Security Director Policy Enforcer
Copyright © 2017 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 http://www.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 ................................................. xi
  Documentation and Release Notes ................................ xi
  Supported Platforms .................................................. xi
  Documentation Conventions ....................................... xi
  Documentation Feedback ........................................... xiii
  Requesting Technical Support .................................... xiv
  Self-Help Online Tools and Resources ........................... xiv
  Opening a Case with JTAC ........................................... xiv

Chapter 1  Overview of Policy Enforcer and Sky ATP ............. 17
  Policy Enforcer Overview ......................................... 17
  Supported Topologies .............................................. 18
  Benefits of Policy Enforcer ....................................... 19
    User Intent-Based Policy ........................................ 21
  Policy Enforcer Components ..................................... 21
  Sky ATP Features .................................................. 26
  Comparing the SDSN and non-SDSN Configuration Steps ....... 26

Chapter 2  Installing Policy Enforcer ............................... 29
  Policy Enforcer Installation Overview ............................ 29
  Deploying and Configuring the Policy Enforcer Virtual Machine .... 31
  Identifying the Policy Enforcer Virtual Machine In Security Director .... 36
  Obtaining a Sky ATP License ...................................... 37
  Creating a Sky ATP Cloud Web Portal Login Account ............ 38
  Loading a Root CA ................................................ 39
  Upgrading Your Policy Enforcer Software ....................... 40

Chapter 3  Configuring Policy Enforcer Settings (Required for Sky ATP, Policy
Enforcer, and Cloud Feeds) ........................................... 43
  Policy Enforcer Settings ......................................... 43
  Policy Enforcer Connector Overview ............................... 45
  ClearPass Configuration for Third-Party Switches ................ 46
  Creating a Policy Enforcer Connector for Third-Party Switches .... 52

Chapter 4  Guided Setup for Sky ATP with SDSN .................... 55
  Using Guided Setup for Sky ATP with SDSN ..................... 55

Chapter 5  Guided Setup for Sky ATP ................................ 59
  Using Guided Setup for Sky ATP ................................ 59

Copyright © 2017, Juniper Networks, Inc.
Chapter 6  Configuring Policy Enforcer (without Guided Setup) ................. 61
  Configuring Sky ATP with SDSN (Without Guided Setup) Overview .......... 62
  Creating Sky ATP Realms and Enrolling Devices or Associating Sites ....... 63
  Secure Fabric Overview ........................................ 65
  Creating Secure Fabric and Sites ................................ 65
  Editing or Deleting a Secure Fabric ................................ 67
  Policy Enforcement Groups Overview ................................ 67
  Creating Policy Enforcement Groups ................................ 67
  Threat Prevention Policy Overview ................................ 68
  Creating Threat Prevention Policies ................................ 69
  Threat Policy Analysis Overview ................................ 73
  Geo IP Overview .................................................. 73
  Creating Geo IP Policies .......................................... 73

Chapter 7  Configuring Sky ATP (without Guided Setup) ......................... 77
  Configuring Sky ATP (No SDSN and No Guided Setup) Overview .......... 77
  Sky ATP Realm Overview ......................................... 78
  Creating Sky ATP Realms and Enrolling Devices or Associating Sites .... 79
  Threat Prevention Policy Overview ................................ 80
  Creating Threat Prevention Policies ................................ 81

Chapter 8  Configuring Cloud Feeds Only ..................................... 87
  Configuring Cloud Feeds Only ..................................... 87

Chapter 9  Threat Prevention - Configure .................................... 89
  Creating Sky ATP Realms and Enrolling Devices or Associating Sites ... 89
  Sky ATP Realm Overview ......................................... 91
  Custom Feed Sources Overview .................................... 91
  Creating Custom Feeds, Dynamic, Black and White ....................... 92
  Creating Custom Feeds, Infected Host ................................ 95
  Sky ATP Email Management Overview ................................ 97
  Sky ATP Email Management: SMTP Settings ................................ 98
  Sky ATP Email Management: Whitelists and Blacklists ...................... 101
  Sky ATP Malware Management Overview ................................ 101
  File Inspection Profiles Overview .................................. 102
  Creating File Inspection Profiles ................................... 103
  Creating Whitelists and Blacklists .................................. 104

Chapter 10  Threat Prevention - Monitor ..................................... 107
  Policy Enforcer Dashboard Widgets .................................. 107
  Infected Hosts Overview ........................................... 108
  Infected Host Details ................................................ 109
  Command and Control Servers Overview ................................ 110
  Command and Control Server Details .................................. 111
  HTTP File Download Overview ...................................... 113
  HTTP File Download Details ........................................ 114
    File Summary ....................................................... 115
    HTTP Downloads ..................................................... 115
  SMTP Quarantine Overview ........................................ 116
  Email Attachments Scanning Overview ................................ 118
## Table of Contents

### Chapter 11  Troubleshooting
- Email Attachments Scanning Details ........................................ 119
- File Summary ................................................................. 119
- File Scanning Limits ....................................................... 120
- **Troubleshooting** .......................................................... 123
  - Policy Enforcer Log File Locations .................................... 123
  - Troubleshooting Common Policy Enforcer Problems .............. 124
  - Troubleshooting Policy Enforcer Installation ...................... 124
  - Troubleshooting Sky ATP Realms and Enrolling Devices .......... 124
  - Troubleshooting Threat Policies and Policy Enforcement Groups . 125
  - HTTPS-Based Malware Not Detected ................................. 125
# List of Figures

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Overview of Policy Enforcer and Sky ATP</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Figure 1: Comparing Traditional SRX Customers to Policy Enforcer Customers</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Figure 2: Perimeter-Defined Security Model</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Figure 3: Policy Enforcer and Software-Defined Security Model</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Figure 4: Components of the Policy Enforcer Deployment Model</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Figure 5: Blocking an Infected Endpoint</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Figure 6: Tracking Infected Endpoint Movement</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Figure 7: Third-Party Switch Support</td>
<td>25</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Installing Policy Enforcer</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Figure 8: Defining the Basic Network Configuration Settings</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Figure 9: Prompt for Configuring the NTP Servers</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Figure 10: Configuring the NTP Servers</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Figure 11: Entering Customer Information</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Figure 12: Changing the Root Password</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Figure 13: Reviewing and Changing Your Configuration Settings</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Figure 14: Reviewing Your Configuration Settings</td>
<td>35</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Configuring Policy Enforcer Settings (Required for Sky ATP, Policy Enforcer, and Cloud Feeds)</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Figure 15: ClearPass API Client Operator Profile Minimum Privileges</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Figure 16: ClearPass Edit API Client</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Figure 17: ClearPass Edit Attribute</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Figure 18: ClearPass Enforcement Profile: Quarantine</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Figure 19: ClearPass Enforcement Profile: Terminate</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Figure 20: ClearPass Enforcement Policy</td>
<td>51</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Threat Prevention - Configure</td>
<td>89</td>
</tr>
<tr>
<td></td>
<td>Figure 21: Email Management Overview</td>
<td>98</td>
</tr>
</tbody>
</table>
# List of Tables

- **About the Documentation** .............................................. xi
- Table 1: Notice Icons .......................................................... xii
- Table 2: Text and Syntax Conventions .................................... xii

**Chapter 1** Overview of Policy Enforcer and Sky ATP ............................. 17
- Table 3: Comparing the SDSN Configuration Steps to the non-SDSN Configuration Steps ................................................................. 26

**Chapter 2** Installing Policy Enforcer ........................................... 29
- Table 4: Overview of Steps to Install and Configure Policy Enforcer ........ 30

**Chapter 3** Configuring Policy Enforcer Settings (Required for Sky ATP, Policy Enforcer, and Cloud Feeds) ........................................ 43
- Table 5: Connectors Information- Main Page ................................ 45
- Table 6: Fields on the Policy Enforcement Connectors Page ................ 53

**Chapter 6** Configuring Policy Enforcer (without Guided Setup) ................... 61
- Table 7: Fields on the Add Sky ATP Realm Page ........................... 63
- Table 8: Fields on the Create Site Page ..................................... 66
- Table 9: Fields on the Sites Main Page ....................................... 66
- Table 10: Fields on the Policy Enforcement Group Page ................... 68
- Table 11: Fields on the Threat Prevention Policy Page ..................... 70
- Table 12: Fields on the Geo IP Policy Page .................................. 74

**Chapter 7** Configuring Sky ATP (without Guided Setup) ........................... 77
- Table 13: Fields on the Add Sky ATP Realm Page ........................... 79
- Table 14: Fields on the Threat Prevention Policy Page ..................... 82

**Chapter 9** Threat Prevention - Configure ........................................ 89
- Table 15: Fields on the Add Sky ATP Realm Page ........................... 90
- Table 16: Custom Feed Categories ........................................... 93
- Table 17: Fields on the Custom Feeds Page, Feeds with Local Files ........ 93
- Table 18: Fields on the Custom Feeds Page, Feeds with Remote File Server .. 94
- Table 19: Fields on the Custom Feeds Page, Feeds with Local Files ........ 96
- Table 20: Fields on the Custom Feeds Page, Feeds with Remote File Server .. 96
- Table 21: Configure Quarantine Malicious Messages ......................... 99
- Table 22: Configure Deliver with Warning Headers ........................ 100
- Table 23: Permit .................................................................... 100
- Table 24: File Category Contents ............................................. 102
- Table 25: File Category Contents ............................................. 103
- Table 26: Whitelist and Black Syntax ........................................ 105

**Chapter 10** Threat Prevention- Monitor ........................................... 107
Table 27: Sky ATP Dashboard Widgets ........................................... 108  
Table 28: Threat Level Definitions ............................................ 109  
Table 29: Command & Control Server Data Fields ....................... 111  
Table 30: Command & Control Server Contacted Host Data ........... 112  
Table 31: HTTP Scanning Data Fields ....................................... 113  
Table 32: General Summary Fields ......................................... 115  
Table 33: Blocked Email Summary View ................................. 116  
Table 34: Blocked Email Detail View ...................................... 116  
Table 35: Email Attachments Scanning Data Fields .................... 118  
Table 36: General Summary Fields ......................................... 119
About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiv

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 http://www.juniper.net/techpubs/.

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 http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- JA2500

Documentation Conventions

Table 1 on page xii defines notice icons used in this guide.
Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![i]</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![!]</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>![W]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>![L]</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td>![T]</td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td>![B]</td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

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

Table 2: Text and Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the <code>configure</code> command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>user@host&gt; configure</code></td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td><code>user@host&gt; show chassis alarms</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No alarms currently active</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>• Introduces or emphasizes important new terms.</td>
<td>• A policy term is a named structure that defines match conditions and actions.</td>
</tr>
<tr>
<td></td>
<td>• Identifies guide names.</td>
<td>• <em>Junos OS CLI User Guide</em></td>
</tr>
<tr>
<td></td>
<td>• Identifies RFC and Internet draft titles.</td>
<td>• RFC 1997, <em>BGP Communities Attribute</em></td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine’s domain name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>[edit]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>root@# set system domain-name domain-name</code></td>
</tr>
</tbody>
</table>
### Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| **Text like this**          | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | • To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.  
• The console port is labeled CONSOLE. |
| < > (angle brackets)        | Encloses optional keywords or variables.                                    | stub <default-metric metric>;                                             |
| | (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. | broadcast | multicast  
(string1 | string2 | string3) |
| # (pound sign)              | Indicates a comment specified on the same line as the configuration statement to which it applies. | rsvp [ # Required for dynamic MPLS only |
| [ ] (square brackets)       | Encloses a variable for which you can substitute one or more values.         | community name members [community-ids ] |
| Indention and braces ( { } ) | Identifies a level in the configuration hierarchy.                           | [edit ]  
route default {  
static {  
nexthop address;  
retain;  
}  
}  
}| |
| : (semicolon)              | Identifies a leaf statement at a configuration hierarchy level.              | |

**GUI Conventions**

| **Bold text like this** | Represents graphical user interface (GUI) items you click or select.          | • In the Logical Interfaces box, select All Interfaces.  
• To cancel the configuration, click Cancel. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; (bold right angle bracket)</td>
<td>Separates levels in a hierarchy of menu selections.</td>
<td>In the configuration editor hierarchy, select Protocols&gt;Osfp.</td>
</tr>
</tbody>
</table>

**Documentation Feedback**

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- **Online feedback rating system**—On any page of the Juniper Networks TechLibrary site at [http://www.juniper.net/techpubs/index.html](http://www.juniper.net/techpubs/index.html), simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience.  
Alternately, you can use the online feedback form at [http://www.juniper.net/techpubs/feedback/](http://www.juniper.net/techpubs/feedback/).
• E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

**Requesting Technical Support**

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.


• Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.

• JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

**Self-Help Online Tools and Resources**

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

• Find CSC offerings: http://www.juniper.net/customers/support/

• Search for known bugs: http://www2.juniper.net/kb/

• Find product documentation: http://www.juniper.net/techpubs/

• Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/

• Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/

• Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/

• Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/

• Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

**Opening a Case with JTAC**

You can open a case with JTAC on the Web or by telephone.

• Use the Case Management tool in the CSC at http://www.juniper.net/cm/.

• Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).
For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.
CHAPTER 1

Overview of Policy Enforcer and Sky ATP

- Policy Enforcer Overview on page 17
- Benefits of Policy Enforcer on page 19
- Policy Enforcer Components on page 21
- Sky ATP Features on page 26
- Comparing the SDSN and non-SDSN Configuration Steps on page 26

Policy Enforcer Overview

Policy Enforcer provides centralized, integrated management of all your security devices (both physical and virtual), 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. It works with cloud-based Sky Advanced Threat Prevention (Sky ATP) to protect both 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 firewall, the file can be sent to the Sky ATP cloud for malware inspection (depending on your configuration settings.) 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.

Policy Enforcer provides the following:

- Pervasive Security—Combine security features and intelligence from devices across your network, including switches, routers, firewalls, to create a “secure fabric” that leverages information you can use to create policies that address threats in real-time and into the future. With monitoring capabilities, it can also act as a sensor, providing visibility for intra- and inter-network communications.

- 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.
• Threat Intelligence Aggregation—Gather threat information from multiple locations and devices, both physical and virtual, as well as third party solutions.

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

Related Documentation

• Benefits of Policy Enforcer on page 19
• Policy Enforcer Components on page 21
• Sky ATP Features on page 26
Benefits of Policy Enforcer

Most enterprise computer security revolves around creating a wall around the perimeter of an organization. See Figure 2 on page 19.

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 20, 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.

User Intent-Based Policy

Generally speaking, with rule-based policies, you manage clients based on IP addresses. There may be one rule or many rules, with the ordering being important as the first rule that matches defines the traffic flow.

Policy Enforcer uses user intent-based policies. 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.

Related Documentation

- Policy Enforcer Overview on page 17
- Policy Enforcer Components on page 21
- Sky ATP Features on page 26
- Using Guided Setup for Sky ATP with SDSN on page 55
- Using Guided Setup for Sky ATP on page 59
- Configuring Sky ATP with SDSN (Without Guided Setup) Overview on page 62

Policy Enforcer Components

The Policy Enforcer Deployment Model uses the following components:
• **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.

• **EX and QFX Series switches**—EX Series Ethernet switches deliver core layer switching services in branch, campus, and data center networks. QFX Series switches are high-performance, low-latency, edge devices optimized for virtualized data center environments.

*Figure 4 on page 23 illustrates how the components in the Policy Enforcer Deployment Model interact.*
Figure 4: Components of the Policy Enforcer Deployment Model

Figure 5 on page 23 shows an example infected endpoint scenario to illustrate how some of the components work together.

Figure 5: Blocking an Infected Endpoint

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A user downloads a file from the Internet.</td>
</tr>
<tr>
<td>2</td>
<td>Based on user-defined policies, the file is sent to the Sky ATP cloud for malware inspection.</td>
</tr>
</tbody>
</table>
### Step 3
The inspection determines this file is malware and informs Policy Enforcer of the results.

### Step 4
The enforcement policy is automatically deployed to the SRX Series device and switches.

### Step 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 6 on page 24.

**Figure 6: Tracking Infected Endpoint Movement**

![Figure 6: Tracking Infected Endpoint Movement](image)

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 7 on page 25.

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 45.
An end-user authenticates to the network through IEEE 802.1X or through MAC-based authentication.

Sky ATP detects the endpoint is infected with malware and adds it to the infected host feed.

Policy Enforcer downloads the infected host feed.

Policy Enforcer enforces the infected host policy using the Connector. See “Policy Enforcer Connector Overview” on page 45.

The Connector queries the RADIUS server for the infected host endpoint details and initiates a Change of Authorization (CoA) for the infected host.

The CoA can be either block or quarantine the infected host.

The enforcement occurs on the NAC device the infected host is authenticated with.

Policy Enforcer communicates the infected host details back to Sky ATP.

Related Documentation

- Policy Enforcer Overview on page 17
- Benefits of Policy Enforcer on page 19
- Sky ATP Features on page 26
- Policy Enforcer Installation Overview on page 29
- Using Guided Setup for Sky ATP with SDSN on page 55
- Using Guided Setup for Sky ATP on page 59
- Configuring Sky ATP with SDSN (Without Guided Setup) Overview on page 62
Sky ATP Features

Sky Advanced Threat Prevention is a cloud-based threat identification and prevention solution. 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.

Sky Advanced Threat Prevention offers the following features:

- Integrated with the SRX Series device to simplify deployment and enhance the anti-threat capabilities of the firewall.
- Delivers protection against “day-zero” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time.
- Provides deep inspection, actionable reporting, and inline malware blocking.

Related Documentation
- Sky ATP Realm Overview on page 78
- Using Guided Setup for Sky ATP on page 59
- Configuring Sky ATP (No SDSN and No Guided Setup) Overview on page 77

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 3 on page 26 compares the basic steps for both.

Table 3: Comparing the SDSN Configuration Steps to the non-SDSN Configuration Steps

<table>
<thead>
<tr>
<th>SDSN Configuration Steps</th>
<th>Non-SDSN Configuration Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create your secure fabric.</td>
<td>Register one or more Sky ATP accounts.</td>
</tr>
<tr>
<td>A secure fabric is a collection of sites which contain network devices such as switches, routers, firewalls, and other security devices.</td>
<td></td>
</tr>
<tr>
<td>Create your policy enforcement groups.</td>
<td>Select your SRX Series devices to register. Only SRX Series devices managed by Security Director are supported.</td>
</tr>
<tr>
<td>You can create policy enforcement groups based on, for example, location or IP subnets. Policy enforcement groups are basically endpoints.</td>
<td></td>
</tr>
<tr>
<td>Register one or more Sky ATP accounts.</td>
<td>Create the Sky ATP profiles and policies. You can create C&amp;C (threat score and actions to take), malware and infected host policies.</td>
</tr>
</tbody>
</table>
Table 3: Comparing the SDSN Configuration Steps to the non-SDSN Configuration Steps (continued)

<table>
<thead>
<tr>
<th>SDSN Configuration Steps</th>
<th>Non-SDSN Configuration Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create threat prevention policies.</td>
<td>Add the Sky ATP policy as a rule in your firewall policy.</td>
</tr>
<tr>
<td>Threat prevention policies provide protection and monitoring for selected threat profiles, including command &amp; control servers, infected hosts, and malware.</td>
<td></td>
</tr>
</tbody>
</table>

Apply your threat prevention policies to policy enforcement groups.

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.

**Related Documentation**

- Using Guided Setup for Sky ATP with SDSN on page 55
- Using Guided Setup for Sky ATP on page 59
- Configuring Sky ATP with SDSN (Without Guided Setup) Overview on page 62
- Configuring Sky ATP (No SDSN and No Guided Setup) Overview on page 77
- Policy Enforcer Overview on page 17
- Benefits of Policy Enforcer on page 19
- Policy Enforcer Components on page 21
- Sky ATP Features on page 26
CHAPTER 2

Installing Policy Enforcer

- Policy Enforcer Installation Overview on page 29
- Deploying and Configuring the Policy Enforcer Virtual Machine on page 31
- Identifying the Policy Enforcer Virtual Machine In Security Director on page 36
- Obtaining a Sky ATP License on page 37
- Creating a Sky ATP Cloud Web Portal Login Account on page 38
- Loading a Root CA on page 39
- Upgrading Your Policy Enforcer Software on page 40

Policy Enforcer Installation Overview

Policy Enforcer is delivered as an OVA package to be deployed inside your VMware ESX network. 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 ESXi servers, see VMware Documentation and select the appropriate VMware vSphere version.

Table 4 on page 30 lists the general steps to install and configure Policy Enforcer.
Table 4: Overview of Steps to Install and Configure Policy Enforcer

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install and configure Junos Space and Security Director 16.1 or later.</td>
<td>Junos Space Network Management Platform software download</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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.</td>
<td>Junos Space Security Director software download</td>
</tr>
<tr>
<td>2</td>
<td>Install and configure your SRX Series devices, EX Series switches or QFX Series switches. Switches are “discoverable” through Junos Space. For information on discovering switches, see “Using Guided Setup for Sky ATP with SDSN” on page 55.</td>
<td>Juniper Tech Library</td>
</tr>
<tr>
<td>3</td>
<td>Download, deploy and configure the Policy Enforcer virtual machine.</td>
<td>“Deploying and Configuring the Policy Enforcer Virtual Machine” on page 31</td>
</tr>
<tr>
<td>4</td>
<td>Use the Policy Enforcer Settings screen in Security Director (Administration &gt; PE Settings) to identify the Policy Enforcer virtual machine to communicate with.</td>
<td>“Identifying the Policy Enforcer Virtual Machine In Security Director” on page 36</td>
</tr>
<tr>
<td>5</td>
<td>Obtain a Sky ATP license and create a Sky ATP portal account.</td>
<td>“Obtaining a Sky ATP License” on page 37 “Creating a Sky ATP Cloud Web Portal Login Account” on page 38</td>
</tr>
<tr>
<td>6</td>
<td>Install the root CA on your Sky ATP-supported SRX Series devices.</td>
<td>“Loading a Root CA” on page 39</td>
</tr>
<tr>
<td>7</td>
<td>Use the Setup Wizard screens in Security Director to configure Threat Prevention policies and deploy to their devices. Optionally, you can configure policies without the setup wizard. Which option you use is based on the mode you select in the PE Setting page.</td>
<td>“Using Guided Setup for Sky ATP with SDSN” on page 55 “Using Guided Setup for Sky ATP” on page 59</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Deploying and Configuring the Policy Enforcer Virtual Machine on page 31
- Policy Enforcer Overview on page 17
- Benefits of Policy Enforcer on page 19
Deploying and Configuring the Policy Enforcer Virtual Machine

To deploy and configure the Policy Enforcer virtual machine, perform the following tasks:

1. Download the Policy Enforcer virtual machine 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 8 on page 32.
10. Enter the following configuration information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Enter the hostname for the Policy Enforcer virtual machine; for example, pe.juniper.net.</td>
</tr>
<tr>
<td>IP address</td>
<td>Enter the IP address for the Policy Enforcer virtual machine.</td>
</tr>
<tr>
<td>NOTE: Make note of this IP address as you’ll need it in a later step.</td>
<td></td>
</tr>
<tr>
<td>Network mask</td>
<td>Enter the netmask for the Policy Enforcer virtual machine.</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Enter the IP address of the default gateway that connects your internal network to external networks.</td>
</tr>
<tr>
<td>Primary DNS server</td>
<td>Enter the IP address of your primary system registered to join the Domain Name System (DNS).</td>
</tr>
<tr>
<td>Secondary DNS server</td>
<td>Enter the IP address of a secondary DNS server. Policy Enforcer uses this address only when the primary DNS server is unavailable.</td>
</tr>
<tr>
<td>Skip DNS servers check</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 9 on page 33.
Figure 9: 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 10 on page 33. 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 10: Configuring the NTP Servers

The Customer Information page appears. See Figure 11 on page 33.

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 11: Entering Customer Information
15. Click OK.

The Root password change page appears. See Figure 12 on page 34.

Figure 12: Changing the Root Password

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 13 on page 34.

Figure 13: Reviewing and Changing Your Configuration Settings.
18. Select one of the options and press **Enter**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review configuration and finish setup</td>
<td>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.</td>
</tr>
<tr>
<td>Change...</td>
<td>Select a setting to update its value.</td>
</tr>
<tr>
<td>Troubleshooting menu</td>
<td>Lets you ping the default gateway and custom IP address and lets you perform a DNS lookup to verify that your settings are correct.</td>
</tr>
</tbody>
</table>

The Review configuration page appears. See [Figure 14 on page 35](#).

**Figure 14: Reviewing Your Configuration Settings**

![Image of Review configuration page](image)

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.
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.

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 43.

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 on page 37
- Policy Enforcer Overview on page 17
- Benefits of Policy Enforcer on page 19
- Policy Enforcer Components on page 21

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/ 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 on page 38
- Policy Enforcer Overview on page 17
- Benefits of Policy Enforcer on page 19
- Policy Enforcer Components on page 21

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 on page 39
- Using Guided Setup for Sky ATP with SDSN on page 55
Using Guided Setup for Sky ATP on page 59

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 Sky ATP-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 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

    http://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-17.1R1-24-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%]
  Upgrading..######################################################## [100%]
  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 16.2R1 to 17.1R1) Check the following log files for errors:
    - /var/log/pe_upgrade_17.1.log
- /var/log/pe_upgrade_17_1_3rd_party_adapter.log
- /var/log/pe_upgrade_nsx.log

Related Documentation
- Policy Enforcer Installation Overview on page 29
CHAPTER 3

Configuring Policy Enforcer Settings (Required for Sky ATP, Policy Enforcer, and Cloud Feeds)

- Policy Enforcer Settings on page 43
- Policy Enforcer Connector Overview on page 45
- ClearPass Configuration for Third-Party Switches on page 46
- Creating a Policy Enforcer Connector for Third-Party Switches on page 52

Policy Enforcer Settings

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

Configuring Policy Enforcer settings enables Security Directory to communicate with the Sky ATP feed connector service running within the context of the Policy Enforcer VM.

---

**NOTE:** 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.

---

**NOTE:** A Sky ATP license and account are needed for all threat prevention 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 29 for instructions on obtaining a Sky ATP premium license.
Before you configure Policy Enforcer, 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 Virtual Machine” on page 31 for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.

3. Select a Threat Prevention Type:
   - 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 55
      • Configuring Sky ATP with SDSN (Without Guided Setup) Overview on page 62

   - 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 59
      • Configuring Sky ATP (No SDSN and No Guided Setup) Overview on page 77

   - Cloud feeds only—Command and control server and Geo IP are the only threat prevention types available.
See the following topic to configure Cloud feeds only:

- Configuring Cloud Feeds Only on page 87

Related Documentation

- Comparing the SDSN and non-SDSN Configuration Steps on page 26
- Using Guided Setup for Sky ATP with SDSN on page 55
- Using Guided Setup for Sky ATP on page 59
- Configuring Cloud Feeds Only on page 87
- Policy Enforcer Dashboard Widgets on page 107

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 which adhere to Radius IETF attributes and support Radius Change of Authorization from 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 5: Connectors Information- Main Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name you entered for the connector.</td>
</tr>
</tbody>
</table>
Table 5: Connectors Information - Main Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>This field always reads Third Party Switch at this time.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the connector. (Active or Inactive.)</td>
</tr>
<tr>
<td>Description</td>
<td>The description you provided.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the ClearPass RADIUS server.</td>
</tr>
</tbody>
</table>

Related Documentation
- ClearPass Configuration for Third-Party Switches on page 46
- Creating a Policy Enforcer Connector for Third-Party Switches on page 52

ClearPass Configuration for Third-Party Switches

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.

On ClearPass you will configure the following:
- API Client
- Custom Attribute
- Enforcement Profiles
- Enforcement Policy

Configure the API Client:

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

   ![NOTE: You must login as ClearPass Guest to see the API services menu.]

   - Client ID: sdsnclient
   - 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 15 on page 47.
Figure 15: ClearPass API Client Operator Profile Minimum Privileges

**Operator Profile**

- **Name:** SDSN API Profile
- **Description:** Default administrative profile.
- **Operator logins:** Enabled

**Privileges:**

- **Administrator:** Full Access
- **API Services:** Custom
  - Allow API Access: Allow Access
  - Manage API Clients: Full Access
- **Guest Manager:** Custom
  - Active Sessions: Full Access
  - Active Sessions History: Read Only
  - Show Details: Read Only
- **Insight:** Full Access
- **Onboard:** Full Access
- **Platform:** Full Access
- **Policy Manager:** Full Access

**Skin:**

- **Start Page:** GuestManager Plugin
- **Language:** (Default)
- **Time Zone:** (Default)

- 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 a time-frame.

---

**WARNING:** When the Access Token Lifetime expires, you must generate a new Client Secret and update it in the Policy Enforcer Connector UI page.
2. Click **Save Changes**.

Configure a Custom Attribute:

1. 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
2. Click **Save**.

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 18: ClearPass Enforcement Profile: Quarantine

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:
   - Name: [JNPR SDSN Terminate Session]
   - Description: System-defined profile to disconnect user (Juniper)
   - 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.
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.

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.

Related Documentation
- Creating a Policy Enforcer Connector for Third-Party Switches on page 52
- Policy Enforcer Connector Overview on page 45

Creating a Policy Enforcer Connector for Third-Party Switches

Access this page from Administration > Policy Enforcer > Connectors.

- Have your ClearPass server information available. For example, IP address, Client ID, and Client Secret.
- Once configured, you select the Third Party Switch as an Enforcement Point in your Secure Fabric.
- Note that only one ClearPass identity server can be added for a given controller, but you can select it multiple times for different sites.
- Note that you cannot delete a controller that is assigned to a site without disassociating the controller first.
- Review the “Policy Enforcer Connector Overview” on page 45 topic.

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

1. Access Administration > Policy Enforcer > Connectors.

2. Click +.

3. Complete the configuration using the information in Table 6 on page 53.

4. Click OK.
NOTE: Once configured, you select the Third Party Switch as an Enforcement Point in your Secure Fabric.

Table 6: Fields on the Policy Enforcement Connectors Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector for</td>
<td>At this time only Third Party Switch is available.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.</td>
</tr>
<tr>
<td>Identity Server Type</td>
<td>Select a server type. (Note that only ClearPass supported at this time.)</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP Address (IPv4 or IPv6) of the server.</td>
</tr>
<tr>
<td>Port</td>
<td>(Optional) Enter the port to be used. When this is left blank, port 443 is used as the default.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Enter the Client ID created while setting up the ClearPass API client. See “ClearPass Configuration for Third-Party Switches” on page 46 for details.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Enter the Client Secret string created while setting up the ClearPass API client. See “ClearPass Configuration for Third-Party Switches” on page 46 for details. <strong>WARNING:</strong> When the Access Token Lifetime expires, you must generate a new Client Secret in ClearPass and update it here too.</td>
</tr>
</tbody>
</table>

**WARNING:** Be sure the correct credentials are provided to the ClearPass server. If the initial connection fails, an error message is shown only at that time. Once that message disappears, the status of connectivity to the ClearPass server is not shown in Policy Enforcer. Note that the ClearPass server is only queried ondemand.

Related Documentation
- Policy Enforcer Connector Overview on page 45
- ClearPass Configuration for Third-Party Switches on page 46
CHAPTER 4

Guided Setup for Sky ATP with SDSN

- Using Guided Setup for Sky ATP with SDSN on page 55

Using Guided Setup for Sky ATP with SDSN

See Policy Enforcer Overview for product information.

If you are using Policy Enforcer for threat prevention with Sky ATP, Guided Setup is the most efficient way to complete your initial configuration. If you are using Sky ATP without PE, you should use Sky ATP Guided Setup. See “Using Guided Setup for Sky ATP” on page 59.

NOTE: 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 43. (Refer to Installing Policy Enforcer for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.)

NOTE: A Sky ATP license and account are needed for all threat prevention 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 Installing Policy Enforcer for instructions on obtaining a Sky ATP license.

Guided Setup is located under Configure > Guided Setup.
The Guided Setup process offers four steps for configuring Sky ATP with SDSN. 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.

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. 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 to the Threat Policy Analysis page. See “Threat Policy Analysis Overview” on page 73. 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 Overview on page 17
- Benefits of Policy Enforcer on page 19
- Policy Enforcer Components on page 21
- Policy Enforcer Settings on page 43
- Configuring Sky ATP with SDSN (Without Guided Setup) Overview on page 62
- Using Guided Setup for Sky ATP on page 59
- Secure Fabric Overview on page 65
- Policy Enforcement Groups Overview on page 67
- Sky ATP Realm Overview on page 78
• Threat Prevention Policy Overview on page 68
CHAPTER 5

Guided Setup for Sky ATP

- Using Guided Setup for Sky ATP on page 59

Using Guided Setup for Sky ATP

See “Sky ATP Features” on page 26 for an overview of Sky ATP.

For configuring Sky ATP policies, guided setup is the most efficient way to complete your initial configuration. If you are using Sky ATP with Policy Enforcer, you should use guided setup for PE Setup with Sky ATP instead. Find those instructions here: “Using Guided Setup for Sky ATP with SDSN” on page 55.

NOTE: 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 Installing Policy Enforcer for instructions on obtaining a Sky ATP premium license.

Guided setup is located under Configure > Guided Setup > Sky ATP. Click Start Setup 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. 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. 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 Features on page 26
- Sky ATP Realm Overview on page 78
- Threat Prevention Policy Overview on page 68
- Configuring Sky ATP (No SDSN and No Guided Setup) Overview on page 77
- Creating Geo IP Policies on page 73
CHAPTER 6

Configuring Policy Enforcer (without Guided Setup)

• Configuring Sky ATP with SDSN (Without Guided Setup) Overview on page 62
• Creating Sky ATP Realms and Enrolling Devices or Associating Sites on page 63
• Secure Fabric Overview on page 65
• Creating Secure Fabric and Sites on page 65
• Editing or Deleting a Secure Fabric on page 67
• Policy Enforcement Groups Overview on page 67
• Creating Policy Enforcement Groups on page 67
• Threat Prevention Policy Overview on page 68
• Creating Threat Prevention Policies on page 69
• Threat Policy Analysis Overview on page 73
• Geo IP Overview on page 73
• Creating Geo IP Policies on page 73
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 Installing Policy Enforcer 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 43. (Refer to Installing Policy Enforcer 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 63 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 65 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 67 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.
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.
- 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 7 on page 63 below.

Table 7: Fields on the Add Sky ATP Realm Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select a region of the world from the available choices.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter your e-mail address. Your username for Sky ATP is your e-mail address.</td>
</tr>
</tbody>
</table>
Table 7: Fields on the Add Sky ATP Realm Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>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 (~!@#$%^&amp;*()-+=[]{}</td>
</tr>
<tr>
<td><strong>Realm</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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 pulldown 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 65.

   **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 slidebar 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.

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.

Creating Secure Fabric and Sites

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.
- Note that devices cannot belong to multiple sites.

To create a site within your secure fabric:

2. Click the + icon.
3. Complete the configuration by using the guidelines in Table 8 on page 66 below.

4. Click OK.

5. Create a new site and assign or reassign devices to a site by following the guidelines in Table 9 on page 66 below.

Table 8: Fields on the Create Site Page

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

Table 9: Fields on the Sites Main Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Name | Click an existing device to edit it or click Add Devices. Select the check box beside the devices in the Unassigned Devices list and click the > icon to move them to the Selected list. The devices in the Selected list will be included in the site. Indicate whether a device is a firewall or a switch by selecting the check box. Only perimeter SRX Series devices can be enrolled with Sky ATP, therefore the system must know which devices those are. **NOTE:** Firewall devices are automatically enrolled with Sky ATP as part of this step. No manual enrollment is required.  
**NOTE:** If you want to enforce an infected host policy within the network, you must assign a switch to the site. |
| IPAddress | Click an existing address or Add Devices in the IP Address field. Select the check box beside the switches in the Unassigned Devices list and click the > icon to move them to the Selected list. The devices in the Selected list will be included in the site. Indicate whether a device is a firewall or a switch by selecting the check box. |
| “Drag and Drop” devices | You can reassign devices to sites by dragging them from the Devices Name column on the main page to the Site column. |

Related Documentation

- Secure Fabric Overview on page 65
- Policy Enforcement Groups Overview on page 67
- Threat Prevention Policy Overview on page 68
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:

   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 on page 65
- Secure Fabric Overview on page 65
- Creating Policy Enforcement Groups on page 67

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**
- Creating Policy Enforcement Groups on page 67
- Threat Prevention Policy Overview on page 68

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 10 on page 68** below.

4. Click **OK**.

### Table 10: Fields on the Policy Enforcement Group Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.</td>
</tr>
<tr>
<td>Group Type</td>
<td>Select a group type from the available choices. IP address/subnet or location.</td>
</tr>
<tr>
<td>Items</td>
<td>Select the check box beside the IP address(es) of the endpoint device(s) in the Available list and click the &gt; icon to move them to the Selected list. The endpoints in the Selected list will be included in the policy enforcement group.</td>
</tr>
<tr>
<td>Add New Endpoint</td>
<td>Click the <strong>Add New Endpoint</strong> button if the address or location you want does not appear in the Available list.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- [Policy Enforcement Groups Overview on page 67](#)
- [Using Guided Setup for Sky ATP with SDSN on page 55](#)

### Threat Prevention Policy Overview

Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control servers, 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.

**Related Documentation**

- [Creating Threat Prevention Policies on page 69](#)
- [Policy Enforcement Groups Overview on page 67](#)
- [Creating Geo IP Policies on page 73](#)
- [Policy Enforcer Overview on page 17](#)
Creating Threat Prevention Policies

To access this page, click 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 26 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 73.
- 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.
3. Complete the configuration by using the guidelines in the Table 11 on page 70 below.
4. Click OK.
### Table 11: Fields on the Threat Prevention Policy Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.</td>
</tr>
</tbody>
</table>

**Profiles**

<table>
<thead>
<tr>
<th>Command and Control Server</th>
<th>Select and choose settings for command and control servers. A C&amp;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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include C&amp;C profile in policy</td>
<td>Select the check box to include management for this threat type in the policy.</td>
</tr>
</tbody>
</table>

**Threat Score**

<table>
<thead>
<tr>
<th>Threat Score</th>
<th>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 Monitor &gt; Threat Management.</th>
</tr>
</thead>
</table>

**Actions**

If the threat score is high enough to cause a connection to be blocked, you have following configurable options:

- Drop connection silently (This is the default and recommended setting.)
- Close connection and do not send a message
  - Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.
  - Send custom message—in the field provided, enter a message to be shown to users when connections are dropped.

**Infected Host**

<table>
<thead>
<tr>
<th>Infected Host</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include infected host profile in policy</td>
<td>Select the check box to include management for this threat type in the policy.</td>
</tr>
</tbody>
</table>

**NOTE:** If you want to enforce an infected host policy within the network, you must include a switch in the site.

**Actions**

You have following options:

- Drop connection silently (This is the default and recommended setting.)
- 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.)
Table 11: Fields on the Threat Prevention Policy Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Malware</strong> (HTTP file download and SMTP File attachment)</td>
<td>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.</td>
</tr>
<tr>
<td>Include malware profile in policy</td>
<td>Select the check box to include management for this threat type in the policy.</td>
</tr>
<tr>
<td>HTTP file download</td>
<td>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.</td>
</tr>
<tr>
<td>Scan HTTPS</td>
<td>Turn this feature to scan encrypted files downloaded over HTTPS.</td>
</tr>
<tr>
<td>Device Profile</td>
<td>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. <em>Device Profiles Overview.</em></td>
</tr>
</tbody>
</table>
| Actions | If the threat score is high enough to cause a connection to be blocked, you have following configurable options:  
  - Drop connection silently (This is the default and recommended setting.)  
  - Close connection and do not send a message  
    - Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.  
    - Send custom message—In the field provided, enter a message to be shown to users when connections are dropped. |
| SMTP File Attachment | Turn this feature on to inspect files received as email attachments (over SMTP only). |
| Device Profile | If you do not click the **Change** button to select a device profile for SMTP scanning, the device profile selected for HTTP will be used by default.  
  Select **Change** to use a different device profile for SMTP.  
  Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection. |
| 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. |
Table 11: Fields on the Threat Prevention Policy Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Setting (Policy setting for all profiles)</td>
<td>Select the log setting for the policy. You can log all traffic, log only blocked traffic, or log no traffic.</td>
</tr>
</tbody>
</table>

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 67.

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 73. 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 on page 26
- Creating Policy Enforcement Groups on page 67
- Threat Policy Analysis Overview on page 73
- Creating Geo IP Policies on page 73
- Threat Prevention Policy Overview on page 68
- Policy Enforcer Overview on page 17
• Benefits of Policy Enforcer on page 19
• Policy Enforcer Components on page 21
• Sky ATP Features on page 26

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.

Use the threat policy analysis page to view your pending policy changes in chronological order. Click the policy 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 on page 68
• Creating Threat Prevention Policies on page 69

Geo IP Overview

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 on page 73
• Threat Prevention Policy Overview on page 68
• Sky ATP Realm Overview on page 78

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 12 on page 74 below.

4. Click OK.

Table 12: Fields on the Geo IP Policy Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.</td>
</tr>
<tr>
<td>Countries</td>
<td>Select the check box beside the countries in the Available list and click the &gt; 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.</td>
</tr>
<tr>
<td>Block Traffic</td>
<td>Choose what traffic to block from the selected countries. Incoming traffic, Outgoing traffic, or Incoming and Outgoing traffic. (Policy Enforcer only)</td>
</tr>
<tr>
<td>Log Setting</td>
<td>Choose to log all traffic or only blocked traffic. (Policy Enforcer only)</td>
</tr>
</tbody>
</table>

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 73. 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 on page 67
- Creating Threat Prevention Policies on page 69
- Threat Policy Analysis Overview on page 73
- Geo IP Overview on page 73
- Hosts Overview
- Command and Control Servers Overview
- Configuring Cloud Feeds Only on page 87
CHAPTER 7

Configuring Sky ATP (without Guided Setup)

• Configuring Sky ATP (No SDSN and No Guided Setup) Overview on page 77
• Sky ATP Realm Overview on page 78
• Creating Sky ATP Realms and Enrolling Devices or Associating Sites on page 79
• Threat Prevention Policy Overview on page 80
• Creating Threat Prevention Policies on page 81

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 Installing Policy Enforcer 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 43. (Refer to Installing Policy Enforcer 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 63 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 69 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
- Creating Sky ATP Realms and Enrolling Devices or Associating Sites on page 63
- Creating Threat Prevention Policies on page 69
- Creating Geo IP Policies on page 73

### 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.

**Related Documentation**
- Creating Sky ATP Realms and Enrolling Devices or Associating Sites on page 63
- Using Guided Setup for Sky ATP on page 59
- Sky Configuring Sky ATP (No SDSN and No Guided Setup) Overview on page 77
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.
- 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 7 on page 63 below.

Table 13: Fields on the Add Sky ATP Realm Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select a region of the world from the available choices.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter your e-mail address. Your username for Sky ATP is your e-mail address.</td>
</tr>
<tr>
<td>Password</td>
<td>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 (~!@#$%^&amp;*()-_=+{}[]</td>
</tr>
<tr>
<td>Realm</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 pulldown 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 65.

**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 slidebar 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 on page 78
- Using Guided Setup for Sky ATP on page 59
- Creating Secure Fabric and Sites on page 65

**Threat Prevention Policy Overview**

Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control servers, 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.
Creating Threat Prevention Policies

To access this page, click 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 26 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 73.
- 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.
3. Complete the configuration by using the guidelines in the Table 11 on page 70 below.

4. Click **OK**.

### Table 14: Fields on the Threat Prevention Policy Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63-character maximum.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.</td>
</tr>
<tr>
<td><strong>Profiles</strong></td>
<td></td>
</tr>
<tr>
<td>Command and Control Server</td>
<td>Select and choose settings for command and control servers. A C&amp;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.</td>
</tr>
<tr>
<td>Include C&amp;C profile in policy</td>
<td>Select the check box to include management for this threat type in the policy.</td>
</tr>
<tr>
<td>Threat Score</td>
<td>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 <strong>Monitor &gt; Threat Management</strong>.</td>
</tr>
<tr>
<td>Actions</td>
<td>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</td>
</tr>
<tr>
<td></td>
<td>• Drop connection silently (This is the default and recommended setting.)</td>
</tr>
<tr>
<td></td>
<td>• Close connection and do not send a message</td>
</tr>
<tr>
<td></td>
<td>• Close connection and redirect to URL—In the field provided, enter a URL to redirect users to when connections are dropped.</td>
</tr>
<tr>
<td></td>
<td>• Send custom message—In the field provided, enter a message to be shown to users when connections are dropped.</td>
</tr>
<tr>
<td>Infected Host</td>
<td>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.</td>
</tr>
<tr>
<td>Include infected host profile in policy</td>
<td>Select the check box to include management for this threat type in the policy.</td>
</tr>
</tbody>
</table>

**NOTE**: If you want to enforce an infected host policy within the network, you must include a switch in the site.
### Table 14: Fields on the Threat Prevention Policy Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actions</strong></td>
<td>You have following options:</td>
</tr>
<tr>
<td></td>
<td>• Drop connection silently (This is the default and recommended setting.)</td>
</tr>
<tr>
<td></td>
<td>• 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.)</td>
</tr>
<tr>
<td><strong>Malware (HTTP file download and SMTP File attachment)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Include malware profile in policy</strong></td>
<td>Select the check box to include management for this threat type in the policy.</td>
</tr>
<tr>
<td><strong>HTTP file download</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Scan HTTPS</strong></td>
<td>Turn this feature to scan encrypted files downloaded over HTTPS.</td>
</tr>
<tr>
<td><strong>Device Profile</strong></td>
<td>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. Device Profiles Overview.</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td>If the threat score is high enough to cause a connection to be blocked, you have following configurable options:</td>
</tr>
<tr>
<td></td>
<td>• Drop connection silently (This is the default and recommended setting.)</td>
</tr>
<tr>
<td></td>
<td>• Close connection and do not send a message</td>
</tr>
<tr>
<td></td>
<td>• Close connection and redirect to URL—in the field provided, enter a URL to redirect users when connections are dropped.</td>
</tr>
<tr>
<td></td>
<td>• Send custom message—in the field provided, enter a message to be shown to users when connections are dropped.</td>
</tr>
<tr>
<td><strong>SMTP File Attachment</strong></td>
<td>Turn this feature on to inspect files received as email attachments (over SMTP only).</td>
</tr>
<tr>
<td><strong>Device Profile</strong></td>
<td>If you do not click the Change button to select a device profile for SMTP scanning, the device profile selected for HTTP will be used by default.</td>
</tr>
<tr>
<td></td>
<td>Select Change to use a different device profile for SMTP.</td>
</tr>
<tr>
<td></td>
<td>Device profiles are configured through Sky ATP and define which files to send to the cloud for inspection.</td>
</tr>
<tr>
<td><strong>Threat Score</strong></td>
<td>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.)</td>
</tr>
</tbody>
</table>
Table 14: Fields on the Threat Prevention Policy Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Actions for SMTP File Attachments include: Quarantine, Deliver malicious</td>
</tr>
<tr>
<td></td>
<td>messages with warning headers added, and Permit. This actions are set</td>
</tr>
<tr>
<td></td>
<td>in Sky ATP. Refer to the Sky ATP documentation for information.</td>
</tr>
<tr>
<td>Log Setting (Policy setting for all</td>
<td>Select the log setting for the policy. You can log all traffic, log only</td>
</tr>
<tr>
<td>profiles)</td>
<td>blocked traffic, or log no traffic.</td>
</tr>
</tbody>
</table>

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 67.

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 73. 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 on page 26
- Creating Policy Enforcement Groups on page 67
- Threat Policy Analysis Overview on page 73
- Creating Geo IP Policies on page 73
• Threat Prevention Policy Overview on page 68
• Policy Enforcer Overview on page 17
• Benefits of Policy Enforcer on page 19
• Policy Enforcer Components on page 21
• Sky ATP Features on page 26
CHAPTER 8

Configuring Cloud Feeds Only

- Configuring Cloud Feeds Only on page 87

**Configuring Cloud Feeds Only**

This in 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 all threat prevention 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 “Obtaining a Sky ATP License” on page 37 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 43. (Refer to “Deploying and Configuring the Policy Enforcer Virtual Machine” on page 31 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:

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 63 for details.

2. Create a threat prevention policy for Command and Control server. (Note that this is the only threat prevention, besides Geo IP, supported for Cloud Feed only mode.)
   
   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 69 for details.

   
   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.

4. You must assign a command and control server threat prevention policy to a firewall rule before it can take effect.
   
   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

- Creating Sky ATP Realms and Enrolling Devices or Associating Sites on page 63
- Creating Geo IP Policies on page 73
- Creating Threat Prevention Policies on page 69
- Policy Enforcer Settings on page 43
CHAPTER 9

Threat Prevention - Configure

- Creating Sky ATP Realms and Enrolling Devices or Associating Sites on page 89
- Sky ATP Realm Overview on page 91
- Custom Feed Sources Overview on page 91
- Creating Custom Feeds, Dynamic, Black and White on page 92
- Creating Custom Feeds, Infected Host on page 95
- Sky ATP Email Management Overview on page 97
- Sky ATP Email Management: SMTP Settings on page 98
- Sky ATP Email Management: Whitelists and Blacklists on page 101
- Sky ATP Malware Management Overview on page 101
- File Inspection Profiles Overview on page 102
- Creating File Inspection Profiles on page 103
- Creating Whitelists and Blacklists on page 104

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.
- 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 7 on page 63 below.

Table 15: Fields on the Add Sky ATP Realm Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Select a region of the world from the available choices.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter your e-mail address. Your username for Sky ATP is your e-mail address.</td>
</tr>
<tr>
<td>Password</td>
<td>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 (~!@#$%^&amp;*()_-+={}[]</td>
</tr>
<tr>
<td>Realm</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 pulldown 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 65.

   **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 slidebar 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 Director that was enrolled from within Sky ATP.

Related Documentation
- Sky ATP Realm Overview on page 78
- Using Guided Setup for Sky ATP on page 59
- Creating Secure Fabric and Sites on page 65

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.

Related Documentation
- Creating Sky ATP Realms and Enrolling Devices or Associating Sites on page 63
- Using Guided Setup for Sky ATP on page 59
- skyConfiguring Sky ATP (No SDSN and No Guided Setup) Overview on page 77

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, including Sky ATP and lists you customize by adding IP addresses, domains, and URLs to your own lists. The following types of 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—A whitelist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the whitelist does not have to be inspected for malware.

• Blacklist—A blacklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blacklist is blocked, and therefore no content can be downloaded from those sites.

• Infected Host—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.

Creating Custom Feeds, Dynamic, Black and White

To access this page, click Configure > Threat Prevention > Custom Feeds.

You can create customs feeds from the custom feeds page.

• Know what type of feed you are configuring and have all the necessary information on hand. For example, for custom feeds from a file server, you must have the file server URL and a valid user name and password for the file server. 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 95.

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 16: Custom Feed Categories

<table>
<thead>
<tr>
<th>Feed Category</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Dynamic Address | 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.  

**NOTE:** For Dynamic Address, you can create multiple custom feeds. For Whitelist, Blacklist, and Infected Host, you can only create one custom feed for each. |
| Whitelist       | A whitelist contains known trusted IP addresses, URLs, and domains. Content downloaded from locations on the whitelist does not have to be inspected for malware.                                      |
| Blacklist       | A blacklist contains known untrusted IP addresses, URLs, and domains. Access to locations on the blacklist 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 “Creating Custom Feeds, Infected Host” on page 95 for configuration details. |

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 17 on page 93 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 18 on page 94.

4. Complete the configuration by using the guidelines in Table 17 on page 93 or Table 18 on page 94.

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.

Use the fields in Table 17 on page 93 to add custom feeds.

Table 17: Fields on the Custom Feeds Page, Feeds with Local Files

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 17: Fields on the Custom Feeds Page, Feeds with Local Files (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Feed Type**

Select one of the following:

- **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.
- **URL and Domain**—Enter the URL using the following format: http://badurl.com/abc and Domain using the following format: http://badurl.com. Wildcards and protocols are not valid entries.

**NOTE:** For Dynamic Address, you can only select IP, Subnet, and Range. For Blacklists and Whitelists, all feed types are available for selection.

**Custom List**

Do one of the following:

- Click **Upload File** to upload a text file with an IP address list. Click the **Add** button to include the address list in your custom list.

  Note that the file must contain only one item per line (no commas or semicolons). All items are validated before being added to the custom list.

  Manually enter your item in the space provided in the Custom List section. To add more items, click + to add more spaces.

### Table 18: Fields on the Custom Feeds Page, Feeds with Remote File Server

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
</tbody>
</table>

| 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. |

**Feed Type**

Select one of the following:

- **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.
- **URL and Domain**—Enter the URL using the following format: http://badurl.com/abc and Domain using the following format: http://badurl.com. Wildcards and protocols are not valid entries.

**NOTE:** For Dynamic Address, you can only enter IP, Subnet, and Range. For Blacklists and Whitelists, all feed types are available for selection.

**Type of Server URL**

Select one of the following:

- **http**
- **https**
Table 18: Fields on the Custom Feeds Page, Feeds with Remote File Server (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server File URL</td>
<td>Enter the URL for the remote file server.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the credentials for the remote file server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the credentials for the remote file server.</td>
</tr>
<tr>
<td>Update Interval</td>
<td>Select how often updates are retrieved from the remote files server: Hourly, Daily, Weekly, Monthly, Never</td>
</tr>
</tbody>
</table>

Related Documentation
- Creating Custom Feeds, Infected Host on page 95
- Custom Feed Sources Overview on page 91
- Sky ATP Realm Overview on page 78

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 Cloud feeds only 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, Black and White” on page 92.

To create local file and remote file custom feeds:
1. Select Configure > Threat Prevention > Custom Feeds.
2. Select the Infected Host tab.
3. Click Create and select one of the following:

   NOTE: When Cloud feeds only is selected as the Threat Prevention Type, the infected host custom feed is not available.
• **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 17 on page 93 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 18 on page 94.

4. Complete the configuration by using the guidelines in Table 17 on page 93 or Table 18 on page 94.

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, Whitelists and Blacklists.

---

Use the fields in Table 17 on page 93 to add custom feeds.

Table 19: Fields on the Custom Feeds Page, Feedswith Local Files

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

Do one of the following:

- Click **Upload File** to upload a text file with an IP address list. Click the **Add** button to include the address list in your custom list.
  - 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.

  Manually enter your item in the space provided in the Custom List section. To add more items, click + to add more spaces.

  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.

---

Table 20: Fields on the Custom Feeds Page, Feedswith Remote File Server

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 20: Fields on the Custom Feeds Page, Feeds with Remote File Server (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Server URL</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• http</td>
</tr>
<tr>
<td></td>
<td>• https</td>
</tr>
<tr>
<td>Server File URL</td>
<td>Enter the URL for the remote file server.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the credentials for the remote file server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the credentials for the remote file server.</td>
</tr>
<tr>
<td>Update Interval</td>
<td>Select how often updates are retrieved from the remote file server: Hourly, Daily, Weekly, Monthly, Never</td>
</tr>
</tbody>
</table>

Related Documentation
- Creating Custom Feeds, Dynamic, Black and White on page 92
- Custom Feed Sources Overview on page 91
- Sky ATP Realm Overview on page 78

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.
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.)

Blacklist and Whitelist

Emails are checked against administrator-configured blacklists and whitelists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches the whitelist, that email is allowed through without any scanning. If an email matches the blacklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

Related Documentation

- Sky ATP Email Management: SMTP Settings on page 98
- Sky ATP Email Management: Whitelists and Blacklists

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 97 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 21: Configure Quarantine Malicious Messages

<table>
<thead>
<tr>
<th>Setting</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action to take</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release option</th>
<th><strong>Action to take</strong></th>
<th><strong>Release option</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 Release the email or Delete it. Either action causes a message to be sent to the administrator.</td>
<td>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 Request to Release the email or Delete 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.</td>
</tr>
</tbody>
</table>

**NOTE:** 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.

**NOTE:** 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.

### Email Notifications for End Users

<table>
<thead>
<tr>
<th>Setting</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Learn More Link URL</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>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 &quot;Malware Detected.&quot;</td>
</tr>
<tr>
<td><strong>Custom Message</strong></td>
<td>Enter information to help email recipients understand what they should do next.</td>
</tr>
</tbody>
</table>
Table 21: Configure Quarantine Malicious Messages *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Link Text</td>
<td>Enter custom text for the Sky ATP quarantine portal link where recipients can preview quarantined emails and take action on them.</td>
</tr>
</tbody>
</table>

**Buttons**
- Click **Preview** to view the custom message that will be sent to a recipient when an email is quarantined. Then click **Save**.
- Click **Reset** to clear all fields without saving.
- Click **Save** if you are satisfied with the configuration.

Table 22: Configure Deliver with Warning Headers

<table>
<thead>
<tr>
<th>Setting</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to take</td>
<td>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.</td>
</tr>
</tbody>
</table>

**SMTP Headers**
- 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.”
- 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.”
- Subject Prefix—You can prepend headers with information for the recipient, such as “Possible Spam.”

**Buttons**
- Click **Reset** to clear all fields without saving.
- Click **OK** if you are satisfied with the configuration.

Table 23: Permit

<table>
<thead>
<tr>
<th>Setting</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to take</td>
<td>Permit—You can select to permit the message and no further configuration is required.</td>
</tr>
</tbody>
</table>

**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 on page 97
- Sky ATP Email Management: Whitelists and Blacklists

## Sky ATP Email Management: Whitelists and Blacklists

Access this page from **Configure > Threat Prevention > Sky ATP Email Management** and choose either the **Whitelist** or **Blacklist** tab.

Use custom blacklists and whitelists to filter email attachments.

- Read the “Sky ATP Email Management Overview” on page 97 topic.
- Compile a list of known malicious email addresses or domains to add to your blacklist. If an email matches the blacklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment, blocked and a replacement email is sent. If an email matches the whitelist, that email is allowed through without any scanning.
- It is worth noting that attackers can easilyfake the “From” email address of an email, making blacklists a less effective way to stop malicious emails.

The procedure for adding addresses to blacklists and whitelists is the same, although the results are very different. Be sure you are adding the entry to the correct list.

1. Select **Configure > Email Management > Whitelist** or **Blacklist**.

2. Click the + sign to add a new entry.

3. 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 on page 97

## 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 whitelists and blacklists.

- 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 whitelist and blacklist pages to configure custom trusted and untrusted URLs and IPs. Content downloaded from locations on the whitelist is trusted and does not have to be inspected for malware. Hosts cannot download content from locations on the blacklist because those locations are untrusted.

Related Documentation
- Creating File Inspection Profiles on page 103
- Creating Whitelists and Blacklists on page 104

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 24: File Category Contents

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>Archive files</td>
</tr>
<tr>
<td>Configuration</td>
<td>Configuration files</td>
</tr>
<tr>
<td>Document</td>
<td>All document types except PDFs</td>
</tr>
<tr>
<td>Executable</td>
<td>Executable binaries</td>
</tr>
<tr>
<td>Java</td>
<td>Java applications, archives, and libraries</td>
</tr>
<tr>
<td>Library</td>
<td>Dynamic and static libraries and kernel modules</td>
</tr>
<tr>
<td>Mobile</td>
<td>Mobile formats</td>
</tr>
<tr>
<td>OS package</td>
<td>OS-specific update applications</td>
</tr>
<tr>
<td>PDF</td>
<td>PDF, e-mail, and MBOX files</td>
</tr>
<tr>
<td>Rich Application</td>
<td>Installable Internet Applications such as Adobe Flash, JavaFX, Microsoft Silverlight</td>
</tr>
<tr>
<td>Script</td>
<td>Scripting files</td>
</tr>
</tbody>
</table>

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.

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 102 topic.
- Read the “File Scanning Limits” on page 120 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 25 on page 103 for the list of file types for each category.

5. Click OK.

### Table 25: File Category Contents

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active media</td>
<td>Flash and Silverlight applications</td>
</tr>
<tr>
<td>Archive</td>
<td>Archive files</td>
</tr>
</tbody>
</table>
Table 25: File Category Contents (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>Source code</td>
</tr>
<tr>
<td>Config</td>
<td>Configuration files</td>
</tr>
<tr>
<td>Document</td>
<td>All document types except PDFs</td>
</tr>
<tr>
<td>Emerging threat</td>
<td>A special category that includes known threat source file types</td>
</tr>
<tr>
<td>Executable</td>
<td>Executable binaries</td>
</tr>
<tr>
<td>Java</td>
<td>Java applications, archives, and libraries</td>
</tr>
<tr>
<td>Library</td>
<td>Dynamic and static libraries and kernel modules</td>
</tr>
<tr>
<td>Media</td>
<td>Audio video formats</td>
</tr>
<tr>
<td>OS package</td>
<td>OS-specific update applications</td>
</tr>
<tr>
<td>Script</td>
<td>Scripting files</td>
</tr>
<tr>
<td>Portable document</td>
<td>PDF, e-mail, and MBOX files</td>
</tr>
</tbody>
</table>

**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 on page 102
- Sky ATP Malware Management Overview on page 101
- File Scanning Limits on page 120

**Creating Whitelists and Blacklists**

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 26 on page 105.
To configure whitelists and blacklists:

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 26 on page 105 for syntax requirements.

5. Click OK.

Table 26: Whitelist and Black Syntax

<table>
<thead>
<tr>
<th>Setting</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>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.</td>
</tr>
<tr>
<td>URL</td>
<td>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.</td>
</tr>
</tbody>
</table>

To edit an existing whitelist or blacklist 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 whitelist or blacklist files.

Related Documentation
- Sky ATP Malware Management Overview on page 101
- Creating File Inspection Profiles on page 103
CHAPTER 10

Threat Prevention– Monitor

• Policy Enforcer Dashboard Widgets on page 107
• Infected Hosts Overview on page 108
• Infected Host Details on page 109
• Command and Control Servers Overview on page 110
• Command and Control Server Details on page 111
• HTTP File Download Overview on page 113
• HTTP File Download Details on page 114
• SMTP Quarantine Overview on page 116
• Email Attachments Scanning Overview on page 118
• Email Attachments Scanning Details on page 119
• File Scanning Limits on page 120

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 27: Sky ATP Dashboard Widgets

<table>
<thead>
<tr>
<th>Widget</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Malware Identified</td>
<td>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.</td>
</tr>
<tr>
<td>Top Compromised Hosts</td>
<td>A list of the top compromised hosts based on their associated threat level and blocked status.</td>
</tr>
<tr>
<td>Top Infected File Types</td>
<td>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.</td>
</tr>
<tr>
<td>Top Infected File Categories</td>
<td>A graph of the top infected file categories. Examples: executables, archived files, libraries. Use the arrows to filter by threat level and time frame.</td>
</tr>
<tr>
<td>Top Scanned File Types</td>
<td>A graph of the top file types scanned for malware. Examples: exe, pdf, ini, zip. Use the arrows to filter by different time frames.</td>
</tr>
<tr>
<td>Top Scanned File Categories</td>
<td>A graph of the top file categories scanned for malware. Examples: executables, archived files, libraries. Use the arrows to filter by different time frames.</td>
</tr>
<tr>
<td>C&amp;C Server and Malware Source</td>
<td>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.</td>
</tr>
</tbody>
</table>

Related Documentation

- Infected Hosts Overview on page 108
- Command and Control Servers Overview on page 110
- HTTP File Download Overview on page 113
- SMTP Quarantine Overview on page 116

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 on page 109
- HTTP File Download Overview on page 113
- HTTP File Download Details on page 114
- Email Attachments Scanning Overview on page 118
- Email Attachments Scanning Details on page 119
- Manual Scanning Overview
- File Scanning Limits on page 120

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 28: Threat Level Definitions

<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Clean; no action is required.</td>
</tr>
<tr>
<td>1–3</td>
<td>Low threat level. Recommendation: Disable this host.</td>
</tr>
<tr>
<td>4–6</td>
<td>Medium threat level. Recommendation: Disable this host.</td>
</tr>
<tr>
<td>7–10</td>
<td>High threat level. Host has been automatically blocked.</td>
</tr>
</tbody>
</table>

- 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 on page 108
- HTTP File Download Overview on page 113
- HTTP File Download Details on page 114
- Manual Scanning Overview
- File Scanning Limits on page 120
- Policy Enforcer Dashboard Widgets on page 107

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 29: Command & Control Server Data Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>C&amp;C Server</td>
<td>The IP address of the suspected command and control server.</td>
</tr>
<tr>
<td>C&amp;C Threat Level</td>
<td>The threat level of the C&amp;C server as determined by an analysis of actions and behaviors.</td>
</tr>
<tr>
<td>Hits</td>
<td>The number of times the C&amp;C server has attempted to contact hosts on your network.</td>
</tr>
<tr>
<td>C&amp;C Country</td>
<td>The country where the C&amp;C server is located.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The date and time of the most recent C&amp;C server hit.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol (TCP or UDP) the C&amp;C server used to attempt communication.</td>
</tr>
<tr>
<td>Client Host</td>
<td>The IP address of the host the C&amp;C server attempted to communicate with.</td>
</tr>
<tr>
<td>Action</td>
<td>The action taken on the communication (permitted or blocked).</td>
</tr>
</tbody>
</table>

Related Documentation
- Command and Control Server Details on page 111
- HTTP File Download Overview on page 113
- Email Attachments Scanning Overview on page 118
- Email Attachments Scanning Details on page 119
- Manual Scanning Overview
- File Scanning Limits on page 120

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 30: Command & Control Server Contacted Host Data**

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Host</td>
<td>The name of the host in contact with the command and control server.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>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.)</td>
</tr>
<tr>
<td>C&amp;C Threat Level</td>
<td>The threat level of the C&amp;C server as determined by an analysis of actions and behaviors.</td>
</tr>
<tr>
<td>Action</td>
<td>The action taken on the communication (permitted or blocked).</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol (TCP or UDP) the C&amp;C server used to attempt communication.</td>
</tr>
<tr>
<td>Port</td>
<td>The port the C&amp;C server used to attempt communication.</td>
</tr>
<tr>
<td>Device Name</td>
<td>The name of the device in contact with the command and control server.</td>
</tr>
<tr>
<td>Date Seen</td>
<td>The date and time of the most recent C&amp;C server hit.</td>
</tr>
<tr>
<td>Username</td>
<td>The name of the host user in contact with the command and control server.</td>
</tr>
</tbody>
</table>

**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 on page 110
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 31: HTTP Scanning Data Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Signature</td>
<td>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.</td>
</tr>
<tr>
<td>Threat Level</td>
<td>The threat score.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Click the three vertical dots at the top of the column to filter the information on the page by threat level.</td>
</tr>
<tr>
<td>Filename</td>
<td>The name of the file, including the extension.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Enter text in the space at the top of the column to filter the data.</td>
</tr>
<tr>
<td>Last Submitted</td>
<td>The time and date of the most recent scan of this file.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL from which the file originated.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Enter text in the space at the top of the column to filter the data.</td>
</tr>
</tbody>
</table>
Table 31: HTTP Scanning Data Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>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 &quot;clean.&quot;</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Enter text in the space at the top of the column to filter the data.</td>
</tr>
<tr>
<td>Category</td>
<td>The type of file. Examples: PDF, executable, document.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Enter text in the space at the top of the column to filter the data.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- HTTP File Download Details on page 114
- SMTP Quarantine Overview on page 116
- Email Attachments Scanning Overview on page 118
- File Scanning Limits on page 120

**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 32: General Summary Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Level</td>
<td>This is the assigned threat level 0-10. 10 is the most malicious.</td>
</tr>
<tr>
<td>Action Taken</td>
<td>The action taken based on the threat level and host settings: block or permit.</td>
</tr>
<tr>
<td>Global Prevalence</td>
<td>How often this file has been seen across different customers.</td>
</tr>
<tr>
<td>Last Scanned</td>
<td>The time and date of the last scan to detect the suspicious file.</td>
</tr>
<tr>
<td>File Name</td>
<td>The name of the suspicious file. Examples: unzippy-set.exe, 20160223158005.exe. wordmui.msi.</td>
</tr>
<tr>
<td>Category</td>
<td>The type of file. Examples: PDF, executable, document.</td>
</tr>
<tr>
<td>File Size</td>
<td>The size of the downloaded file.</td>
</tr>
<tr>
<td>Platform</td>
<td>The target operating system of the file. Example. Win32</td>
</tr>
<tr>
<td>Malware Name</td>
<td>If possible, Sky ATP determines the name of the malware.</td>
</tr>
<tr>
<td>Malware Type</td>
<td>If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.</td>
</tr>
<tr>
<td>Malware Strain</td>
<td>If possible, Sky ATP determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.</td>
</tr>
<tr>
<td>sha256 and md5</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 IP addresses 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, whitelist, and blacklist 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 on page 114
- SMTP Quarantine Overview on page 116
- Email Attachments Scanning Overview on page 118
- Manual Scanning Overview
- File Scanning Limits on page 120
- Policy Enforcer Dashboard Widgets on page 107

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 blacklist.

The following information is available from the Summary View:

Table 33: Blocked Email Summary View

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range</td>
<td>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.</td>
</tr>
<tr>
<td>Total Email Scanned</td>
<td>This lists the total number of emails scanned during the chosen time-frame and then categorizes them into blocked, quarantined, released, and permitted emails.</td>
</tr>
<tr>
<td>Malicious Email Count</td>
<td>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.</td>
</tr>
<tr>
<td>Emails Scanned</td>
<td>This is a graphical representation of emails, organized by time, with lines for total emails, and emails with one or more attachments.</td>
</tr>
<tr>
<td>Email Classification</td>
<td>This is another graphical view of classified emails, organized by percentage of blocked emails, quarantined and not released emails, and quarantined and released emails.</td>
</tr>
</tbody>
</table>

The following information is available from the Detail View:

Table 34: Blocked Email Detail View

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient</td>
<td>The email address of the recipient.</td>
</tr>
</tbody>
</table>
### Table 34: Blocked Email Detail View (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>The email address of the sender.</td>
</tr>
<tr>
<td>Subject</td>
<td>Click the <strong>Read This</strong> link to go to the Sky ATP quarantine portal and preview the email.</td>
</tr>
<tr>
<td>Date</td>
<td>The date the email was received.</td>
</tr>
<tr>
<td>Malicious Attachment</td>
<td>Click on the attachment name to go to the Sky ATP file scanning page where you can view details about the attachment.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the attachment in kilobytes.</td>
</tr>
<tr>
<td>Threat Score</td>
<td>The threat score of the attachment, 0-10, with 10 being the most malicious.</td>
</tr>
<tr>
<td>Threat Name</td>
<td>The type of threat found in the attachment, for example, worm or trojan.</td>
</tr>
<tr>
<td>Action</td>
<td>The action taken, including the date and the person (recipient or administrator) who took the action.</td>
</tr>
</tbody>
</table>

Using the available buttons on the Details page, you can take the following actions on blocked emails:

- Add domain to blacklist
- Add sender to blacklist
- Release

**Related Documentation**
- HTTP File Download Overview on page 113
- HTTP File Download Details on page 114
- Email Attachments Scanning Overview on page 118
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 35: Email Attachments Scanning Data Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Signature</td>
<td>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.</td>
</tr>
<tr>
<td>Threat Level</td>
<td>The threat score.</td>
</tr>
<tr>
<td>Date Scanned</td>
<td>The date and time the file was scanned.</td>
</tr>
<tr>
<td>Filename</td>
<td>The name of the file, including the extension.</td>
</tr>
<tr>
<td>Recipient</td>
<td>The email address of the intended recipient.</td>
</tr>
<tr>
<td>Sender</td>
<td>The email address of the sender.</td>
</tr>
<tr>
<td>Malware Name</td>
<td>The type of malware found.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the file was blocked or permitted.</td>
</tr>
<tr>
<td>Category</td>
<td>The type of file. Examples: PDF, executable, document.</td>
</tr>
</tbody>
</table>

Related Documentation:
- Email Attachments Scanning Details on page 119
- SMTP Quarantine Overview on page 116
- Manual Scanning Overview
- File Scanning Limits on page 120
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 36: General Summary Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Level</td>
<td>This is the assigned threat level 0-10. 10 is the most malicious.</td>
</tr>
<tr>
<td>Action Taken</td>
<td>The action taken based on the threat level and host settings: block or permit.</td>
</tr>
<tr>
<td>Global Prevalence</td>
<td>How often this file has been seen across different customers.</td>
</tr>
<tr>
<td>Last Scanned</td>
<td>The time and date of the last scan to detect the suspicious file.</td>
</tr>
<tr>
<td>File Name</td>
<td>The name of the suspicious file. Examples: unzippersetup.exe, 20160223158005.exe, wordmui.msi.</td>
</tr>
<tr>
<td>Category</td>
<td>The type of file. Examples: PDF, executable, document.</td>
</tr>
<tr>
<td>File Size</td>
<td>The size of the downloaded file.</td>
</tr>
<tr>
<td>Platform</td>
<td>The target operating system of the file. Example. Win32</td>
</tr>
<tr>
<td>Malware Name</td>
<td>If possible, Sky ATP determines the name of the malware.</td>
</tr>
</tbody>
</table>
### Table 36: General Summary Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Type</td>
<td>If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.</td>
</tr>
<tr>
<td>Malware Strain</td>
<td>If possible, Sky ATP determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.</td>
</tr>
<tr>
<td>sha256 and md5</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

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 on page 118
- Infected Hosts Overview on page 108
- HTTP File Download Overview on page 113
- SMTP Quarantine Overview on page 116
- Manual Scanning Overview
- File Scanning Limits on page 120
- Policy Enforcer Dashboard Widgets on page 107

### 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."

<table>
<thead>
<tr>
<th>Perimeter Device</th>
<th>Free License (files per day)</th>
<th>Premium License (files per day)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRX340</td>
<td>200</td>
<td>1,000</td>
</tr>
<tr>
<td>SRX345</td>
<td>300</td>
<td>2,000</td>
</tr>
<tr>
<td>SRX550m</td>
<td>500</td>
<td>5,000</td>
</tr>
<tr>
<td>SRX1500</td>
<td>2,500</td>
<td>10,000</td>
</tr>
<tr>
<td>SRX5400</td>
<td>5,000</td>
<td>50,000</td>
</tr>
<tr>
<td>SRX5600</td>
<td>5,000</td>
<td>70,000</td>
</tr>
<tr>
<td>SRX5800</td>
<td>5,000</td>
<td>100,000</td>
</tr>
<tr>
<td>vSRX(10mbps)</td>
<td>25</td>
<td>200</td>
</tr>
<tr>
<td>vSRX(100mbps)</td>
<td>200</td>
<td>1,000</td>
</tr>
<tr>
<td>vSRX(1000mbps)</td>
<td>2,500</td>
<td>10,000</td>
</tr>
<tr>
<td>vSRX(2000mbps)</td>
<td>2,500</td>
<td>10,000</td>
</tr>
<tr>
<td>vSRX(4000mbps)</td>
<td>3,000</td>
<td>20,000</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Infected Hosts Overview on page 108
- HTTP File Download Overview on page 113
- Email Attachments Scanning Overview on page 118
- Manual Scanning Overview
CHAPTER 11

Troubleshooting

- Policy Enforcer Log File Locations on page 123
- Troubleshooting Common Policy Enforcer Problems on page 124

Policy Enforcer Log File Locations

The following Policy Enforcer configuration settings files are located under /srv/feeder/etc/log:

- auto_upgrades_log.yml—Internal use only.
- config_server_log.yml—Defines the format for the config_server.log file. For example, message and date format and maximum file size.
- feeder_cleaner_log.yml—Internal use only.
- feed_scheduler_log.yml—Defines the format for the feed_scheduler.log file. For example, message and date format and maximum file size.
- feed_server_log.yml—Defines the format for the feed_server.log file. For example, message and date format and maximum file size.
- ha_vip_controller_log.yml—Internal use only.
- upgrades_cli_log.yml—Internal use only.

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, config_server.log, config_server.log.1, config_server.log.2, etc. After 10 files are created, the oldest file (in this example, config_server.log) is overwritten next.

- config_server.log—Contains log messages for the interaction of Security Director with Policy Enforcer.
- feed_scheduler.log—Contains log messages for the downloading of feeds.
- feed_server.log—Contains log messages for distributing feeds to the SRX Series devices.

NOTE: Do not edit these files unless instructed by the Juniper Networks Technical Assistance Center (JTAC).
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

This topic lists some common problem areas you may encounter and how to remedy them.

- Troubleshooting Policy Enforcer Installation on page 124
- Troubleshooting Sky ATP Realms and Enrolling Devices on page 124
- Troubleshooting Threat Policies and Policy Enforcement Groups on page 125
- HTTPS-Based Malware Not Detected on page 125

### 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:

```bash
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 39.