remains intact and has not been modified.
Threat Level	The threat score.
Date Scanned	The date and time the file was scanned.
Filename	The name of the file, including the extension.



Table 79: Email Attachments Scanning Data Fields (*continued*)

Field	Definition
Recipient	The email address of the intended recipient.
Sender	The email address of the sender.
Malware Name	The type of malware found.
Status	Indicates whether the file was blocked or permitted.
Category	The type of file. Examples: PDF, executable, document.

## RELATED DOCUMENTATION

[Email Attachments Scanning Details | 265](#)

[SMTP Quarantine Overview | 262](#)

[File Scanning Limits | 269](#)

# Email Attachments Scanning Details

To access this page, navigate to **Monitor > File Scanning > Email Attachments**. Click on the **File Signature** to go to the File Scanning Details page.

Use this page to view analysis information and malware behavior summaries for the downloaded file. This page is divided into several sections:

**Report False Positives**—Click the **Report False Positive** button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.

**Printable View**—Click this link to organize the information into a print-ready format.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the threat category and the action taken.

- **Top Indicators**—In this box, you will find the malware name, the signature it matches, and the IP address/URL from which the file originated.
- **Prevalence**—This box provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

## File Summary

Table 80: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Action Taken	The action taken based on the threat level and host settings: block or permit.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.
Category	The type of file. Examples: PDF, executable, document.
File Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Sky ATP determines the name of the malware.
Malware Type	If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, Sky ATP determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

In the Network Activity section, you can view information in the following tabs:

**NOTE:** This section will appear blank if there has been no network activity.

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Sky ATP sandbox.
- **Contacted IPs**—If available, lists all IPs that were contacted while executing the file, along with the destination IP's country, ASN, and reputation. The reputation field is based on Juniper IP intelligence data destination.
- **DNS Activity**— This tab lists DNS activity while executing the file, including reverse lookup to find the domain name of externally contacted servers. This tab also provides the known reputation of the destination servers.

In the Behavior Details section, you can view the behavior of the file on the system. This includes any processes that were started, files that were dropped, and network activity seen during the execution of the file. Dropped files are any additional files that were downloaded and installed by the original file.

#### RELATED DOCUMENTATION

[Email Attachments Scanning Overview | 264](#)

[Infected Hosts Overview | 253](#)

[HTTP File Download Overview | 259](#)

[SMTP Quarantine Overview | 262](#)

[File Scanning Limits | 269](#)

[Policy Enforcer Dashboard Widgets | 252](#)

## IMAP Block Overview

Access this page from **Monitor > Threat Prevention > IMAP Block**.

The IMAP Block monitor page lists blocked emails with their threat score and other details including sender and recipient. You can also take action on blocked emails here, including releasing them and adding them to the blocklist.

[Table 81 on page 268](#) shows information available from the Summary View tab.

**Table 81: Blocked Email Summary View**

Field	Description
Sky ATP Realm	Select the registered Sky ATP realm from the list.
Time Range	Use the slider to narrow or increase the time-frame within the selected the time parameter in the top right: 12 hrs, 24 hrs, 7 days or custom.
Malicious Email Count	This lists the total number of malicious emails scanned during the chosen time-frame and then categorizes them into blocked, blocked and not allowed, quarantined and allowed.
Emails Scanned	This is a graphical representation of all scanned emails, organized by date.

[Table 82 on page 268](#) shows information available from the Detail View tab.

**Table 82: Blocked Email Detail View**

Field	Description
Recipient	Specifies the email address of the recipient.
Sender	Specifies the email address of the sender.
Subject	Click <b>Read This</b> to go to the Sky ATP quarantine portal and preview the email.
Date	Specifies the date the email was received.
Malicious Attachment	Click on the attachment name to go to the Sky ATP file scanning page where you can view details about the attachment.
Size	Specifies the size of the attachment in kilobytes.
Threat Score	Specifies the threat score of the attachment, in a scale of 0-10, with 10 being the most malicious.
Threat Name	Specifies the type of threat found in the attachment, for example, worm or trojan.
Action	Specifies the action taken, including the date and the person (recipient or administrator) who took the action.

Using the available buttons on the Details page, you can take the following actions on blocked emails:

- Unblock Attachment for Selected User(s)

- Unblock Attachment for All Users

RELATED DOCUMENTATION

# File Scanning Limits

There is a limit to the number of files which can be submitted to the cloud for inspection. This limit is dictated by the device and license type. When the limit is reached, the file submission process is paused.

**NOTE:** This limit applies to all files, HTTP and SMTP.

Limit thresholds operate on a sliding scale and are calculated within 24-hour time-frame starting "now."

Perimeter Device	Free License (files per day)	Premium License (files per day)
SRX340	200	1,000
SRX345	300	2,000
SRX550m	500	5,000
SRX1500	2,500	10,000
SRX5400	5,000	50,000
SRX5600	5,000	70,000
SRX5800	5,000	100,000
vSRX(10mbps)	25	200
vSRX(100mbps)	200	1,000
vSRX(1000mbps)	2,500	10,000
vSRX(2000mbps)	2,500	10,000

Perimeter Device	Free License (files per day)	Premium License (files per day)
vSRX(4000mbps)	3,000	20,000

## RELATED DOCUMENTATION

[Infected Hosts Overview](#) | 253

[HTTP File Download Overview](#) | 259

[Email Attachments Scanning Overview](#) | 264

# All Hosts Status Details

Use the All Hosts Status page to view the enforcement status of infected hosts feeds. The supported host feeds are custom and Sky ATP.

By default, details for both custom and Sky ATP hosts are shown. You must select the required feed type from the Feed Source column.

**NOTE:** To view the All Hosts Status page, you must have the Threat Management privileges or predefined roles enabled.

To see the details of all hosts status:

1. Select **Monitor > Threat Prevention > All Hosts Status**.

The All Hosts Status page appears.

2. [Table 83 on page 270](#) shows the information provided on the All Hosts Status page.

**Table 83: Fields on All Hosts Status Page**

Column Name	Description
IP Address	Specifies the IP address of the feed.
MAC Address	Specifies the MAC address of the feed.

Table 83: Fields on All Hosts Status Page (*continued*)

Column Name	Description
Feed Name	Specifies the name of the feed.
Feed Source	Specifies type of the feed source.
Action	Specifies the action of the infected host. For example: Block or Quarantine.
Enforcement Status	Specifies the enforcement status of the infected host.
Switch Name	Specifies the name of the Juniper Networks switch used to monitor the feed.
Interface Name	Specifies the interface on the switch where the user is connected to a network.
Policy Associated	<p>Specifies the name of the associated threat prevention policy.</p> <p>This column is not shown by default. Click <b>Show Hide Column</b> and select this field to appear on the All Hosts Status page.</p>
PEG Associated	<p>Specifies the Policy Enforcement Group (PEG) associated with the policy.</p> <p>This column is not shown by default. Click <b>Show Hide Column</b> and select this field to appear on the All Hosts Status page.</p>
Matched Subnet	<p>Specifies the subnet that is added as an endpoint for the PEG.</p> <p>This column is not shown by default. Click <b>Show Hide Column</b> and select this field to appear on the All Hosts Status page.</p>
Connector Type	Specifies the type of connector used as an enforcement point.
Connector Name	<p>Specifies the name of the connector.</p> <p>This column is not shown by default. Click <b>Show Hide Column</b> and select this field to appear on the All Hosts Status page.</p>
Endpoint Address Space Type	<p>Specifies the type of endpoints added to a PEG.</p> <p>This column is not shown by default. Click <b>Show Hide Column</b> and select this field to appear on the All Hosts Status page.</p>
Endpoint Address Space Name	<p>Specifies the name of an endpoint.</p> <p>This column is not shown by default. Click <b>Show Hide Column</b> and select this field to appear on the All Hosts Status page.</p>

You can click the filter icon to filter the data based on the following fields:

- Feed source type
- Action
- Enforcement status
- Connector type

RELATED DOCUMENTATION

| [Custom Feed Sources Overview](#) | 209

# DDoS Feeds Status Details

Use the DDoS Feeds Status page to view the enforcement status of Distributed Denial of Service (DDoS) feeds.

In Sky ATP Only mode, you do not see the DDoS Feeds Status page under Monitor. An error message is shown that the page is unavailable because the current threat prevention type is set to Sky ATP only mode.

**NOTE:** To view the DDoS Feeds Status page, you must have the Threat Management privileges or predefined roles enabled.

To view details of DDoS feeds status:

1. Select **Monitor > Threat Prevention > DDoS Feeds Status**.

The DDoS Feeds Status page appears.

2. [Table 84 on page 272](#) shows information provided on the DDoS Feeds Status page.

Table 84: Fields on the DDoS Feeds Status Page

Column Name	Description
Feed Name	Specifies the DDoS feed name to monitor the feeds.
Site	Specifies the associated site name with the DDoS feeds



Table 84: Fields on the DDoS Feeds Status Page (*continued*)

Column Name	Description
MX Name	Specifies the name of the MX router where DDoS is enabled.
MX IP	Specifies the IP address of the MX router.
MX Status	Specifies the status of the MX router.
Action	<p>Specifies the action taken for the DDoS profile</p> <p>To filter the data based on a specific action, click the filter icon and select the required DDoS profile action from the list.</p>
Enforcement Status	<p>Specifies the enforcement status of the feed. Hover over the status to view the reason for that particular status.</p> <p>To filter the data based on a specific enforcement status, click the filter icon and select the required enforcement status from list to monitor the feed.</p>
Policy	Specifies the name of the associated threat prevention policy.
PEG	Specifies the Policy Enforcement Group (PEG) associated with the policy.

## RELATED DOCUMENTATION

[Custom Feed Sources Overview | 209](#)

[Creating Custom Feeds, DDoS | 220](#)

# 14

CHAPTER

## Troubleshooting

---

Policy Enforcer Log File Locations | **275**

Troubleshooting Common Policy Enforcer Problems | **275**

Troubleshooting ClearPass Issues | **278**

---

# Policy Enforcer Log File Locations

The following Policy Enforcer configuration settings files are located under `/srv/feeder/etc/log`:

**NOTE:** Do not edit these files unless instructed by the Juniper Networks Technical Assistance Center (JTAC).

- **controller\_log.yml**—Defines the format for the **controller.log** file. For example, message and date format and maximum file size.
- **feed\_collector\_log.yml**—Defines the format for the **feed\_collector.log** file. For example, message and date format and maximum file size.
- **feed\_provider\_log.yml**— Defines the format for the **feed\_provider.log** file. For example, message and date format and maximum file size.

The following Policy Enforcer log files are located under `/srv/feeder/log`. By default, a maximum of 10 files are created for each log file. For example, **controller.log**, **controller.log.1**, **controller.log.2**, etc. After 10 files are created, the oldest file (in this example, **controller.log**) is overwritten next.

- **controller.log**—Contains log messages for the interaction of Security Director with Policy Enforcer.
- **feed\_collector.log**—Contains log messages for the downloading of feeds.
- **feed\_provider.log**—Contains log messages for distributing feeds to the SRX Series devices.

The following Policy Enforcer log files are located under `/var/log`:

- **prepare\_vm.log**—Contains information about your Policy Enforcer software installation.
- **pe\_upgrade.log**—Contains information about your Policy Software software upgrade.

## Troubleshooting Common Policy Enforcer Problems

### IN THIS SECTION

- [Troubleshooting Policy Enforcer Installation | 276](#)
- [Troubleshooting Sky ATP Realms and Enrolling Devices | 277](#)

- Troubleshooting Threat Policies and Policy Enforcement Groups | 277
- HTTPS-Based Malware Not Detected | 278

This topic lists some common problem areas you may encounter and how to remedy them.

## Troubleshooting Policy Enforcer Installation

Most common Policy Enforcer installation problems occur around creating and deploying the OVA file. If you are not familiar with virtual machines or OVA files, please see [VMware Documentation](#) and select the appropriate VMware vSphere version.

Other areas to look for include:

- Configuring the virtual machine with the correct network configuration. These values vary according to your installation. When configuring the virtual machine network, you will need to know the following:
  - Virtual machine hostname, IP address and network mask.
  - Default gateway that connects your internal network to external networks.
  - Primary and secondary DNS servers.
  - (optional) NTP servers.
- Virtual machine IP address and ssh root credentials. When configuring the virtual machine, you must identify and record the IP address and the ssh root password. In order for Security Director to communicate with your Policy Enforcer virtual machine, you must enter these values into the PE Settings page (**Administration > PE Settings**) of Security Director.

If you forget the virtual machine IP address, log into the virtual machine again. The setup script automatically runs each time you log in so that you can review your settings.

If you forget the root password, there is no way to retrieve it. You must instead reset your password. Be sure to enter your new password into the PE settings page in Security Director. To reset your password, see [CentOS root password reset instructions](#).

## Troubleshooting Sky ATP Realms and Enrolling Devices

Sky ATP has two service levels: free and premium. The free model solution performs basic malware detection while the premium model solution offers more protection. For more information on Sky ATP license types and the features for each type, see [Sky Advanced Threat Prevention Licenses](#).

Some common problems areas with Sky ATP are:

- Trying to enroll devices that are not supported by Sky ATP. See the [Sky ATP Supported Platforms Guide](#) for more information on supported devices.
- The Sky ATP file limit has been reached. Sky ATP has a maximum number of files per day that you can submit to the cloud for inspection. When an SRX Series device has reached its maximum number of files, it goes into a paused state and cannot submit files for inspection. The device automatically changes to the allowed state when it once again is below the maximum limit. See [Sky ATP File Limits](#) for more information on the maximum number of files per day per device type.
- The vSRX instance fails to enroll. Check to make sure the proper Sky ATP license is installed. See [Managing the Sky ATP License](#) for more information on license management with vSRX deployments.

## Troubleshooting Threat Policies and Policy Enforcement Groups

This section lists some common issues found with threat policies and policy enforcement groups.

- You create a threat policy but don't see the appropriate profiles to choose.

Select **Administration > PE Settings** and make sure the correct mode has been selected. You can only change the mode in the follow order: **Cloud Feed Only** to **SKY ATP** to **SKY ATP with PE**.

- Assigning a threat policy to a policy enforcement group in the Sky ATP with PE mode.

Threat policies are enforced and pushed to devices that support the given profile. If a device is not supported by a profile, it will be listed in the analysis results and in the Junos Space job details.

- You create a policy enforcement group with an IP address subnet but no IP addresses are listed in the GUI.

Make sure that a switch is assigned to the site and that the L3 interfaces are configured on the aggregate switch.

## HTTPS-Based Malware Not Detected

If your HTTPS-based malware is not detected by Sky ATP, the root certificate on your SRX Series device (for HTTPS forward proxy) may be invalid. This may occur when the CA profile name is not correct. It must be named **policyEnforcer**.

For example:

```
root@host# set security pki policyEnforcer ssl-inspect-ca ca-identity  
ssl-inspect-ca  
root@host# set security pki policyEnforcer ssl-ca ca-identity ssl-ca
```

For more information on loading root certificates with Policy Enforcer, see [“Loading a Root CA” on page 64](#).

## Troubleshooting ClearPass Issues

### IN THIS SECTION

- [Viewing Logs Files | 279](#)
- [Configuration Issues | 281](#)
- [Error Code 500 | 282](#)
- [Unable to Block Infected Endpoint | 282](#)
- [Unable to Quarantine Infected Endpoint | 284](#)
- [Unable to Clear Blocked or Quarantined Endpoint | 284](#)

This section describes general troubleshooting tips when dealing with ClearPass issues with Policy Enforcer. For detailed information on troubleshooting ClearPass and ClearPass logs, see your ClearPass documentation.

## Viewing Logs Files

Policy Enforcer writes third-party plug-in log information to `/srv/3rd-party-adaptor/logs/plugin_server.log` using the following format:

```
[<date><time>:<line number>:<function name>:<level>]<detailed message>
```

Three types of information are recorded in the logs:

- Application initialization information.
- Heart-beat with Policy Enforcer—communication status between Policy Enforcer and the third-party plug-in.
- Application operations—for troubleshooting third-party plug-in functionality.

The default logging level is set to DEBUG.

The following is an example of a heart-beat message log:

```
[07/20/2017 04:21:59 PM:_internal.py:87:_log():INFO ] 10.92.82.125 - - [20/Jul/2017
16:21:59] "GET /api/v1/adaptor/heartbeat HTTP/1.1" 200 -
[07/20/2017 04:22:29 PM:produces.py:117:wrapper():DEBUG ] Jsonifing
http://10.92.82.125:8082/api/v1/adaptor/heartbeat
[07/20/2017 04:22:29 PM:parameter.py:90:wrapper():DEBUG ] Function Arguments: []
```

The following is an example of an application operation log:

```
[07/20/2017 05:45:52 PM:default_controller.py:228:adaptor_threats_post():DEBUG ]
Incoming threat POST request: {u'action': u'block', u'threatType': u'InfectedHost',
u'endpoint': {u'macAddress': u'unknown', u'ip': u'192.168.140.20', u'name': u'',
u'tags': []}}
[07/20/2017 05:45:52 PM:track_endpoint.py:27:__init__():INFO ] Creating new infected
host tracking DB.
[07/20/2017 05:45:52 PM:clearpass_agent.py:66:getApiAuthenticationToken():DEBUG ]
Get Oauth2 access token for API client
[07/20/2017 05:45:52 PM:connectionpool.py:805:_new_conn():INFO ] Starting new HTTPS
connection (1): 10.92.81.112
[07/20/2017 05:45:52 PM:connectionpool.py:401:_make_request():DEBUG ] "POST
/api/oauth HTTP/1.1" 200 116
[07/20/2017 05:45:52 PM:clearpass_agent.py:73:getApiAuthenticationToken():INFO ]
Successful get Oauth2 access token
```

```
[07/20/2017 05:45:52 PM:thirdparty_controller.py:84:infectedHostNotif():DEBUG ]
Validating endpoint [192.168.140.20] against Clearpass Endpoint DB
[07/20/2017 05:45:52 PM:clearpass_agent.py:80:getEndpointDataByIp():DEBUG ] Getting
Endpoint detail by IP Address [192.168.140.20]
...
```

You can also access logs within ClearPass Policy Manager and ClearPass Guest to assist in troubleshooting.

- Checking session logs

The Access Tracker window displays information of per-session access activity. To view this activity, select **Monitoring > Access Tracker** within ClearPass Policy Monitor. Click a session in the table to display the Request Details window with details about that session. Click **Show Logs** to view the log details. See [Figure 65 on page 280](#). Change your log level to view more or less session information.

Figure 65: Checking Session Logs

The screenshot shows the ClearPass Policy Manager interface. The breadcrumb navigation is "Monitoring » Live Monitoring » Access Tracker". The main heading is "Access Tracker Jul 25, 2017 18:29:34 PST". A "Request Details" window is open, displaying session information for a selected record (row 1).

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000a6d-01-5977e929		
Date and Time:	Jul 25, 2017 16:58:17 PST		
End-Host Identifier:	24-77-03-5A-F2-64 (Computer / Windows / Windows Vista/7/2008)		
Username:	vlanuser3		
Access Device IP/Port:	10.92.80.228:91 (WLC880R / Trapeze)		
System Posture Status:	UNKNOWN (100)		
<b>Policies Used -</b>			
Service:	srniv_wireless_testing 802.1X Wireless		
Authentication Method:	MSCHAP		
Authentication Source:	Local:localhost		
Authorization Source:	[Local User Repository], [Endpoints Repository], [Insight Repository]		
Roles:	[Onboard Windows], [User Authenticated]		
Enforcement Profiles:	srniv_wireless_testing 802.1X Wireless Profile1		
Service Monitor Mode:	Disabled		
Online Status:	Online		





At the bottom of the window, it says "Showing 1 of 1-8 records" and includes buttons for "Change Status", "Show Configuration", "Export", "Show Logs", and "Close".

- Errors reported by ClearPass

To view events and messages generated by the ClearPass application, select **Administration > Support > Application Log** within ClearPass Guest. See [Figure 66 on page 281](#).



Figure 66: Viewing ClearPass Errors

ClearPass Guest					<a href="#">Support</a>   <a href="#">Help</a>   <a href="#">Logout</a> sriniv (Super Administrator)
Time	IP	User	Severity	Message	
2017-07-19 10:10:18	10.92.82.135	oauth2:sdsnapclient	 error	API call 'POST /api/session/SESS-50-7096e8-930117-afca39/disconnect' failed due to an exception: Error disconnecting session for user vlanuser3. Please check ClearPass Policy Manager > Monitoring > Live Monitoring > Access Tracker for more details.	
2017-07-19 10:27:58	10.92.82.135	oauth2:sdsnapclient	 error	API call 'POST /api/session/SESS-50-7096e8-930117-afca39/disconnect' failed due to an exception: Error disconnecting session for user vlanuser3. Please check ClearPass Policy Manager > Monitoring > Live Monitoring > Access Tracker for more details.	
2017-07-19 10:44:19	10.92.82.135	oauth2:sdsnapclient	 error	API call 'POST /api/session/SESS-54-7096e8-990627-2d191a/disconnect' failed due to an exception: Error disconnecting session for user vlanuser3. Please check ClearPass Policy Manager > Monitoring > Live Monitoring > Access Tracker for more details.	
2017-07-19 10:48:54	172.29.109.86	oauth2:sdsncient	 error	API call 'POST /api/session/SESS-54-7096e8-990627-2d191a/disconnect' failed due to an exception: Error disconnecting session for user vlanuser3. Please check ClearPass Policy Manager > Monitoring > Live Monitoring > Access Tracker for more details.	

Click an event to view details, such as possible causes for that error or a pointer for where to look for more information.

## Configuration Issues

The following are mandatory ClearPass information that must be passed to the Policy Enforcer third-party plug-in to ensure proper communication:

- ClearPass IP address and port number.
- Client ID (**clientId**) for the API to access (configured with ClearPass Guest module).
- Client secret key, used together with **clientId** to obtain the access token for performing REST API calls to the ClearPass server.

If you see a 404 error with “ClearPass configuration is missing” in the log file, then ClearPass is not configured for Policy Enforcer. See [“ClearPass Configuration for Third-Party Plug-in”](#) on page 104 for information on configuring ClearPass with Policy Enforcer.

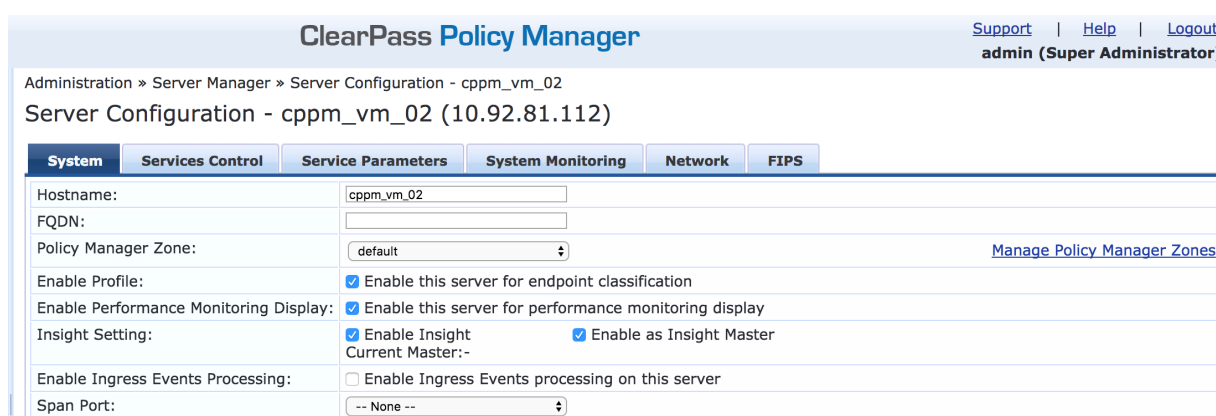
Another method for checking whether ClearPass is configured for Policy Enforcer is to look for the `/srv/3rd-party-adapter/configuration.yaml` file. If this file exists, then the configuration step has been performed.

## Error Code 500

If you receive an error code 500 with the log message **There are no sessions to display. You should enable Insight on at least one node in Policy Manager: Administration > Server Manager > Server Configuration** then the configured ClearPass server does not have Insight enabled. ClearPass Insight is used by ClearPass Policy Manager for in-depth reporting and enhanced analytics.

To enable ClearPass Insight, select **Administration > Server Manager > Server Configuration** from ClearPass Policy Manager. Click the ClearPass server and enable Insight. See [Figure 67 on page 282](#).

Figure 67: Enabling ClearPass Insight



ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Administration » Server Manager » Server Configuration - cppm\_vm\_02

Server Configuration - cppm\_vm\_02 (10.92.81.112)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	cppm_vm_02				
FQDN:					
Policy Manager Zone:	default				<a href="#">Manage Policy Manager Zones</a>
Enable Profile:	<input checked="" type="checkbox"/> Enable this server for endpoint classification				
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight <input checked="" type="checkbox"/> Enable as Insight Master Current Master:-				
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Span Port:	-- None --				

## Unable to Block Infected Endpoint

If you are unable to block an infected endpoint and are using an SRX Series device, make sure the SRX Series device can talk to the Internet. Sky ATP requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet but the “to-cloud” connection should not go through the management interface, for example, fxp0. You do not need to open any ports on the SRX Series device to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have ports 8080 and 443 open.

Use the **show services advanced-anti-malware status** CLI command to verify that connection is made to the cloud server from the SRX Series device. Your output will look similar to the following.

```
root@host> show services advanced-anti-malware status
Server connection status:
  Server hostname: https://skyatp.argon.junipersecurity.net
  Server port: 443
  Control Plane:
```

```

Connection Time: 2015-11-23 12:09:55 PST
Connection Status: Connected
Service Plane:
  fpc0
Connection Active Number: 0
Connection Failures: 0

```

For more information, see the [Sky ATP Administration Guide](#).

If you are able to connect to the Internet, and are still unable to block infected endpoints, perform the following tasks:

- Validate the IP address using ClearPass API Explorer.
  1. Select the Insight API, endpoint service.
  2. Use the **GET /insight/endpoint/ip/{ip}** method.
- Validate the corresponding active session using ClearPass API Explorer.
  1. Select the GuestManager API, ActiveSession service.
  2. Use the **GET /session** method with **framedipaddress** equal to the infected endpoint's IP address.
  3. Sort by **accstarttime** to view the most recent active sessions associated with the IP first.

If there no current active session is returned, the IP address passed down to the plug-in to block is invalid or does not existed.

- If the IP address is valid, confirm that the custom attribute **sdsnEpStatus** has been set **toblocked**. Use the ClearPass API Explorer's Endpoint API, Managed Endpoint services by issuing the API **GET /endpoint/mac-address/{mac-address}** ,with **{mac-address}** of the endpoint obtained from the output of the active session query issued earlier.
- The **sdsnEpStatus** custom attribute can also be verified using ClearPass Policy Manager's Access Tracker.
  1. Click the session in the Access Tracker table to display the Request Details window with details about that session.
  2. Click the Input tab to show protocol-specific attributes that Policy Manager received in a transaction request.
  3. Scroll to view the **Endpoint:sdsnEpStatus** attribute. It's value should be **blocked**.

If it is not blocked, view the plug-in log for possible reasons. The plug-in log is located at `/srv/3rd-party-adapter/logs/plugin_server.log`.

## Unable to Quarantine Infected Endpoint

If you are unable to quarantine an infected endpoint, first validate the IP address of the infected host following the same procedure as in [“Unable to Block Infected Endpoint” on page 282](#). Verify that the value of the custom attribute `sdsnEpStatus` has been set to `quarantine`.

## Unable to Clear Blocked or Quarantined Endpoint

If you are unable to clear blocked or quarantined endpoints, it's usually because the passing IP address does not exist in the infected endpoint tracking database maintained by the plug-in. Infected hosts are located in the `/srv/3rd-party-adapter/infectedEndpointList` file. It is expected that a clear request will come with the same IP address of the endpoint as in the earlier blocked or quarantined endpoint request. If the clear request arrives with a new IP address that is not in the infected endpoint tracking database, the request fails.

Check the ClearPass application log for possible internal errors.

# 15

CHAPTER

## Migration Instructions for Spotlight Secure Customers

---

Moving From Spotlight Secure to Policy Enforcer | **286**

---

# Moving From Spotlight Secure to Policy Enforcer

## IN THIS SECTION

- [Spotlight Secure and Policy Enforcer Deployment Comparison | 286](#)
- [License Requirements | 287](#)
- [Sky ATP and Spotlight Secure Comparison Table | 287](#)
- [Migrating Spotlight Secure to a Policy Enforcer Configuration Overview | 288](#)
- [Installing Policy Enforcer | 289](#)
- [Configuring Advanced Threat Prevention Features: Spotlight Secure/Policy Enforcer Comparison | 295](#)

The Spotlight Secure Threat Intelligence Platform aggregates threat feeds from multiple sources to deliver open, consolidated, actionable intelligence to SRX Series Devices across an organization. This product is now superseded by the SDSN Policy Enforcer. The Juniper Software Defined Secure Network (SDSN) framework delivers enhanced security from external as well as internal attacks by leveraging both security as well as network devices as a coherent security system.

Policy Enforcer is an orchestration solution that orchestrates user intent policy enforcement for threat remediation as well as micro-segmentation across the entire network. This document talks about the logistics of migrating from Spotlight Secure to Policy Enforcer.

Spotlight Secure and Policy Enforcer with Sky ATP are two different platforms and therefore a direct migration of threat policies from Spotlight Secure to Policy Enforcer is not supported. Instead it is recommended that you remove Spotlight Connector from your Space Fabric and remove threat related configurations on Security Director before you install Policy Enforcer. Then you will need to reconfigure your data and threat feeds. The following sections provide an overview of the transition process from Spotlight Secure to Policy Enforcer with Sky ATP.

## Spotlight Secure and Policy Enforcer Deployment Comparison

The function of Spotlight Secure connector, to bring together all the available threat intelligence and make it available to security policies, is now done via Policy Enforcer with Sky ATP. In addition, Policy enforcer is a key part of the Software Defined Security Solution.

Spotlight Secure was installed to a separate virtual machine and then added as a specialized node to the Junos Space Fabric on Junos Space until version 15.1. Policy Enforcer is shipped as a virtual machine that

is deployed independently. Instead of adding the new VM as a Junos Space node, the configuration has been simplified with a workflow using the Security Director user interface.

**NOTE:** Spotlight Secure supported a HA deployment. The current version of Policy Enforcer is supported only as a single stand-alone deployment.

## License Requirements

For existing Spotlight Secure customers, no new additional license is needed. If you have a Spot-CC license, it can be used with Policy Enforcer and Sky ATP as well. A Policy Enforcer license would only be needed if you want to use the complete set of SDSN features with Sky ATP. SDSN/Policy Enforcer features includes all threat prevention types: C&C, infected hosts, malware, GeolP, and policy management and deployment features such as secure fabric and threat prevention policies. See [“Features By Sky ATP Configuration Type” on page 35](#) for more details.

## Sky ATP and Spotlight Secure Comparison Table

The following table provides a product comparison:

**Table 85: SKY ATP and Spotlight support Quick Summary**

Feature	Support in Spotlight Secure	Support with Policy Enforcer and Sky ATP	Workflow using Sky ATP, Security Director and Policy Enforcer
Command and Control Feed	Fully Supported	Fully Supported	<ul style="list-style-type: none"> <li>• Create a Realm in Sky ATP if you do not already have one</li> <li>• Configure Policy Enforcer in Cloud feed only or Sky ATP or Sky ATP with SDSN modes to connect to the realm</li> <li>• Configure a Threat Prevention Profile using Command and Control options</li> <li>• Use this Threat Prevention Profile in Firewall Policy</li> </ul>

Table 85: SKY ATP and Spotlight support Quick Summary (*continued*)

Feature	Support in Spotlight Secure	Support with Policy Enforcer and Sky ATP	Workflow using Sky ATP, Security Director and Policy Enforcer
Custom Feeds	Blocklist, Allowlist and Dynamic Address features are fully supported.	Blocklist, Allowlist, Infected Host, and Dynamic Address features are fully supported	<ul style="list-style-type: none"> <li>• Create a Realm in Sky ATP if you do not already have one</li> <li>• Configure Policy Enforcer Setting in Sky ATP mode</li> <li>• Create a Custom Feed using Blocklist, Allowlist or Dynamic address options selecting static IP or file options</li> </ul>
Infected Host	Not directly supported by Spotlight. You must create custom feeds	Sky ATP supports an Infected Host feed, natively integrated with Policy Enforcer and Security Director.	Sky ATP supports an Infected Host feed, natively integrated with Policy Enforcer and Security Director.
Infected Host Remediation at the Access Network level	Not supported using Spotlight and Security Director	<p>Sky ATP supports an Infected Host feed which is natively integrated with Policy Enforcer. Policy Enforcer can take block/quarantine actions at the access network level.</p> <p><b>NOTE:</b> This requires a Policy Enforcer license and does not come with a SPOT_CC license.</p>	Sky ATP supports an Infected Host feed which is natively integrated with Policy Enforcer. Policy Enforcer can take block/quarantine actions at the switch port level.

## Migrating Spotlight Secure to a Policy Enforcer Configuration Overview

In this section, there is a side by side comparison of feature configuration for Spotlight Secure on Security Director 15.1 and Policy Enforcer on Security Director 16.1 and higher to aid in re-configuring your threat policies.



This is an overview of the tasks needed to migrate:

1. Document the current data and feed configuration from current version of Security Director.
2. Remove Spotlight Connector from your Junos Space Fabric and remove the threat prevention configuration.
3. Upgrade to the latest versions of Junos Space and Security Director.

**NOTE:** Since the underlying operation system is upgraded to Centos6.8 on Junos Space version 16.1, first upgrade Junos Space and applications to 15.2R2 and then follow the documentation to restore the database before deploying 16.1 or higher. Please refer to the [Junos Space 16.1 release notes](#) for details.

4. Deploy the Policy Enforcer virtual machine. See instructions in the following section.
5. Deploy Security Director and install Policy Enforcer to Security Director.
6. Configure a Sky ATP realm and enroll SRX Series devices into the realm. For all deployment models, it is necessary to configure a Sky realm and enroll firewalls.
7. Configure feeds and threat policies.

## Installing Policy Enforcer

Policy Enforcer provides centralized, integrated management of all your security devices (both physical and virtual), allowing you to combine threat intelligence from different solutions and act on that intelligence from one management point. Using Policy Enforcer and the intelligence feeds it offers through Sky ATP, you can create threat prevention policies that provide monitoring and actionable intelligence for threat types such as known malware, command and control servers, infected hosts, and Geo IP-based server data.

Policy enforcer is shipped as a OVA file that should be deployed over VMware ESX.

1. Download the Policy Enforcer virtual machine OVA image from the Juniper Networks software [download page](#). It is recommended to deploy Policy Enforcer on the same ESX server as Junos Space.

**NOTE:** Do not change the name of the Policy Enforcer virtual machine image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Policy Enforcer virtual machine can fail.

Figure 68: Deploy Policy Enforcer OVF File 1

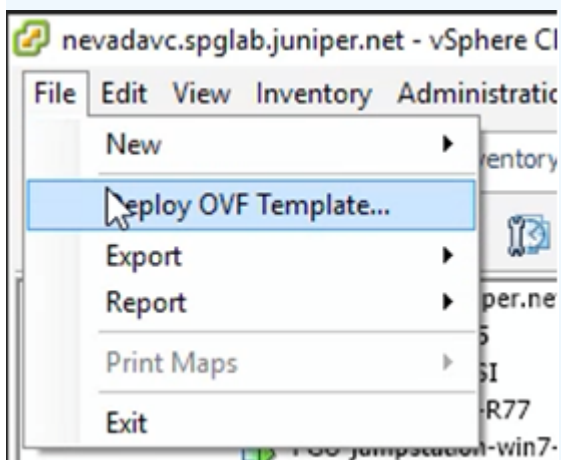
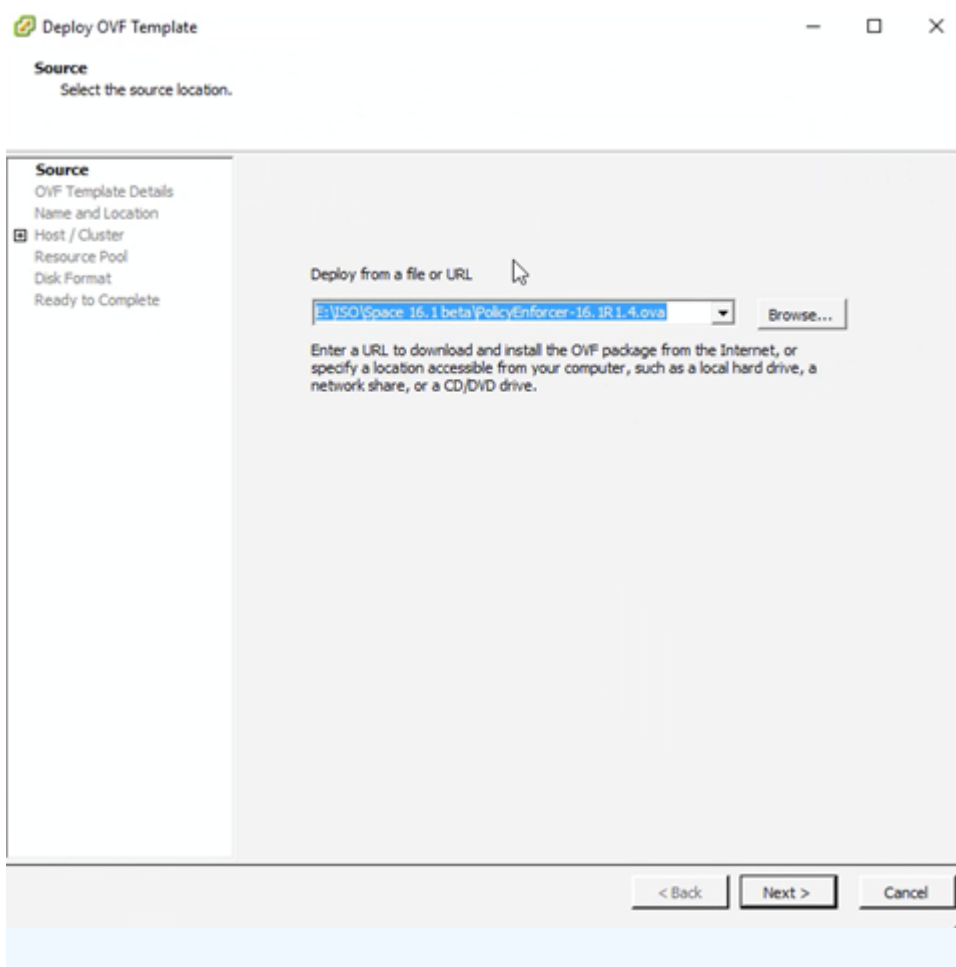


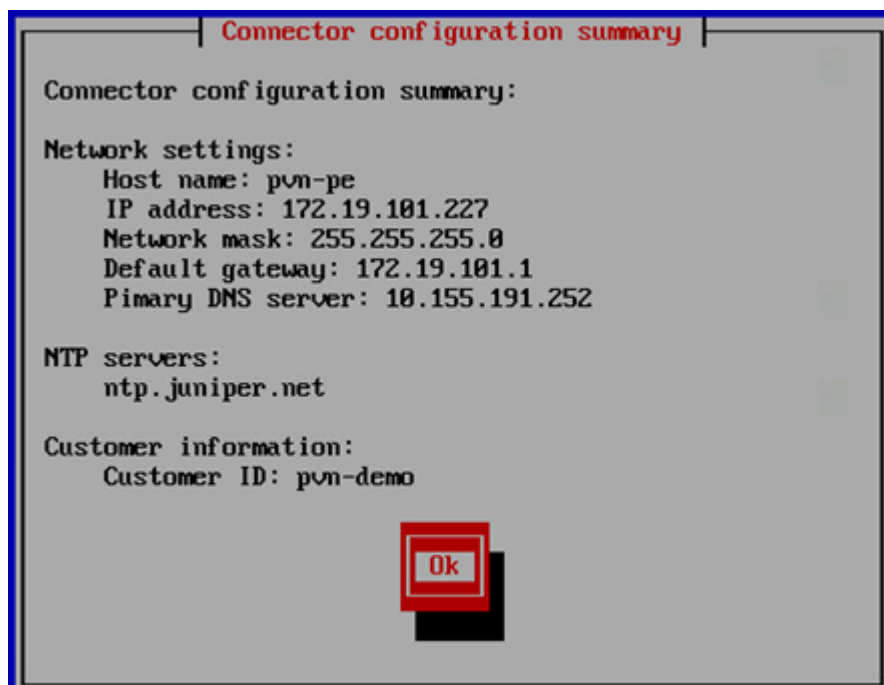
Figure 69: Deploy Policy Enforcer OVF File 2



**NOTE:** See [“Deploying and Configuring the Policy Enforcer with OVA files”](#) on page 42 for the complete Policy Enforcer installation documentation.

2. Initial configuration is done through the console. In addition to network and host configuration, you must set a customer ID and reset the root password. The default login to Policy Enforcer is Username: **root**, Password: **abc123**

Figure 70: Policy Enforcer Configuration Summary



3. Once Policy Enforcer is deployed, it must be added to Security Director via Security Director User Interface. From the Security Director UI, navigate to **Administration > Policy Enforcer > Settings**.

**NOTE:** Unlike Spotlight Secure, Policy Enforcer does not need to be added to Junos Space Fabric. The addition is done only through the Security Director UI.

4. On the Settings page, there three Sky ATP Configuration Types to choose from.
  - Sky ATP with SDSN—All Policy Enforcer features and threat prevention types are available
  - Sky ATP—All threat prevention types are available: Command and control server, Geo IP, and Infected hosts.
  - Cloud feeds only—Command and control server and Geo IP are the only threat prevention types available.
  - No selection (No Sky ATP)—You can choose to make no selection. When you make no selection, there are no feeds available from Sky ATP, but the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer are available. Infected hosts is the only prevention type available

**NOTE:** You can switch from Cloud feeds only to Sky ATP, or SKY ATP to SKY ATP with SDSN, but the reverse is not supported.

**NOTE:** If you upgrade from Cloud feeds only to Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention, and you must re-enroll them with Sky ATP. This is true for upgrading from Sky ATP to SKY ATP with SDSN. “SKY ATP with SDSN” is for the SDSN solution and not covered in this section.

**NOTE:** See [“Sky ATP Configuration Type Overview”](#) on page 32 for the Policy Enforcer documentation on this topic.

**NOTE:** Policy Enforcer with Sky ATP does not support a workflow for removing Policy Enforcer. To switch to a different Policy Enforcer, replace the IP and login information in the Policy Enforcer settings page.

## Configuring Advanced Threat Prevention Features: Spotlight Secure/Policy Enforcer Comparison

The following section is a side by side comparison of how advanced threat prevention features were configured on Spotlight Secure compared to how they are configured with Policy Enforcer.

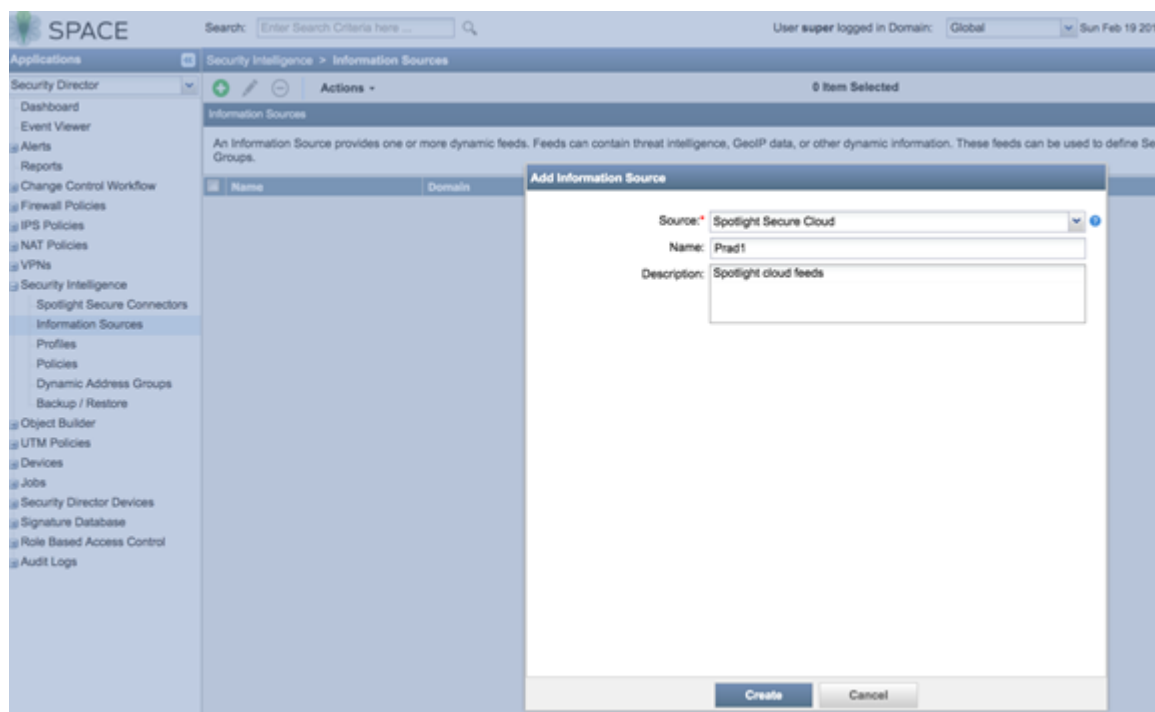
### Configuring Command and Control and Infected Host

## Spotlight Secure: C&C and Infected Host

This is how C&C and infected host feeds were configured on Security Director 15.1 with Spotlight Secure:

1. Under **Security intelligence > Information Source**, click + to add a new information source. Select **Spotlight Secure Cloud** as source.

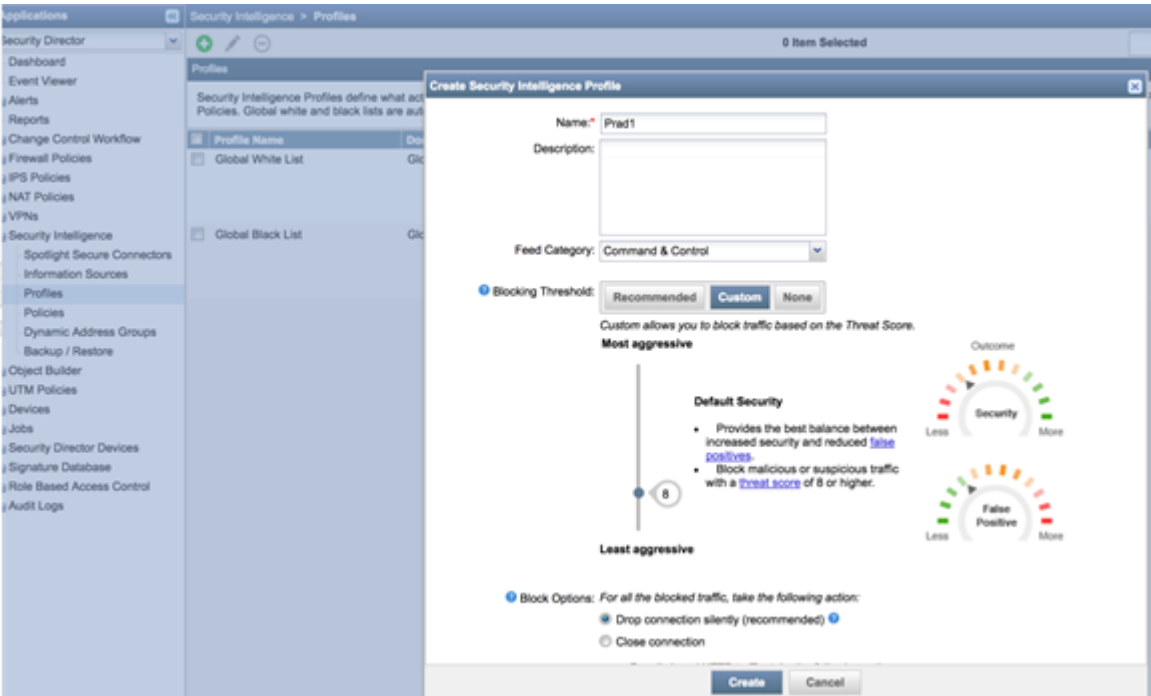
Figure 71: Spotlight Secure: Add Information Source



2. Create a Security Intelligence profile from **Security intelligence > Profiles**. Choose **Command and Control** as the feed category and set the Blocking threshold. Configure Block Options and Logging.

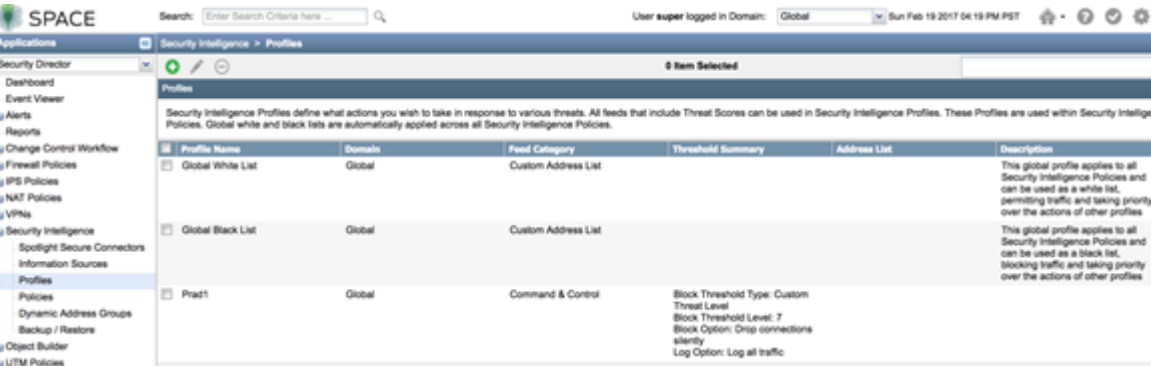


Figure 72: Spotlight Secure: Create Security Intelligence Profile



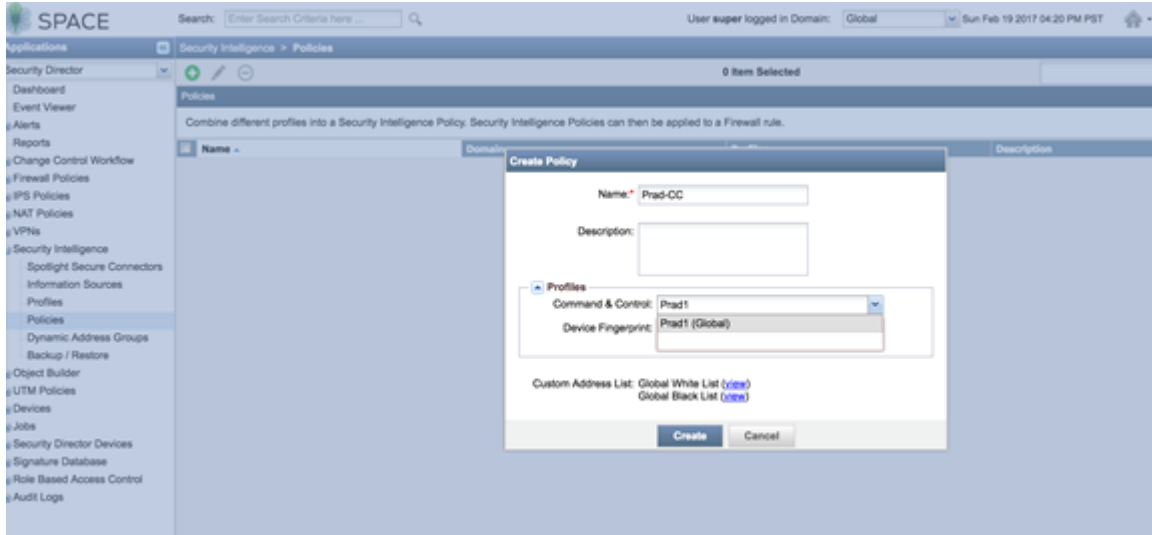
3. Complete the workflow to create a profile.

Figure 73: Spotlight Secure: Create Profile



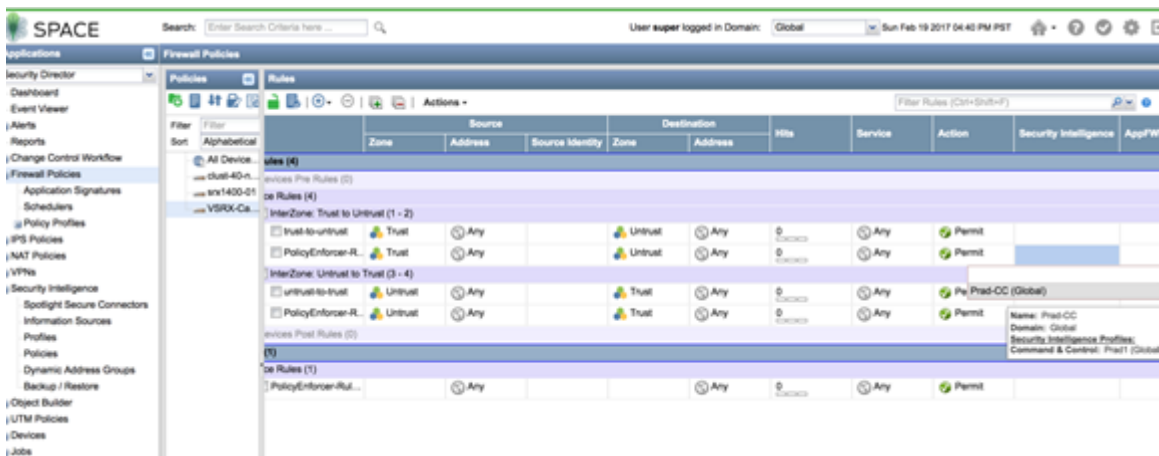
4. Create a security intelligence policy.

Figure 74: Spotlight Secure: Create Security Intelligence Policy



5. Apply the security intelligence policy to a firewall policy.

Figure 75: Spotlight Secure: Apply Security Intelligence Policy to Firewall Policy



## Policy Enforcer with Sky ATP: C&C and Infected Host

This is how C&C and infected host feeds are configured on Security Director 16.1 and higher with Policy Enforcer:

**NOTE:** Policy Enforcer can be configured with Sky ATP or Cloud feeds only to enable Command and Control feeds. The following instructions are for Cloud feeds only.

**NOTE:** In addition to the instructions provided here, Threat Prevention Guided Setup under **Configuration > Guided Setup > Threat Prevention** can be leveraged for a wizard driven workflow.

1. Configure a Sky ATP Realm by navigating to **Configure > Threat Prevention > Sky ATP Realms**. Click **+** to create a realm.

(You must have a Sky ATP account to configure a realm. If you do not have an account please click on the link provided in the Sky ATP Realm window to create one at the Sky ATP account page. See [“Creating Sky ATP Realms and Enrolling Devices or Associating Sites” on page 138](#) for details).

**NOTE:** You do not need a Sky ATP premium license to create an account or realm.

2. Once the Sky ATP realm is created, add a policy by navigating to **Configure > Threat Prevention > Policies**. Click **+** to create a policy. Enable the check box to **Include C&C profile in policy** and set threat score thresholds, actions, and logging.

Figure 76: Policy Enforcer: Create Threat Prevention Policy

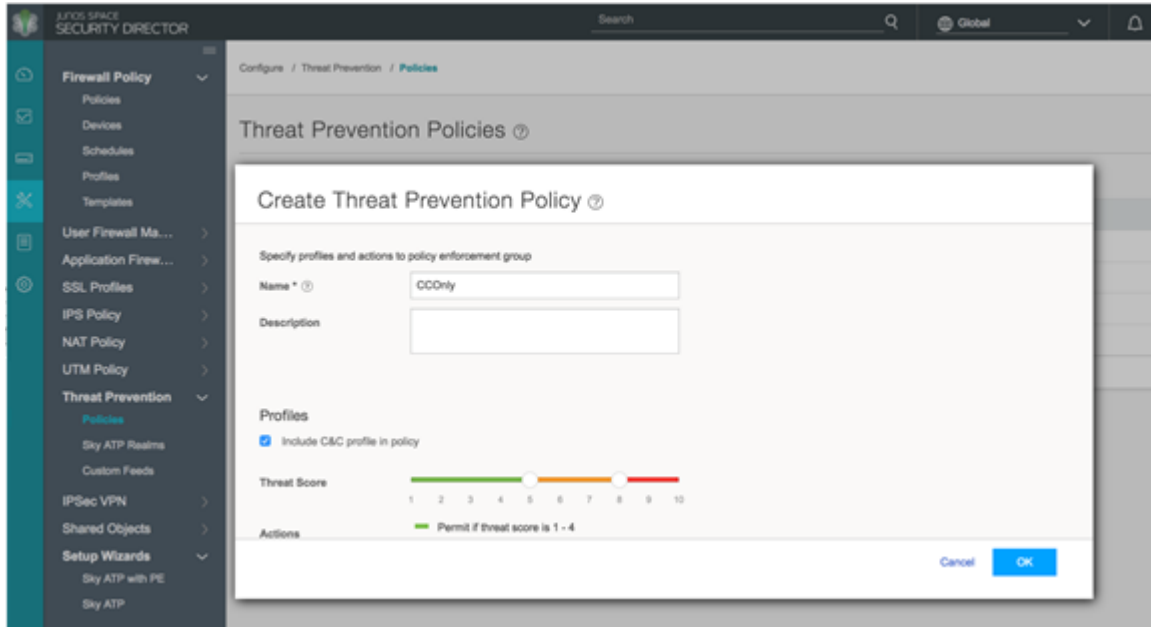
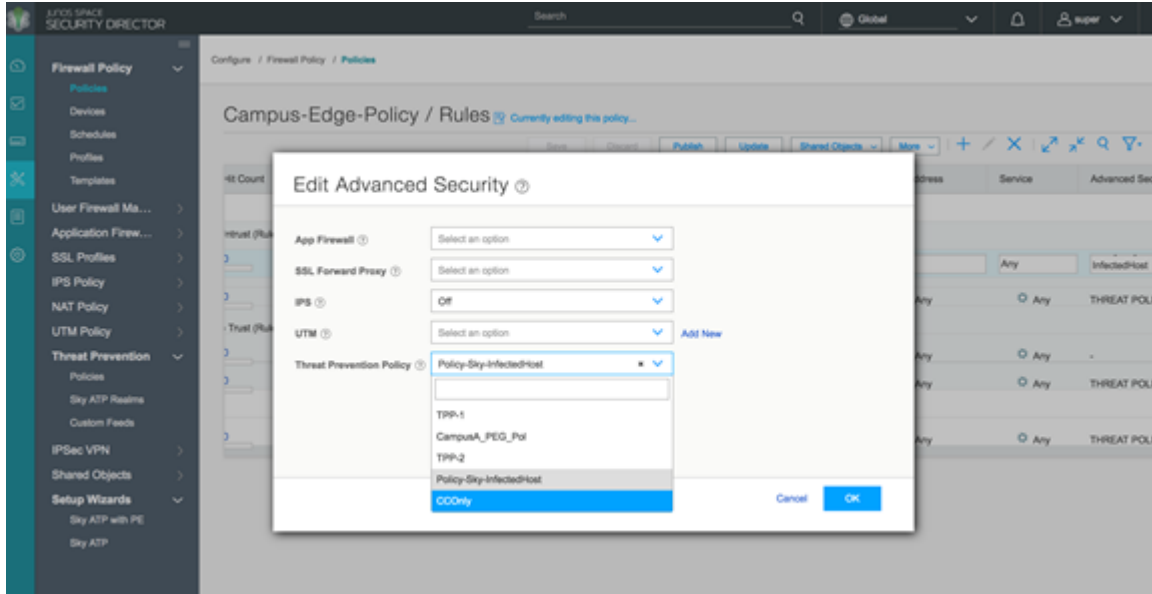


Figure 77: Policy Enforcer: Create Threat Prevention Policy, Select Threat Score and Logging



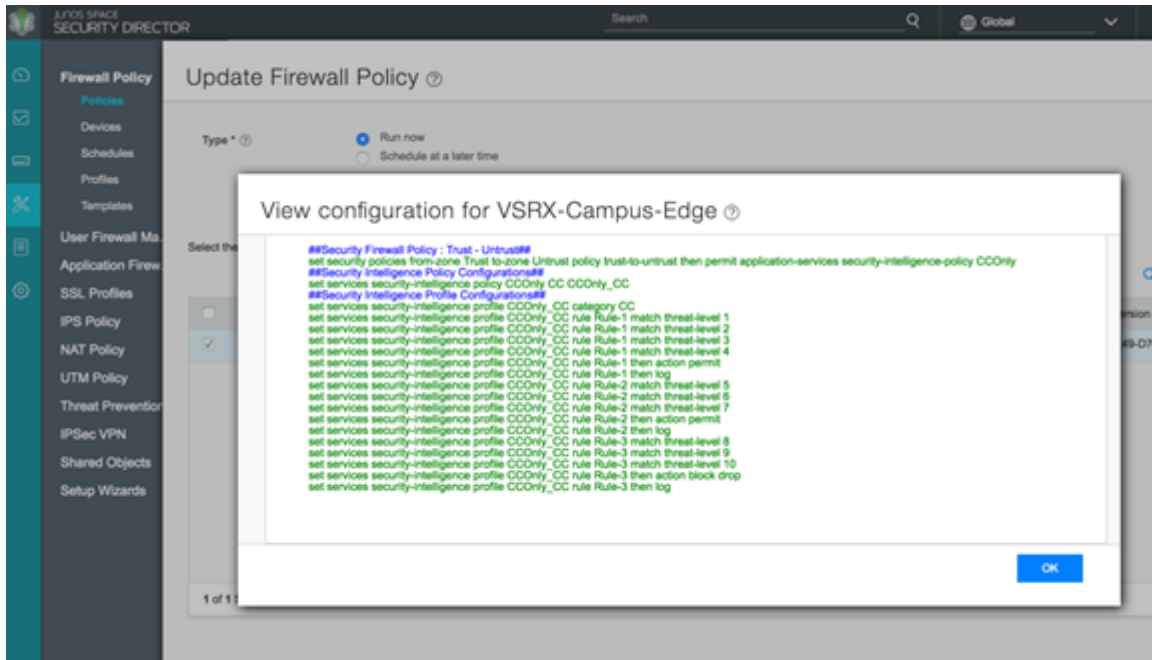
3. Apply the threat prevention policy to a firewall policy.

Figure 78: Policy Enforcer: Apply Threat Prevention Policy to Firewall Policy



4. Publish, verify the configuration and update to the firewall.

Figure 79: Policy Enforcer: Update Firewall Policy



**NOTE:** If Sky ATP is chosen as the Sky ATP Configuration Type under **Administration > Policy Enforcer > Settings**, the workflow remains the same, but additional parameters become available for configuring anti-malware.

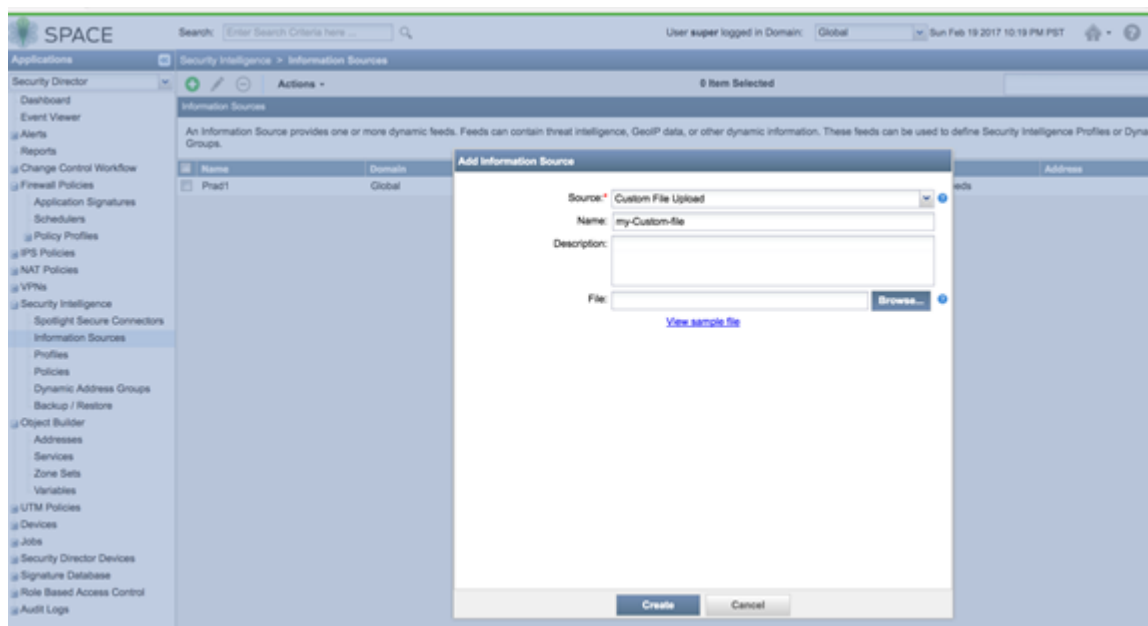
## Configuring Custom Feeds

### Spotlight Secure: Custom Feeds

This is how custom feeds were configured on Security Director 15.1 with Spotlight Secure:

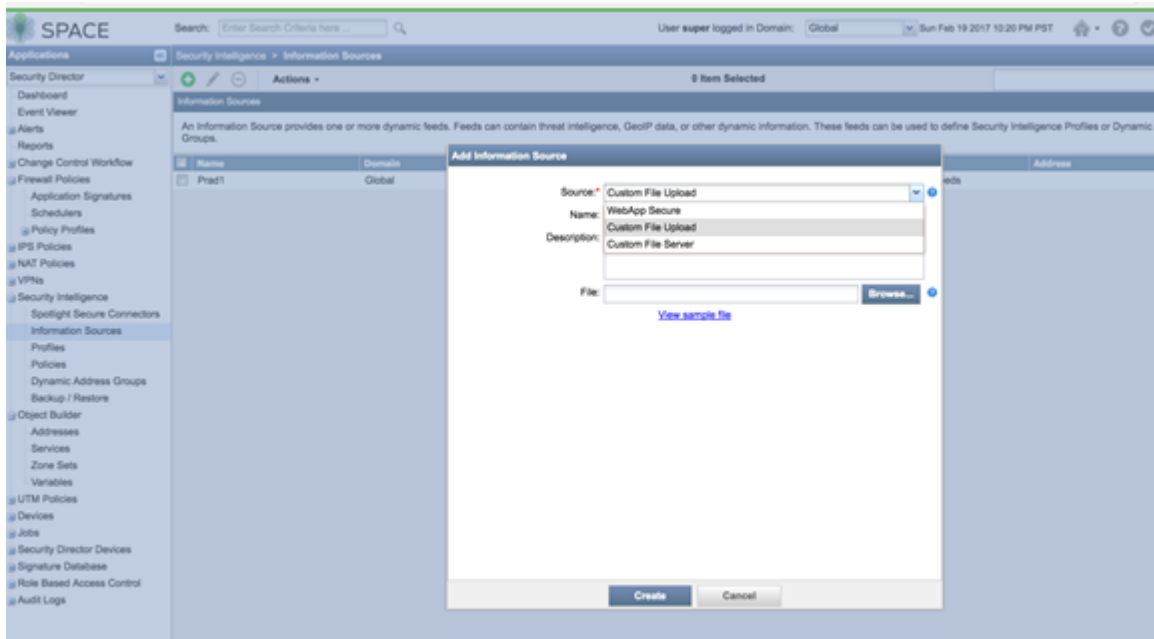
1. Create an information source by navigating to **Security Intelligence > Information Source**. Click + to add a source. (Note that WebApp Secure is no longer supported.)

Figure 80: Spotlight Secure: Add Information Source



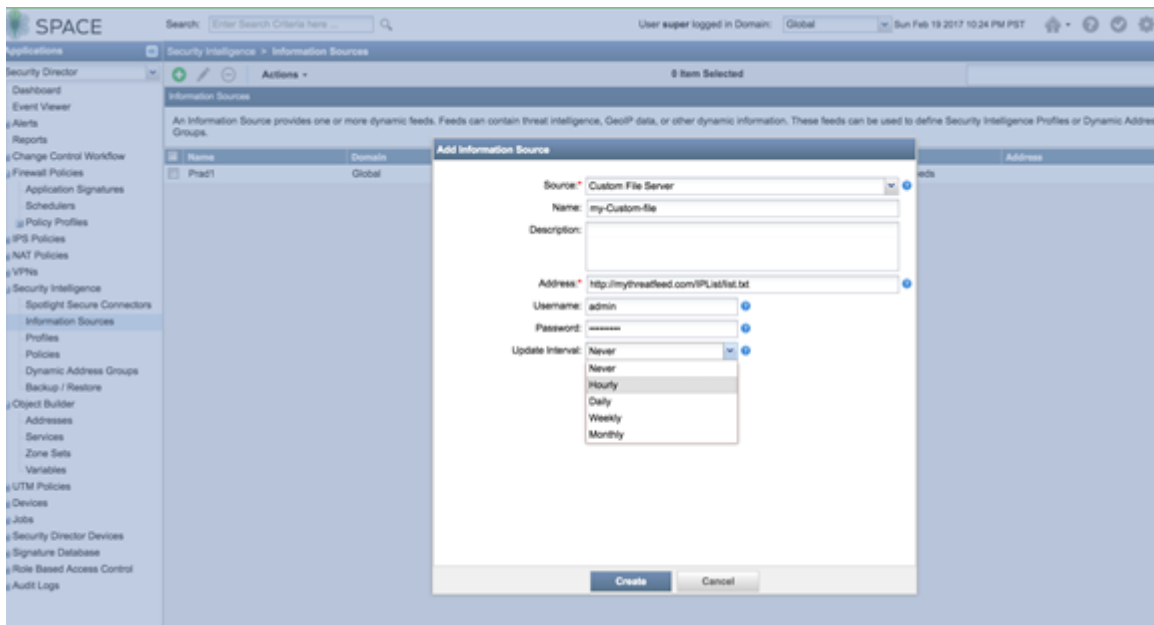
2. Upload from a custom file. Select **Source** as **Custom File Upload** and point to a local file.

Figure 81: Spotlight Secure: Configure Custom File Upload



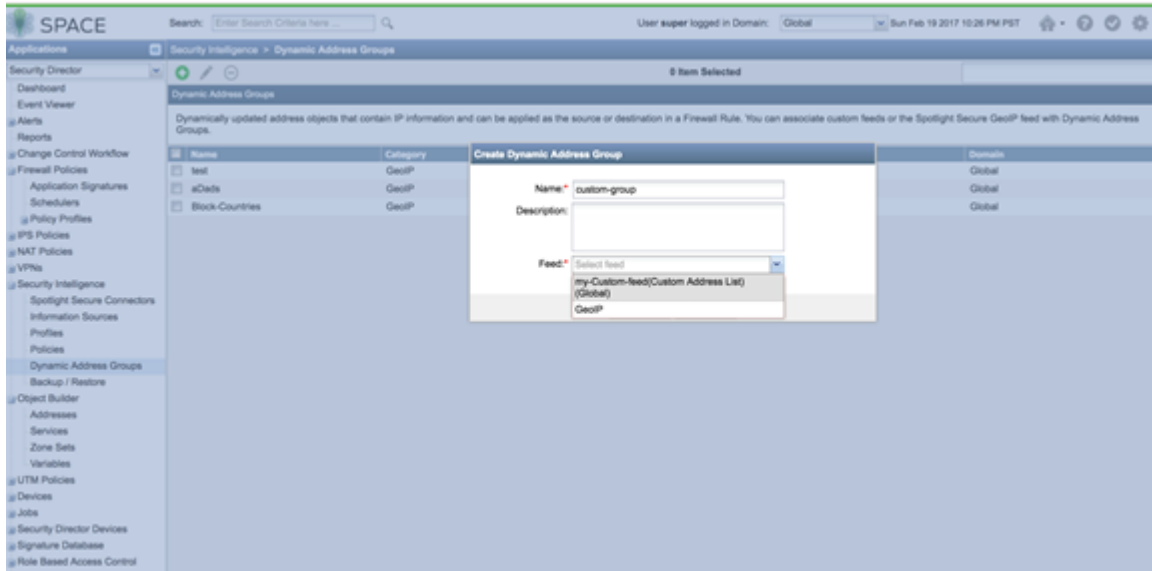
3. Configure a periodic upload from a remote file server. Provide the full URL to the plain text file you want to poll and enter server login information, **Username** and **Password**.

Figure 82: Spotlight Secure: Enter Server Login for Custom File Upload



4. Create a dynamic object by navigating to **Security Intelligence > Dynamic Address Group**. Configure the feed as the custom feed that was created in the previous step.

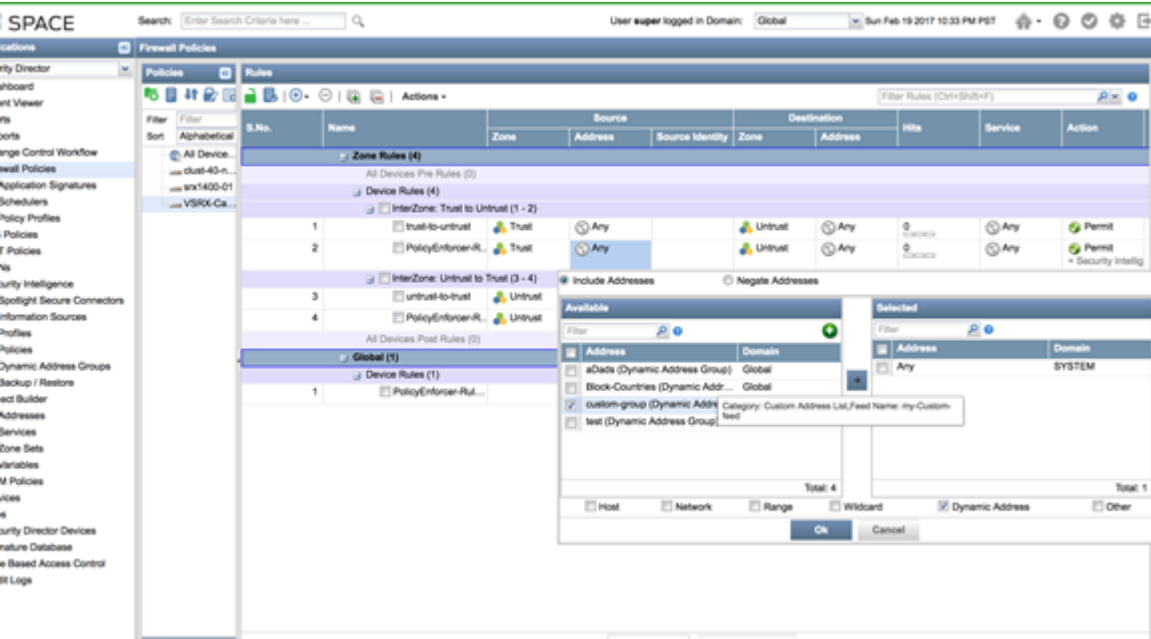
Figure 83: Spotlight Secure: Select Custom Feed in Dynamic Address Group



5. Use the dynamic object in a security policy.

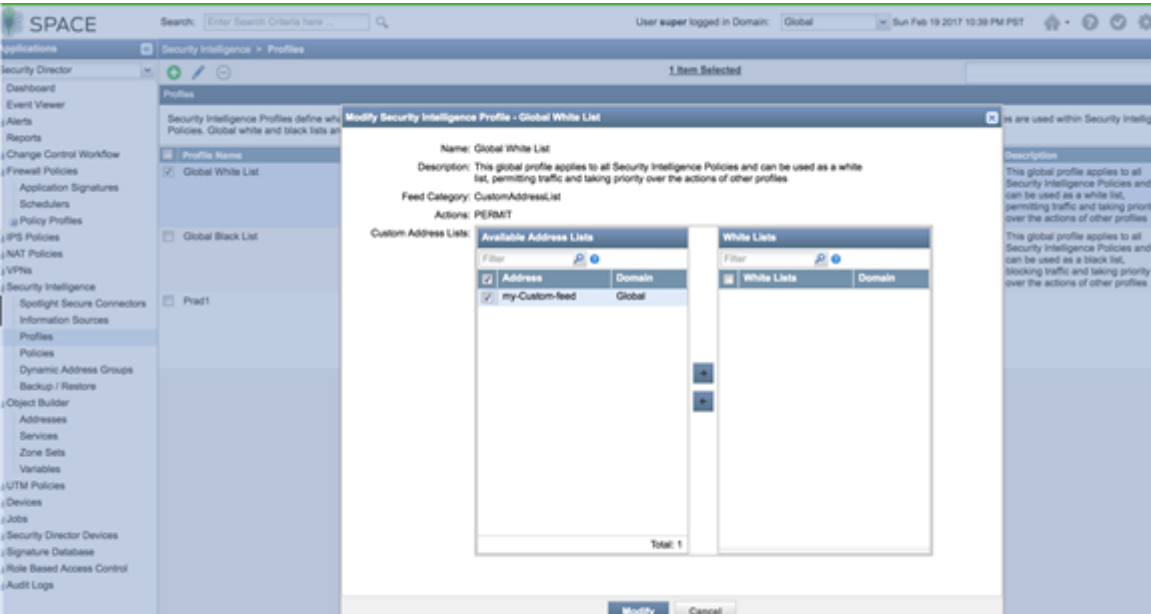


Figure 84: Spotlight Secure: Select Dynamic Address in Security Policy



6. Configure a custom feed as an allowlist or blocklist by navigating to **Security Intelligence > Profiles**. Edit **Global White List** or **Global Back List** to add a custom feed created in the previous steps.

Figure 85: Spotlight Secure: Edit Global Whitelist or Blacklist



## Policy Enforcer with Sky ATP: Custom Feeds

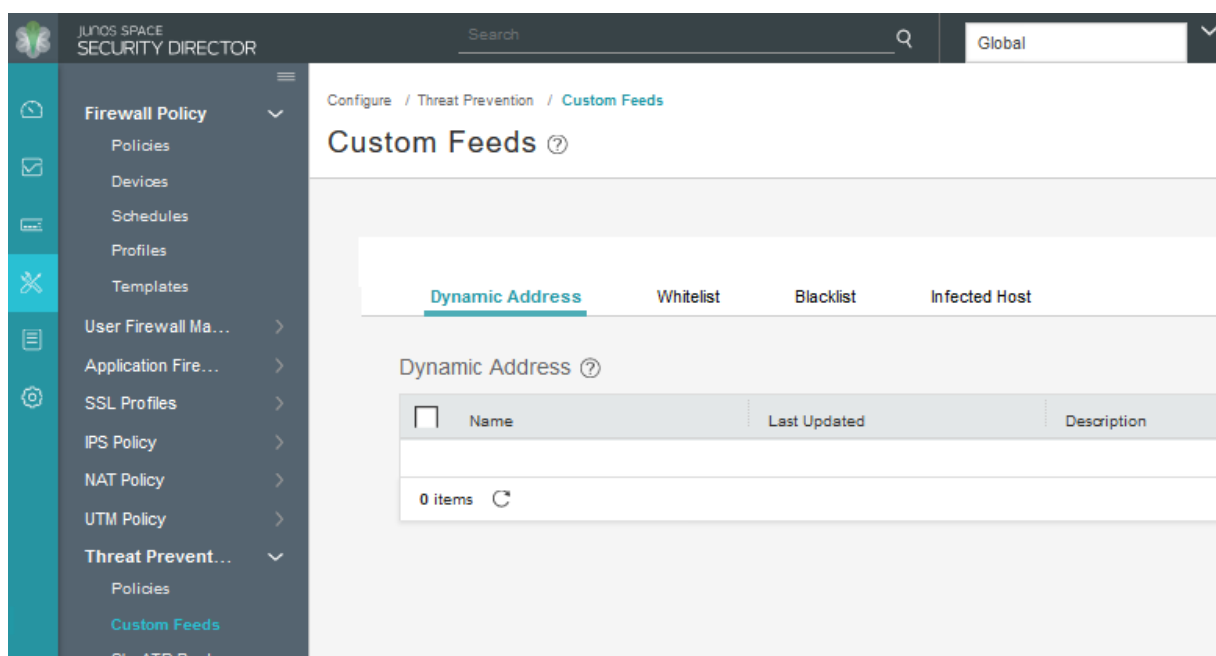
This is how custom feeds are configured on Security Director 16.1 and higher with Policy Enforcer:

**NOTE:** In addition to the instructions provided here, Threat Prevention Guided Setup under **Configuration > Guided Setup > Threat Prevention** can be leveraged for a wizard driven workflow.

Policy Enforcer supports manually adding or uploading custom feed information from a file server. The custom feed can be a dynamic object, infected hosts list, allowlist or blacklist which can then be used within the match criteria of a firewall rule.

1. Create Custom Feeds by navigating to **Configure > Threat Prevention > Custom Feeds**. Click + to create a new feed.
2. Provide a Name and Description for the custom feed and choose the tab for the type of feed: **Dynamic Address**, **Blacklist**, **Whitelist** or **Infected Host**.

Figure 86: Policy Enforcer: Configure Custom Feed



3. Manually configure the IP list or upload it from a local file. The IP list can be defined as individual IP addresses, IP address ranges, or subnets. See [“Creating Custom Feeds: Dynamic Address, Allowlist and Blocklist” on page 184](#) for complete details.

**NOTE:** Dynamic objects can be used within a firewall policy to match criteria as a source or destination address object.

**NOTE:** Policy Enforcer supports only cloud based C&C feeds and not custom C&C feeds. Policy Enforcer APIs can be used to extend this functionality.

4. Upload a local file. Select the **Upload file** option in the right corner of the page.

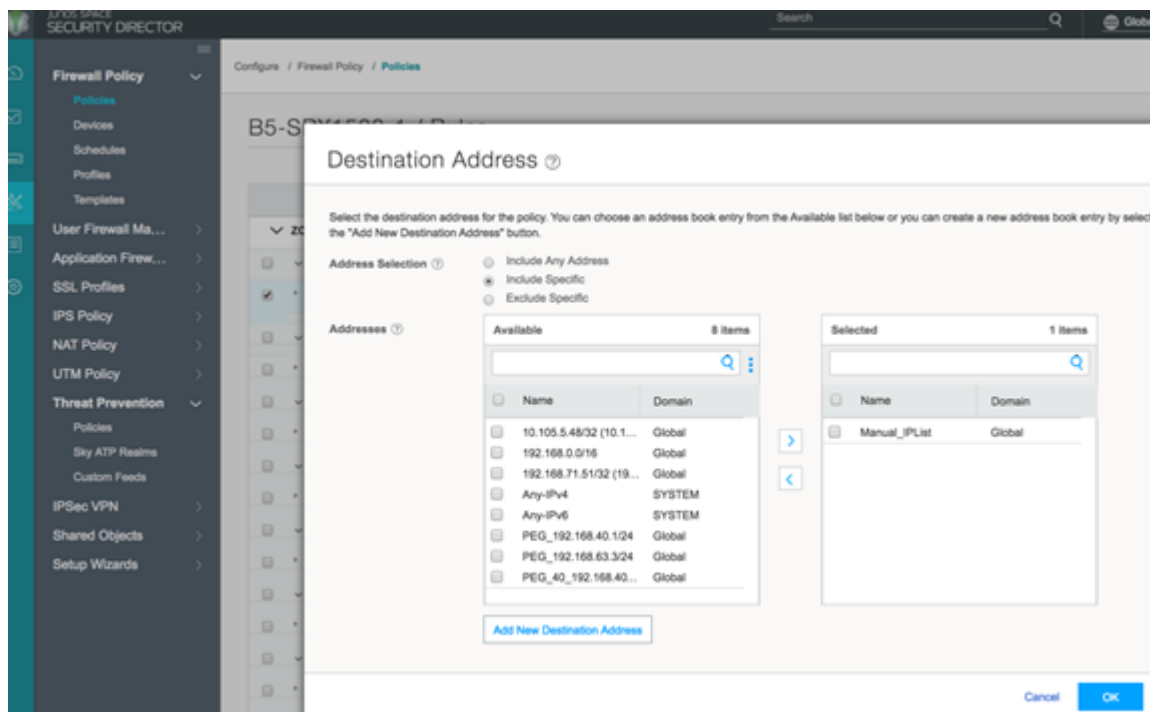
**Figure 87: Policy Enforcer: Upload Custom File**

The screenshot shows the 'Create Whitelist Feed' dialog box in the Policy Enforcer interface. The dialog has a title bar with a question mark icon. It contains the following fields and options:

- Name \***: A text input field containing 'manual\_Plist'.
- Description**: A text area with the placeholder text 'Write description...'.
- Feed Type \***: Three radio button options: 'IP, Subnet and Range', 'URL', and 'Domain'. The 'IP, Subnet and Range' option is selected.
- Custom List \***: A section with a header 'Item' and a table below it. The table has one row with the text 'Data is not available'.
- Buttons**: An 'Upload file' button with a plus icon, a pencil icon, and an 'X' icon are located in the top right corner of the dialog. At the bottom right, there are 'Cancel' and 'OK' buttons.

5. If you have configured an allowlist, downloads from those IP addresses are considered trusted. For blocklists, all downloads from those IP addresses are blocked. Dynamic objects can be used within a firewall policy match criteria as a source or destination address object.

Figure 88: Policy Enforcer: Use Dynamic Addresses in Firewall Policy



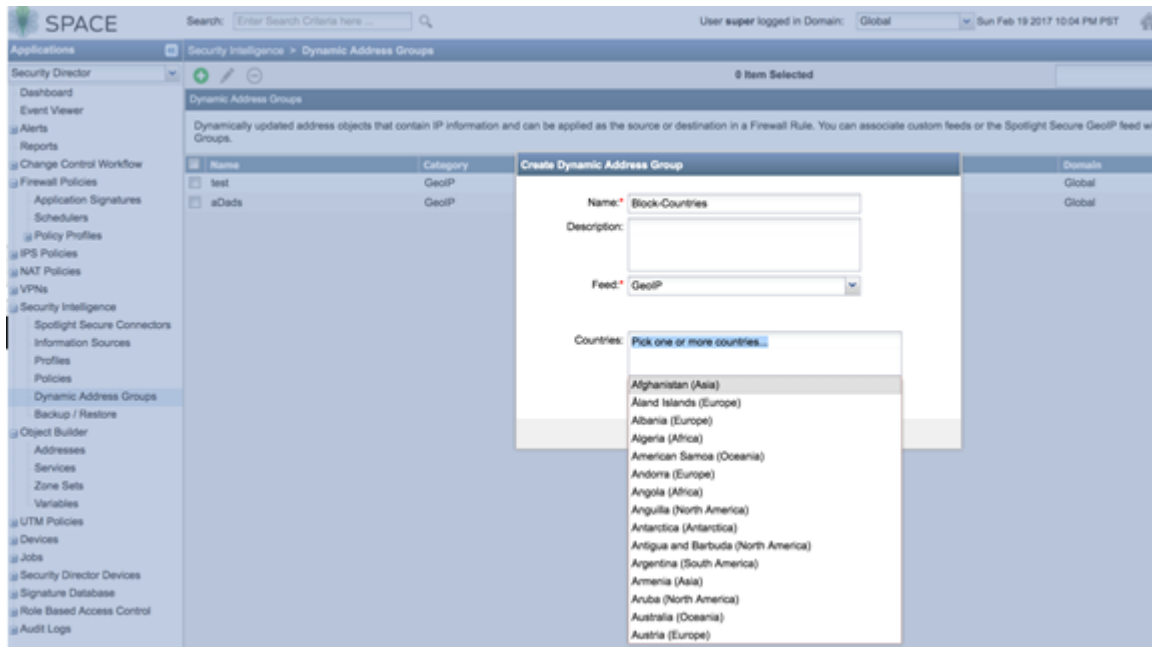
## Configuring Geo IP

### Spotlight Secure: Geo IP

This is how Geo IP feeds were configured on Security Director 15.1 with Spotlight Secure:

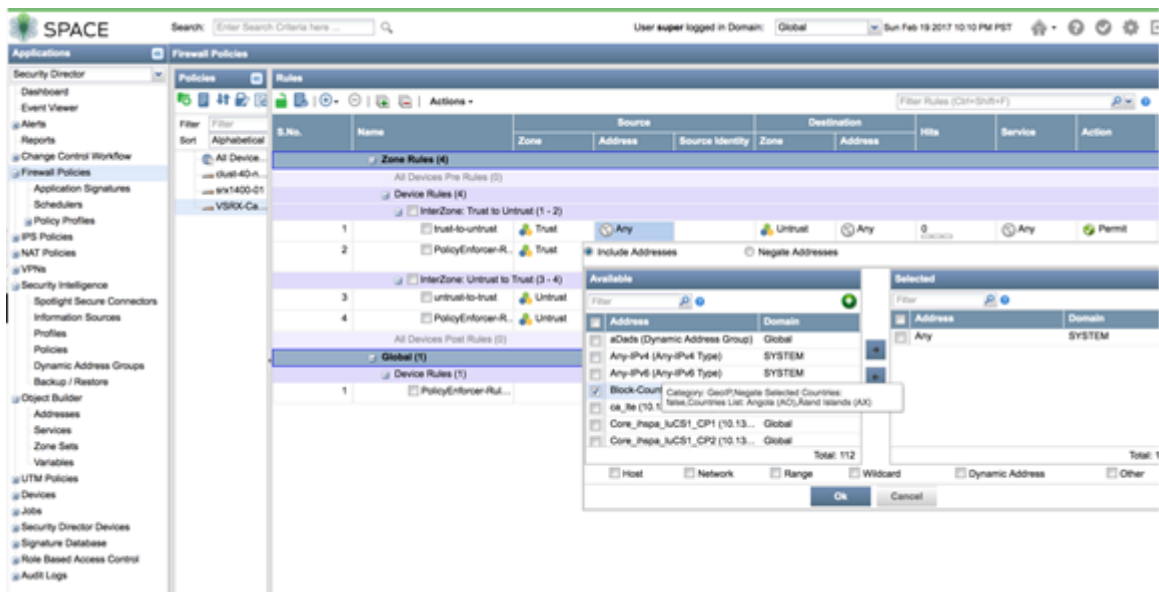
1. Create a GeoIP object under dynamic object by navigating to **Security Intelligence > Dynamic Address Group**. Select the feed as **GeoIP** and pick the countries from the drop down list.

Figure 89: Spotlight Secure: Create Geo IP with Dynamic Address Group



2. Use the Geo IP object in a firewall policy.

Figure 90: Spotlight Secure: Use Geo IP in Firewall Policy

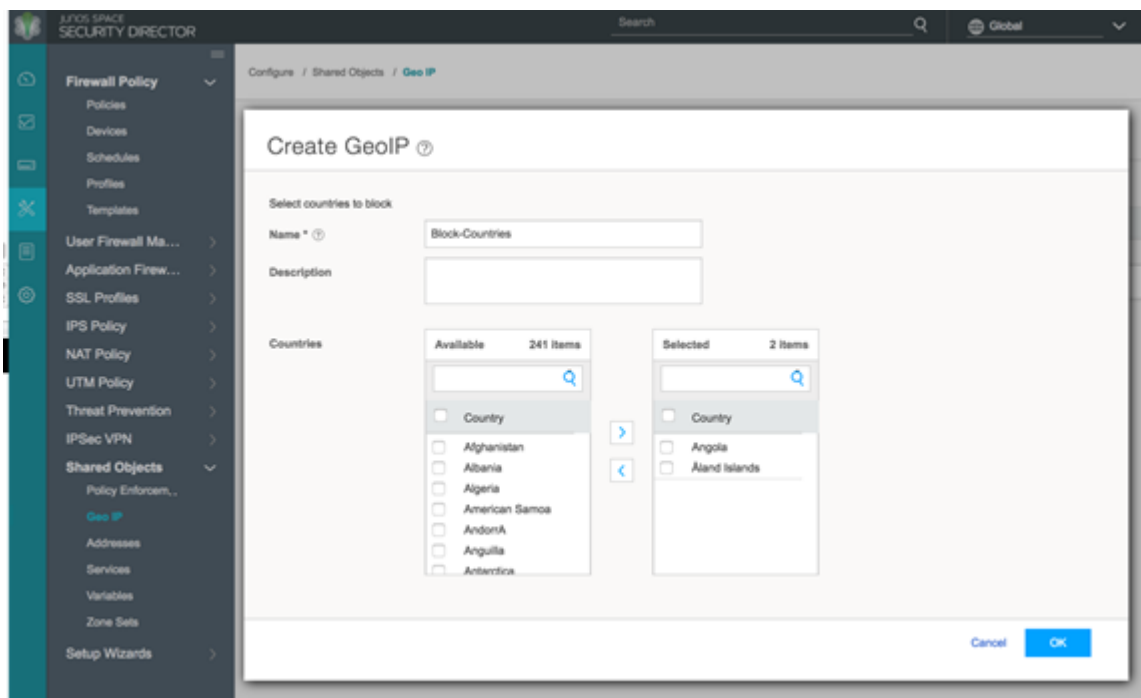


## Policy Enforcer with Sky ATP: Geo IP

This is how Geo IP feeds are configured on Security Director 16.1 and higher with Policy Enforcer:

1. Define GeoIP objects that can then be used within the match criteria of a firewall policy by navigating to **Configure > Shared Objects > Geo IP**. Create a Geo IP feed and choose countries to include from the list.(This feature requires a SecIntel or SKY ATP license.)

Figure 91: Policy Enforcer: Create Geo IP



2. Use the Geo IP feed you created as the source or destination address in a firewall policy.

Figure 92: Policy Enforcer: Use Geo IP in the Firewall Policy

