

# Spotlight Secure Connector

Published  
2020-09-29

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Spotlight Secure Connector*

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

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

## YEAR 2000 NOTICE

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

## END USER LICENSE AGREEMENT

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

# Table of Contents

## About the Documentation | vi

Documentation and Release Notes | vi

Documentation Conventions | vi

Documentation Feedback | ix

Requesting Technical Support | ix

Self-Help Online Tools and Resources | x

Creating a Service Request with JTAC | x

## 1

## Overview

### Introduction to Security Intelligence | 2

Perimeter Security Today | 2

Juniper Networks Security Intelligence | 3

Security Intelligence in the Network | 6

Dynamic Address Entry and Security Intelligence Services | 8

Dynamic Address Entry Configuration on the SRX Series Enforcement Point for Security Intelligence | 8

### Security Intelligence Configurations | 10

Security Intelligence and Command and Control Server Threats | 11

Security Intelligence and Fingerprinted Attackers | 13

Security Intelligence and Undesired Locales | 14

Security Intelligence and Custom Feeds | 15

## 2

## Initial Setup

### Configuration Steps | 18

Configuring Spotlight Secure Connector | 18

Configuring Spotlight Secure Connector Network Settings | 19

Adding Spotlight Secure Connector as a Specialized Node in Junos Space | 27

Setting Up High Availability | 32

Spotlight Secure Connector General Settings Overview | 34

Associating an SRX Series Device With Spotlight Secure Connector | 36

About Trusted Server CAs | 42

Updating the Schema | 43

Managing Spotlight Secure Connectors | 44

Adding Spotlight Secure Connector Global Settings | 45

Uploading Trusted Server CAs | 46

Associating Devices to Spotlight Secure Connectors | 47

Updating Spotlight Secure Connector Configuration | 49

Deleting Spotlight Secure Connectors | 50

Viewing Spotlight Secure Connector Feed Status | 50

Upgrading Spotlight Secure Connector Software or Package | 51

Creating a Backup or Restoring the Connector Settings | 52

### 3

## Configuring Spotlight Secure Connector in Security Director

Configuring the Information Sources | 54

Spotlight Secure Connector Information Source Overview | 54

Allowlist and Blocklists | 55

Geolocation IP Address | 57

Command and Control Lists | 59

WebApp Secure Threats | 61

About Custom Address Lists | 64

Feed Status | 64

Information Source Update Interval | 65

Creating an Information Source | 66

Managing Information Sources | 68

Modifying an Information Source | 69

Deleting an Information Source | 69

Updating Feeds to Connectors | 69

## Configuring Profiles and Policies | 71

Spotlight Secure Connector Profile Overview | 71

About Threat Levels | 72

Verifying Profiles On the SRX Series Device | 75

Creating Security Intelligence Profiles | 76

Managing Security Intelligence Profiles | 80

Modifying a Security Intelligence Profile | 80

Deleting a Security Intelligence Profile | 81

Modifying a Global Allowlist or Global Blocklist | 81

Spotlight Secure Connector Policy Overview | 81

Creating Security Intelligence Policies | 83

Managing Security Intelligence Policies | 85

Modifying a Security Intelligence Policy | 85

Deleting a Security Intelligence Policy | 85

## Applying Spotlight Secure to Security Rules | 87

Using Spotlight Secure Connector Policies in Security Rules | 87

Dynamic Address Group Overview | 91

Creating Dynamic Address Groups | 95

Managing Dynamic Address Groups | 97

Modifying a Dynamic Address Group | 98

Deleting an Address from a Dynamic Address Group | 99

## 4

## Examples

### Configuration Examples | 101

Example: Pushing a Allowlist, Blocklist, C&C, and GeolIP to a Security Device | 101

Defining the Information Sources | 101

Creating the Profiles | 105

Creating the Spotlight Secure Policy | 110

Creating the Dynamic Address Groups | 111

Associating the SRX Series Device With the Connector | 112

Creating the Firewall Policy and Rules | 113

# About the Documentation

## IN THIS SECTION

- Documentation and Release Notes | vi
- Documentation Conventions | vi
- Documentation Feedback | ix
- Requesting Technical Support | ix

## Documentation and Release Notes

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

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

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

## Documentation Conventions

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

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

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

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

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

## GUI Conventions



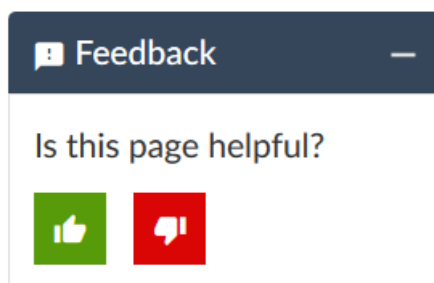
Table 2: Text and Syntax Conventions (*continued*)

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

## Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

## Creating a Service Request with JTAC

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

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

# 1

PART

## Overview

---

Introduction to Security Intelligence | 2

Security Intelligence Configurations | 10

---

# Introduction to Security Intelligence

## IN THIS CHAPTER

- [Perimeter Security Today | 2](#)
- [Juniper Networks Security Intelligence | 3](#)
- [Dynamic Address Entry and Security Intelligence Services | 8](#)

## Perimeter Security Today

Threats to your network continue to evolve. And defensive software and appliances that you can deploy to defend your network, and the assets that are available through your network, are becoming more complex. The typical approach to dealing with new security threats is to add layers of security. Defense in depth is a basic approach to network security, but it adds complexity by adding gateways that must often be managed and configured separately. The complexity of the system can slow your ability to react and respond to a threat.

Traditional network perimeter security uses stateful firewall protection and intrusion prevention tied to an enterprise business policy. This type of enforcement works well against known threats. The emergence of next-generation firewalls combined with unified threat management (UTM) has allowed a more granular degree of filtering. These integrated security functions expand security measures beyond basic stateful firewall filtering. However, the security policies must be manually configured and maintained in most cases.

The threat landscape has evolved. Attackers have migrated from using broad, unfocused tactics and are now creating specialized malware that attacks specific targets or groups of targets. Often, the goal of these attacks is to embed malware in the target's infrastructure and continue the attack, without detection, over long periods. If malware infiltrates a rich target, it can carry out a wide range of undetected malicious activities over months or years, including data theft, espionage, and disruption or destruction of infrastructure and processes. While methods vary, the commonality of these specialized attacks is that they are designed to avoid detection by mainstream security technologies, such as antivirus, firewalls, and content inspection gateways.

To respond more quickly to evolving network security threats, the next-generation firewall must adapt dynamically in real time. The next-generation firewall needs access to external threat detection systems that are updated dynamically with information about new and evolving threats. With access to dynamic threat data, security policies can adapt and evolve over time without manual intervention.

## RELATED DOCUMENTATION

[Juniper Networks Security Intelligence](#) | 3

## Juniper Networks Security Intelligence

Juniper Networks Security Intelligence (SecIntel) is a security framework that protects web servers in the DMZ against evolving security threats by employing threat detection software, both local and cloud-based security information, and control software with a next-generation firewall system.

SecIntel delivers dynamic threat intelligence to the firewall. It enables automatic and dynamic traffic filtering at both the network and application layers. A SecIntel solution includes, at a minimum, one or more Juniper Networks SRX Series Services Gateways and Spotlight Secure Connector, a premises-hosted application that accepts and distributes threat intelligence information to enforcement points. In addition, the SecIntel framework integrates Juniper Networks WebApp Secure, which protects websites from attackers by using Web intrusion prevention to detect, track, profile, and block attackers in real time, and Log Director for detailed logging, reporting, and event visualization of SRX Series activity. Optional Spotlight Secure cloud-based threat intelligence feeds provide a stream of information about evolving threats that is gathered, analyzed, and prioritized by Juniper Networks from multiple collection points.

SecIntel offers the following features:

- Dynamic security policies and flexible enforcement options on the firewall to react to rapidly changing threats. The security policy on the firewall can use dynamic intelligence sources, both local and cloud based. The SecIntel security policy enables a wide range of enforcement actions beyond just “allow” or “deny.”
- An open platform approach that can adapt to customer needs and use cases. You can easily employ local intelligence and third-party information sources in threat recognition.
- Tunable controls. The SecIntel security policy recognizes threat levels, which allows you to fine-tune your security policy response to different types of threats.
- Centrally managed security data for one or many firewalls. One control point brokers the feeds from the data sources and passes the information directly to the firewall security policies.
- Actionable intelligence with fewer false positives. Normalized threat scores enable intuitive security policies. Cloud-based security intelligence and prioritized threat feeds maximize firewall resources.

SecIntel employs the following threat-detection mechanisms:

- **Juniper Networks WebApp Secure**—WebApp Secure protects websites from attackers. Its Web intrusion prevention system uses deception to detect, track, profile, and block attackers in real time by inserting detection points into your webserver's output to identify attackers before they can do damage. WebApp Secure then tracks the attackers, profiles their behavior, and deploys countermeasures.

WebApp Secure sits between your web servers and the outside world. It inspects HTTP and HTTPS traffic and functions as a reverse proxy. WebApp Secure seeks out potential attack attempts or probes by adding detection points to outbound Web traffic and removing detection points from inbound Web traffic. These detection points are transparent to common, legitimate users. It then monitors and strips these points from the requests coming back from the user's browser. Any change to a detection point is an indicator of an attempted attack. The system logs incidents to a database of attacker profiles and exposes them to the security administrators through a Web-based interface. System administrators can then apply automated abuse-prevention policies or respond manually.

SecIntel uses the following information sources:

- **Spotlight Secure**—Spotlight Secure, formerly known as Spotlight Cloud, is a cloud-based dynamic intelligence service for WebApp Secure. It enables a two-way communication process that shares information about attackers and attacks to and from a Spotlight server run by Juniper Networks. The updates allow WebApp Secure to positively identify attackers that have attacked other Juniper customers. This service also provides additional details about sessions, which allows Juniper to make more informed decisions on how to respond to threats. The Spotlight Secure service provides the following information feeds that target the following specific threats:

**Spotlight Command and Control**

- Blocks Command and Control (CC) connections.
- Blocks botnet activity.
- Identifies and isolates internal infections.

**Spotlight GeoIP**

- Blocks traffic from specified countries.
- **Local and third-party information**—You can create allowlists and blocklists using locally derived information and use it as part of your firewall security policies. A allowlist is a list of known IP addresses that you trust, and a blocklist identifies IP addresses that you do not trust. You configure the lists through Spotlight Secure Connector. Typically, you configure a security policy to either allow traffic from allowlist addresses and prevent everything else or block blocklist address traffic and allow everything else. You can create your own lists or obtain lists from a third-party vendor.

Spotlight Secure Connector is the central connection point between information sources and enforcement points. Spotlight Secure Connector receives the information feeds from Spotlight Secure and from the locally defined information sources, and makes that threat information available to the enforcement points. Spotlight Secure Connector manages the flow of threat information and serves as the interface where the

security administrator defines and publishes security policies to the enforcement points. Spotlight Secure Connector is a virtual machine that runs within the Juniper Space Fabric and is managed through Security Director. Junos Space is a comprehensive network management solution that enables management applications that improve the agility of network platforms and applications.

**NOTE:** The Spotlight Secure Connector information consumers periodically query Spotlight Secure Connector for updates. Spotlight Secure Connector does not push data to the consumers.

Figure 1: Junos Space > Security Director > Security Intelligence



Enforcement points (security devices):

- SecIntel uses SRX Series Services Gateways as enforcement points.

SRX Series Services Gateways are high-performance network security solutions for enterprises and service providers. SRX Series deliver next-generation firewall protection with application awareness, intrusion prevention system (IPS), and extensive user role-based control options. Next-generation firewalls can perform full packet inspection and can apply security policies based on Layer 7 information. You configure security policies from within Spotlight Secure Connector and then publish them to the enforcement points. The *Security Intelligence Supported Platforms Guide* provides complete details on supported enforcement points.

## Security Intelligence in the Network

Figure 2 on page 7 shows the how the components of the SecIntel solution work together.





## Dynamic Address Entry and Security Intelligence Services

In a typical security environment, traffic flowing across an enforcement point is evaluated against a security policy that is defined on that enforcement point. When a policy match occurs, a specific action, such as block, is applied to the traffic. The threat information that is used by the security policy to evaluate the traffic, typically IP source and destination addresses, is part of the policy.

A Dynamic Address Entry (DAE) provides dynamic IP address information to security policies. A DAE is a group of IP addresses, not just a single IP prefix, that can be imported into Spotlight Secure Connector 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. The administrator can then configure security policies to use the DAE within a security policy. When the DAE is updated, the changes automatically become part of the security policy. There is no need to update the policy manually.

Any data source that is available to Spotlight Secure Connector can be used as a DAE.

### Dynamic Address Entry Configuration on the SRX Series Enforcement Point for Security Intelligence

Security Intelligence feeds support security policy enforcements without requiring a configuration commit action. After you have created a security policy through Security Director and published it to one or more SRX Series enforcement points, updated threat intelligence updates are passed from Spotlight Secure Connector to the SRX Series enforcement point automatically.

A category is a list of feeds of the same type. The type defines SRX Series enforcement point criteria for feed lookup and enforcement. A feed is a collection of objects, and an object defines criteria for a positive threat match. A SecIntel object can be of the following types:

- IP addresses—IPv4 or IPv6 Classless Interdomain Routing (CIDR) ranges, prefixes, or a single address entry.
- Command and Control servers—IP addresses, URLs, and domain names. SRX Series enforcement points support IPv4 URLs for Command and Control (CC) objects.
- WebApp Secure—IP addresses and session cookies that WebApp Secure uses to track potentially malicious (Web) clients.

An object is declared as matched only if all the criteria within that object have matched. For example, a CC object might have IP, URL, domain name, and/or IPS signature in combination or in isolation.

Some typical examples of object matching criteria include the following:

- Always allow specific IP addresses (allowlist) to minimize false positives.

- Always deny or redirect certain IP addresses (blocklist) to minimize false negatives.

The security policy enforces the following policy match hierarchy:

- Firewall policies. Allowlist, blocklist, and other policies including GeoIP are matched first.
- SecIntel service policies based on allowlist feeds, blocklist feeds, and other service feeds including CC and WebApp Secure feeds.

The Dynamic Address Entry (DAE) feature allows feed-based IP objects to be used in security policies to either deny or allow traffic based on either source or destination IP criteria. The key difference with DAE is that feed data on SRX Series enforcement points can be updated dynamically; no configuration commit action is required.

A security administrator defines the DAE as an import of IP objects (an IP list feed) using Security Director, and uses the DAE in firewall security policies.

The properties for IP lists can include the following:

- Severity
- GeoIP filters (Country, County, City, Zip, and so on)

## RELATED DOCUMENTATION

| [Juniper Networks Security Intelligence](#) | 3

# Security Intelligence Configurations

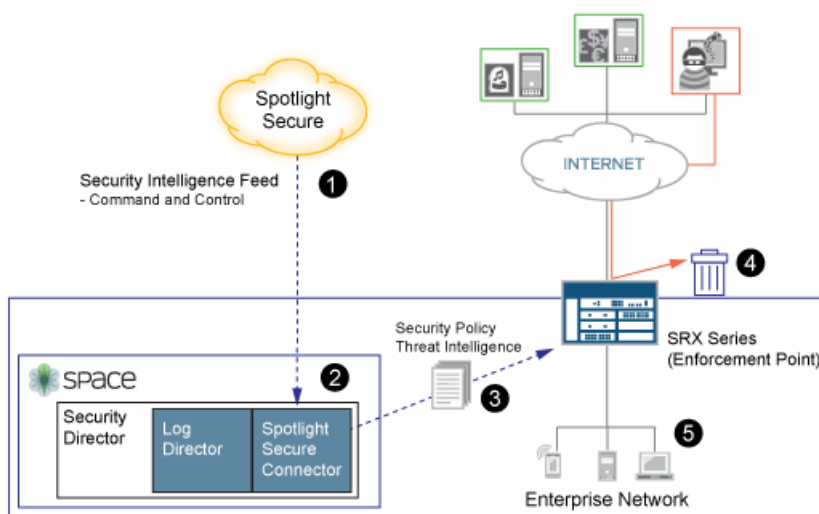
## IN THIS CHAPTER

- Security Intelligence and Command and Control Server Threats | 11
- Security Intelligence and Fingerprinted Attackers | 13
- Security Intelligence and Undesired Locales | 14
- Security Intelligence and Custom Feeds | 15

## Security Intelligence and Command and Control Server Threats

When a compromised host tries to initiate contact with a possible Command and Control (CC) server on the Internet, the SRX Series enforcement point can intercept the traffic and perform an enforcement action based on real-time feed information from Spotlight Secure Connector that identifies the CC server IP address and URL. The data feed from Spotlight Secure is automatically passed through Spotlight Secure Connector as a Dynamic Address Entry (DAE) to the security policy without requiring an explicit commit or a configuration change to the SRX Series enforcement point. [Figure 3 on page 11](#) shows how SecIntel handles a CC threat.

**Figure 3: Spotlight Secure Connector Command and Control Feed into Spotlight Connector**



- 1 Spotlight Secure delivers threat intelligence that identifies command and control servers to Spotlight Secure Connector.
- 2 Spotlight Secure Connector makes the information available to security policies on the SRX Series enforcement point. Spotlight Secure Connector brings together all of the available threat intelligence and makes it available to the security policies on the enforcement point. One instance of Spotlight Secure Connector can support many enforcement points with threat intelligence.
- 3 As the threat intelligence is updated on Spotlight Secure Connector, the SRX Series enforcement point can poll Spotlight Secure Connector to keep threat intelligence updated on the deployed security policies.
- 4 All CC server traffic that matches the feed data is discarded or redirected and the activity is tracked in Log Director. The SRX Series enforcement point security policies perform real-time enforcement.
- 5 Web application traffic is protected.

- 6 Enforcement actions include discarding or redirecting network traffic that is identified as a threat. All threat events are logged by Log Director.
- 

## RELATED DOCUMENTATION

[Security Intelligence and Fingerprinted Attackers | 13](#)

---

[Security Intelligence and Undesired Locales | 14](#)

---

[Security Intelligence and Custom Feeds | 15](#)



- 5 Web application traffic is protected.

## RELATED DOCUMENTATION

[Security Intelligence and Command and Control Server Threats | 11](#)

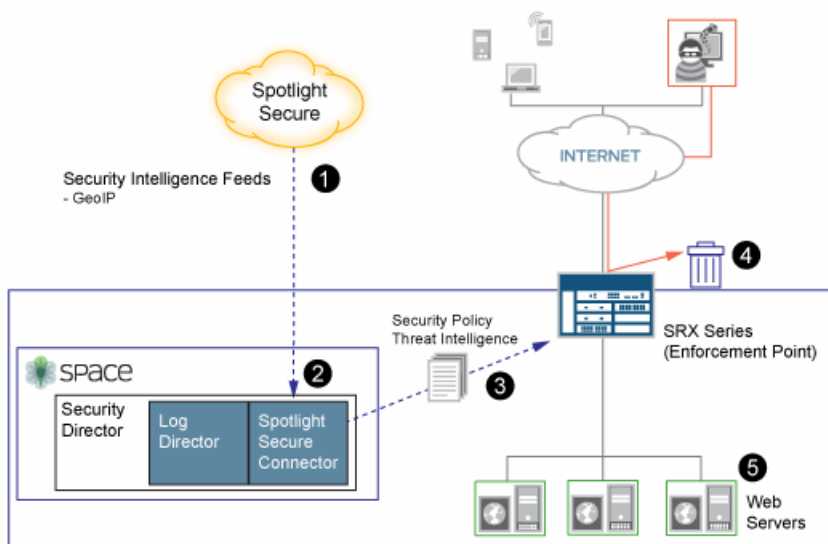
[Security Intelligence and Undesired Locales | 14](#)

[Security Intelligence and Custom Feeds | 15](#)

## Security Intelligence and Undesired Locales

Identified locations and their associated IP addresses can be profiled within a Spotlight Secure GeoIP data feed. In the event of fraudulent activity or known illegal traffic that is sourced from a particular geography, SecIntel can filter network traffic based on the location of a host. You can base packet filtering on blocks of IP addresses that have been identified and attributed to a particular geography. [Figure 5 on page 14](#) shows how SecIntel handles threats based on locales.

Figure 5: GeoIP Based Feed into Spotlight Secure Connector



- 1 Spotlight Secure delivers threat intelligence that identifies geographic locations that pose a threat to network security to Spotlight Secure Connector. Another instance of WebApp Secure identifies and collects the threat information, which is then uploaded to Juniper Networks to be analyzed and weighted. This amalgamated threat intelligence is then made available as a service to subscribers.



2	Spotlight Secure Connector makes the information available to security policies on the SRX Series enforcement point.
3	As the threat intelligence is updated on Spotlight Secure Connector, the SRX Series enforcement point can poll Spotlight Secure Connector to keep security policy threat intelligence updated on the deployed security policies.
4	<p>All traffic that matches the feed data is discarded or redirected. The SRX Series enforcement point security policies perform real-time enforcement.</p> <p>Enforcement actions include discarding or redirecting network traffic that is identified as a threat. All threat events are logged by Log Director.</p>
5	Web application traffic is protected.

## RELATED DOCUMENTATION

[Security Intelligence and Command and Control Server Threats | 11](#)

[Security Intelligence and Fingerprinted Attackers | 13](#)

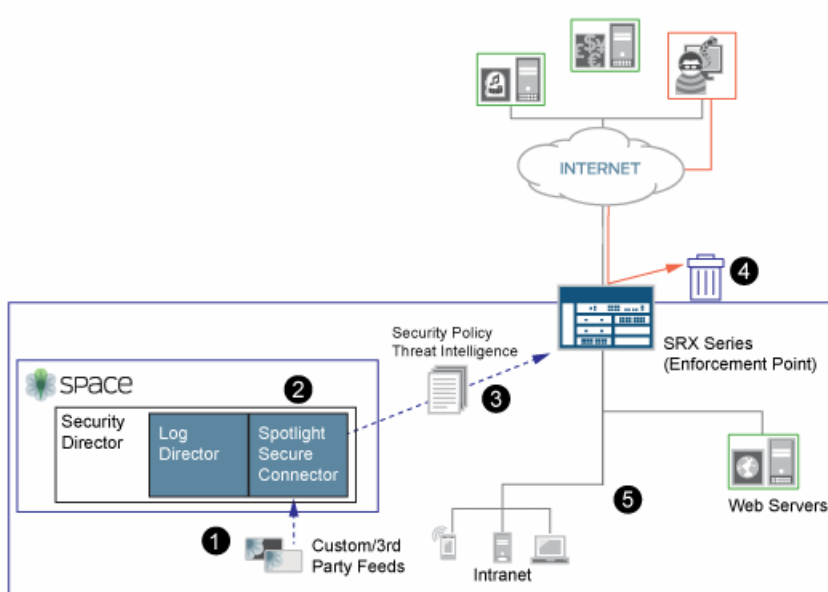
[Security Intelligence and Custom Feeds | 15](#)

## Security Intelligence and Custom Feeds

The Juniper Security Intelligence Solution (SecIntel) is designed so that you can customize it for your unique environment. For example, you can define allowlist and blocklist feeds based on local information or from a third party and include it within the SecIntel enforcement configuration.

Your custom security intelligence information that is used for policy enforcement can be provided by a trusted third party or generated from known IP addresses. The custom information must be posted in a file that is accessible to Spotlight Secure Connector. Spotlight Secure Connector polls the file according to a configured schedule and updates the SRX Series enforcement point security policy without an explicit commit or configuration change. [Figure 6 on page 16](#) shows how SecIntel uses allowlists and blocklists to protect a network.

Figure 6: Scenario for Allowlist or Blocklist Custom Feed into Spotlight Connector



1	The security administrator creates formatted lists that contain allowlisted IP addresses and blocklisted IP addresses. The security administrator can use local information and also third-party lists. The information only needs to be formatted according to the simple rules appropriate for use with Spotlight Secure Connector.
2	Spotlight Secure Connector makes the information available to security policies on the SRX Series enforcement point.
3	As the threat intelligence is updated on Spotlight Secure Connector, the SRX Series enforcement point can poll Spotlight Secure Connector to keep security policy threat intelligence updated on the deployed security policies.
4	All traffic that matches the feed data is handled according to the security policy configuration. Allowlisted addresses are allowed to pass while block listed addresses are blocked. The SRX Series enforcement point security policies perform real-time enforcement. All threat events are logged by Log Director.
5	Web application traffic is protected. False positive and false negatives are minimized.

## RELATED DOCUMENTATION

[Security Intelligence and Command and Control Server Threats | 11](#)

[Security Intelligence and Fingerprinted Attackers | 13](#)

[Security Intelligence and Undesired Locales | 14](#)

# 2

PART

## Initial Setup

---

Configuration Steps | **18**

---

# Configuration Steps

## IN THIS CHAPTER

- [Configuring Spotlight Secure Connector | 18](#)
- [Setting Up High Availability | 32](#)
- [Spotlight Secure Connector General Settings Overview | 34](#)
- [Associating an SRX Series Device With Spotlight Secure Connector | 36](#)
- [About Trusted Server CAs | 42](#)
- [Updating the Schema | 43](#)
- [Managing Spotlight Secure Connectors | 44](#)
- [Creating a Backup or Restoring the Connector Settings | 52](#)

## Configuring Spotlight Secure Connector

### IN THIS SECTION

- [Configuring Spotlight Secure Connector Network Settings | 19](#)
- [Adding Spotlight Secure Connector as a Specialized Node in Junos Space | 27](#)

Spotlight Secure Connector is delivered as an OVA package to be deployed inside your VMware ESX network. As with other Junos Space virtual appliances, the connector 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:

- 2 CPUs
- 8-GB RAM
- 80-GB disk space

You need to enter several configuration settings for Spotlight Secure Connector. You can use the following table to record your settings for later use.

Configuration Setting	Value
Spotlight Secure Connector hostname	
Spotlight Secure Connector static IP address	
Network mask	
Default gateway	
Primary and secondary DNS server	
(Optional) Failover Spotlight Secure Connector static IP address	
(Optional) Virtual IP address	
(Optional) NTP servers	
Customer ID—Your Juniper Networks-defined identifier that entitles you to use Spotlight Secure Connector. This is typically the same as the SiteID tied to your support account.	
Administrator password	

The steps to configuring the connector are as follows:

### Configuring Spotlight Secure Connector Network Settings

Once you have deployed the connector, you can configure its basic network settings.

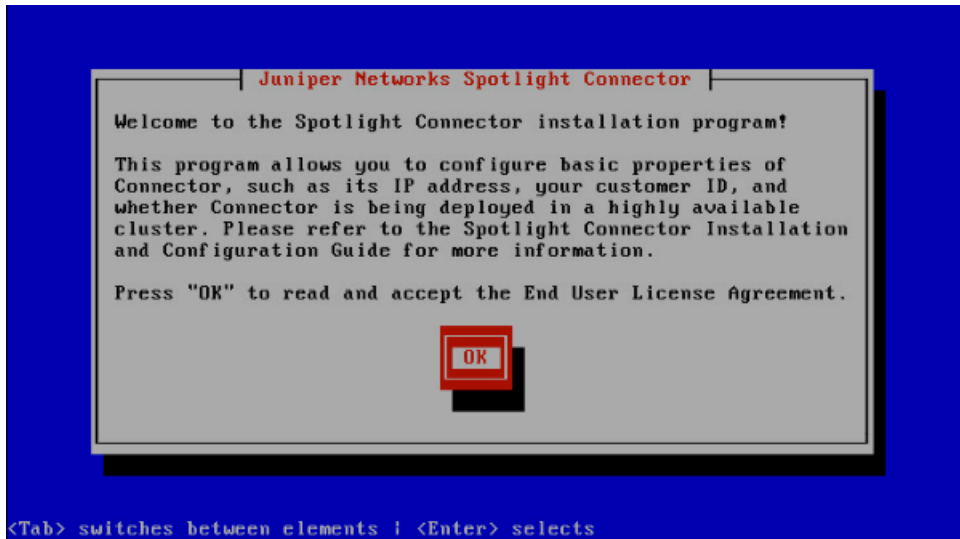
**NOTE:** When you first log in to the connector, you are prompted for credentials. The default username is **root**. The default password is **abc123**.

To configure the connector network settings:

1. Launch the vSphere Client that is connected to the ESX Server where Spotlight Secure Connector is to be deployed and power on the connector virtual machine.

The welcome page appears. See [Figure 7 on page 20](#).

Figure 7: Spotlight Secure Connector Welcome Page



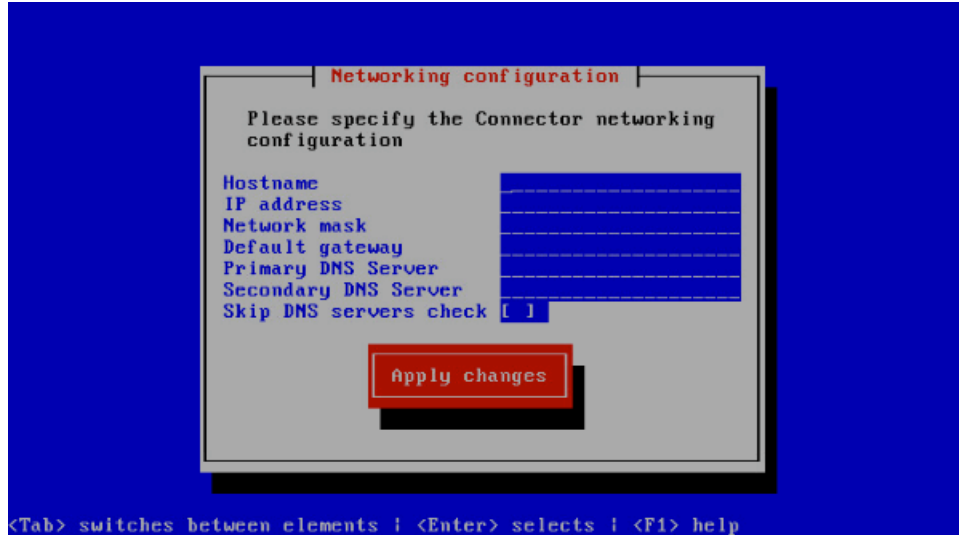
2. Click **OK**.

The End User License Agreement (EULA) window appears.

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

The Network configuration page appears. See [Figure 8 on page 21](#).

Figure 8: Defining the Basic Network Configuration Settings



4. Enter the following configuration information.

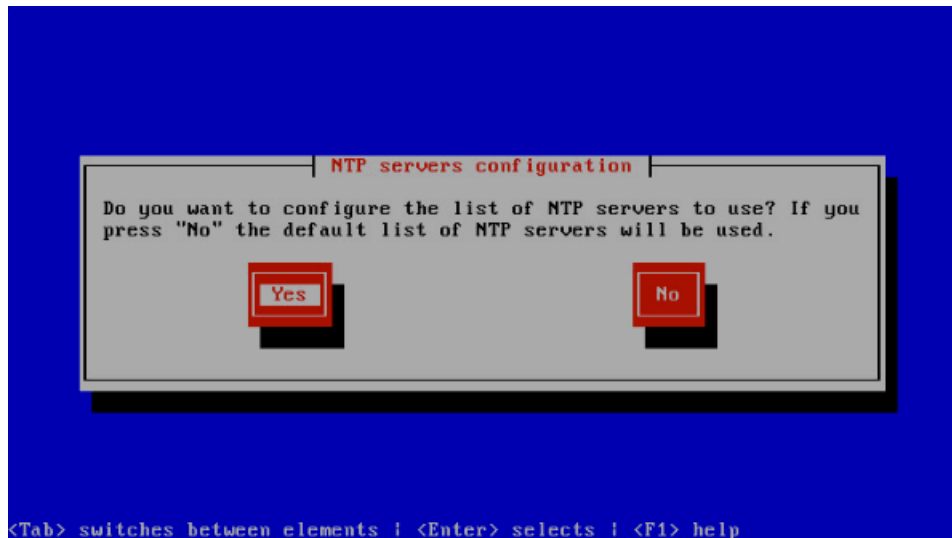
Option	Description
Hostname	Enter the hostname for the Spotlight Secure Connector virtual appliance; for example, <b>connector.juniper.net</b> .
IP address	Enter the static IP address for the Spotlight Secure Connector virtual appliance; for example, <b>172.24.1.105</b> . Spotlight Secure Connector does not support DHCP to assign its IP address.
Network mask	Enter the netmask for the Spotlight Secure Connector virtual appliance; for example, <b>255.255.255.0</b> .
Default gateway	Enter the IP address of the default gateway that connects your internal network to external networks; for example, <b>172.24.0.1</b> .
Primary DNS server	Enter the IP address of your primary system registered to join the Domain Name System (DNS); for example, <b>8.8.8.8</b> .
Secondary DNS server	Enter the IP address of a secondary DNS server; for example, <b>8.8.4.4</b> . Spotlight Secure Connector uses this address only when the primary DNS server is unavailable.
Skip DNS servers check	Select this check box if you do not want to check basic network settings. By default, the system will ping the gateway to ensure it receives a response indicating your settings are correct.

5. Click **Apply Changes**.

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

When the system is finished updating your network settings, an NTP server window appears and prompts you to configure the NTP server list. See [Figure 9 on page 22](#).

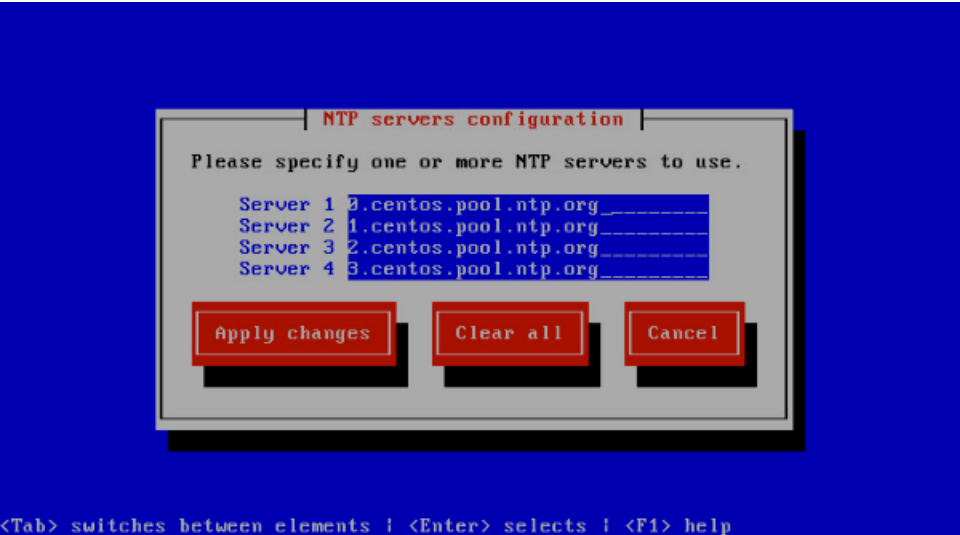
Figure 9: Prompt for Configuring the NTP Servers



6. Click **Yes** to customize the NTP server list. Click **No** to use the default list of 0, 1, 2 and 3.centos.pool.ntp.org.
7. (Optional) Specify the NTP servers to use. See [Figure 10 on page 23](#). 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 HA Cluster Configuration prompt appears.

- 8. (Optional) Click **Yes** to set up a high-availability cluster (also called a failover cluster.)

The HA Cluster Configuration page appears. See [Figure 11 on page 23](#).

Figure 11: Option to Define a Failover Device



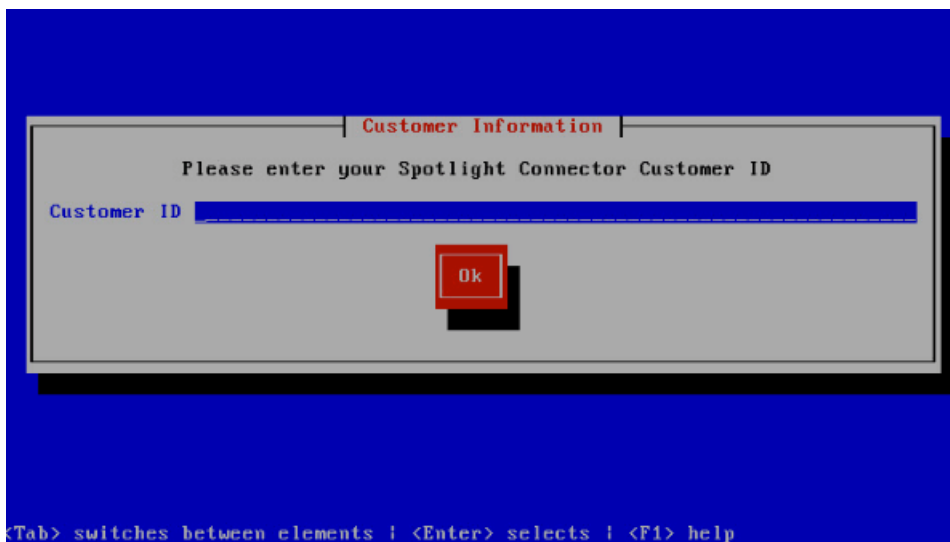
9. Enter the following configuration information.

Option	Description
Remote connector instance IP address	<p>Enter the IP address of the failover Spotlight Secure Connector virtual appliance; for example, <b>172.24.1.106</b>.</p> <p>When the primary Spotlight Secure Connector virtual appliance is unreachable, the failover Spotlight Secure Connector is used. A health check is performed every 60 seconds. Depending on the severity of the failure, failover can take between 60 seconds and 15 minutes. If the remote host cannot be reached, failover occurs in 60 seconds. If there is an internal failure in updating multiple Spotlight Secure Connector feeds, it can take up to 15 minutes for failover to occur.</p>
Virtual IP address	<p>Enter the virtual IP (VIP) shared between the two Spotlight Secure Connector hosts. The VIP serves as the primary external contact point for connected devices like the SRX Series Services Gateways. When failover occurs, the VIP is reassigned to the standby Spotlight Secure Connector host and it becomes the new active device.</p>

10. Click **Apply**.

The Customer Information page appears. See [Figure 12 on page 24](#).

**Figure 12: Entering Customer Information**

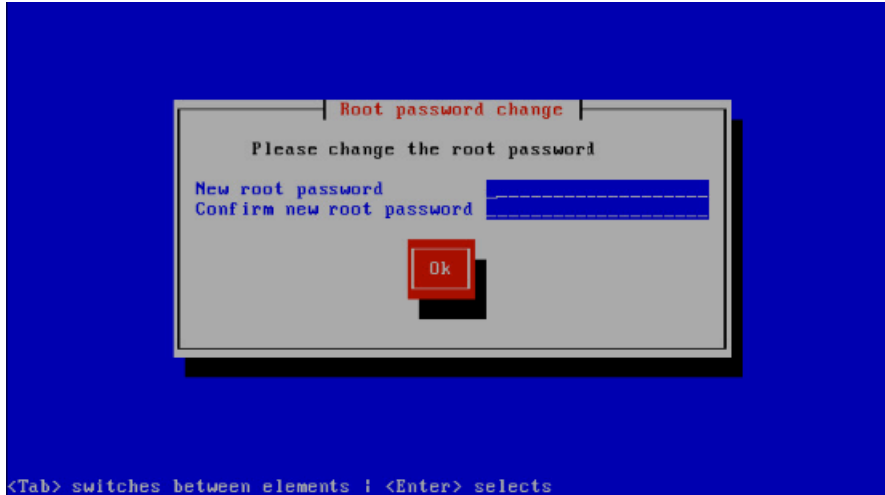


11. Enter your customer ID. This might be your SiteID tied to your support account.

12. Click **OK**.

The Root password change page appears. See [Figure 13 on page 25](#).

Figure 13: Changing the Root Password



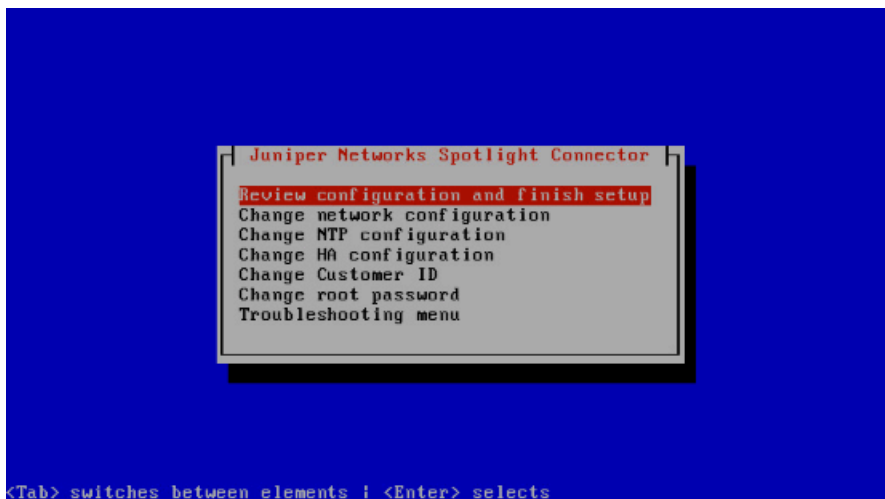
13. Enter and reenter a new administrator password for the connector virtual appliance.

Passwords must be at least eight characters in length. If you forget your password, see [CentOS root password reset instructions](#).

14. Click **OK**.

The Juniper Networks Security Intelligence Connector page appears. See [Figure 14 on page 25](#).

Figure 14: Reviewing and Changing Your Configuration Settings.

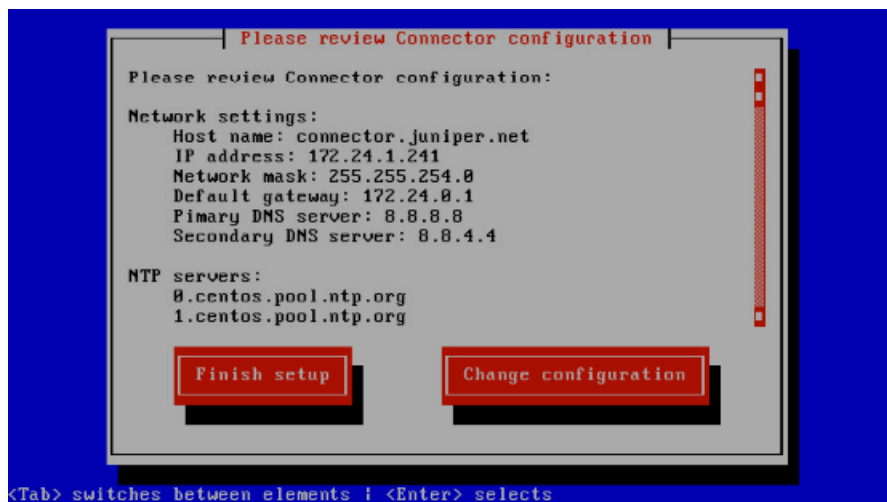


15. Select one of the options and press **Enter**.

Option	Description
Review configuration and finish setup	Lets you review the configuration settings you defined one last time before applying them to the connector virtual appliance.  We recommend that you do not change your configuration settings after the connector is added as a specialized node to the Junos Space fabric.
Change...	Select a setting to update its value.
Troubleshooting menu	Lets you ping the default gateway, remote HA device (if configured), and custom IP address (if configured). Also lets you perform a DNS lookup to verify that your settings are correct.

The Review configuration page appears. See [Figure 15 on page 26](#).

Figure 15: Reviewing Your Configuration Settings



16. 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 connector virtual appliance. A status page indicates the progress.

When done, the Setup Complete page appears. See [Figure 16 on page 27](#).

Figure 16: Completing the Setup Steps



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

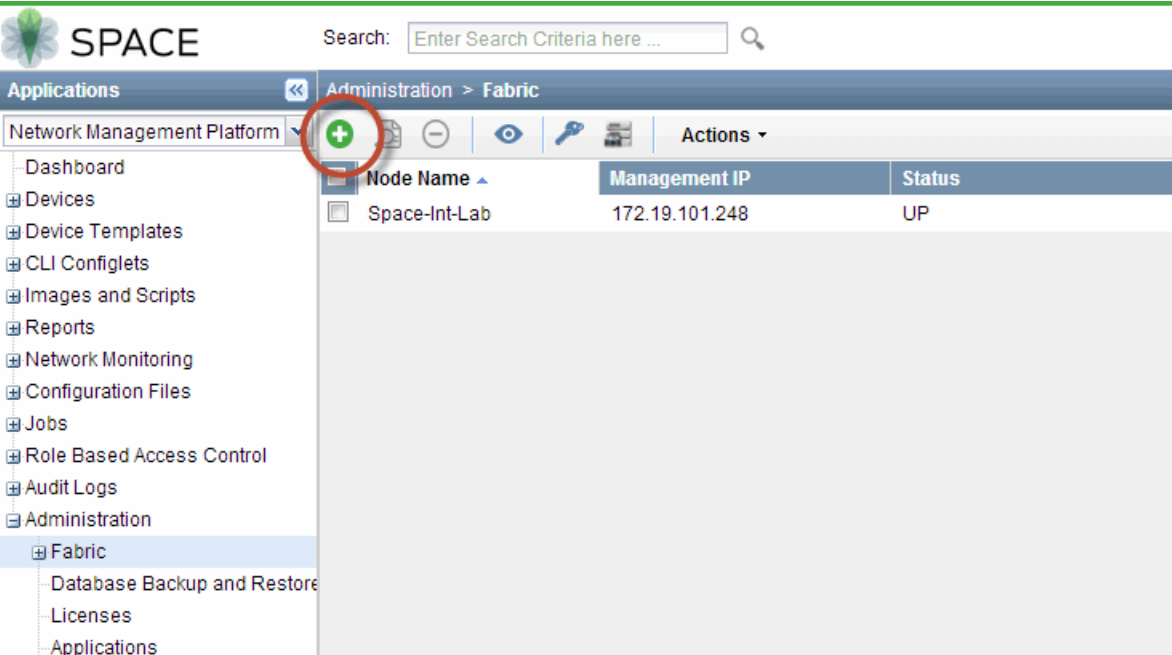
### Adding Spotlight Secure Connector as a Specialized Node in Junos Space

As with other Junos Space appliances, you add Spotlight Secure Connector to the Junos Space Network Management Platform. You can add multiple connector devices to the existing Junos Space fabric, but you can add only one at a time.

To add Spotlight Secure Connector to the Junos Space fabric:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric** and then click the **Add Fabric Node** icon. See [Figure 17 on page 29](#).

Figure 17: Adding a New Fabric



The Add Node to Fabric dialog box appears. See [Figure 18 on page 29](#).

Figure 18: Add Node to Fabric Dialog Box

Add Node to Fabric

Name:   
IP address:

☒ [Add as a specialized node](#)

Provide the credentials for administrative ssh access.  
User:   
Password: 

Warning: After adding/deleting specialized nodes, please log out and log-in again to ensure new functionality is properly installed and SNMP target would be updated on all the devices.

Adding/Deleting specialized nodes involves optimization and readjustment of memory used for various software components. Space servers must be rebooted in order to operate under this new setting.

☒ [Schedule at a later time](#)

Date and time:

Add

Cancel

2. Enter the following information.

Option	Description
Name	Enter a name for the Spotlight Secure Connector device. The name cannot exceed 32 characters and cannot contain spaces.
IP	Enter the IP address of the Spotlight Secure Connector. This is the IP address you assigned to the Spotlight Secure Connector when running the bootstrap script.
User and Password	<p>Enter the login credentials (SSH username and password) of the Spotlight Secure Connector.</p> <p>The credentials must be the same as those you specified when you ran the configuration step.</p> <p>If the credentials do not match, the add node operation (job) fails and Junos Space Network Management Platform displays the following error message on the Job Management workspace: <b>Please check network credentials.</b></p>

3. (Optional) Schedule when you want to add the fabric node:

- Clear the **Schedule at a later time** check box (the default) to initiate the add operation when you complete Step 7 of this procedure.



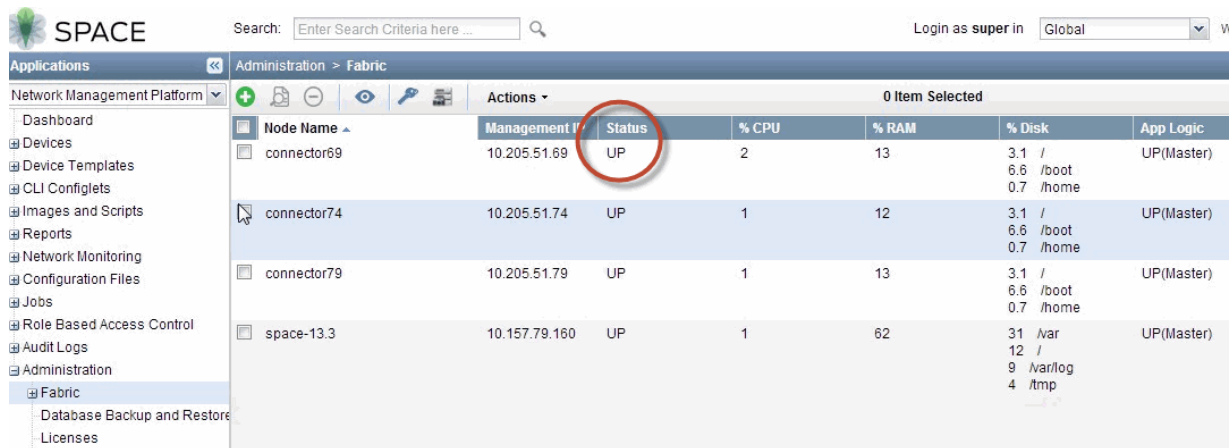
- Select the **Schedule at a later time** check box to specify a later start date and time for the add operation.

**NOTE:** The selected time in the scheduler corresponds to the Junos Space server time but is mapped to the local time zone of the client computer.

4. Click **Add** to add the connector to the fabric.

It might take a few minutes to add Spotlight Secure Connector. When done, the Network Management Platform shows the appliance as having an UP status. See [Figure 19 on page 31](#).

**Figure 19: Spotlight Secure Connector Status in the Network Management Platform**



Node Name	Management IP	Status	% CPU	% RAM	% Disk	App Logic
connector69	10.205.51.69	UP	2	13	3.1 / 6.6 / 0.7	UP(Master)
connector74	10.205.51.74	UP	1	12	3.1 / 6.6 / 0.7	UP(Master)
connector79	10.205.51.79	UP	1	13	3.1 / 6.6 / 0.7	UP(Master)
space-13.3	10.157.79.160	UP	1	62	31 / 12 / 9 / 4	UP(Master)

Similarly, in the Junos Space Security Director Platform user interface select **Security Intelligence > Spotlight Connectors**. The Security Director Platform shows Spotlight Secure Connector as having an UP connection status when it is available. See [Figure 20 on page 32](#).

Figure 20: Spotlight Secure Status in the Security Director Platform



Connector Name	Connection Status	Feed Status	Associated Devices
connector74	UP	OK	0
connector79	UP	OK	0
connector69	UP	OK	0

## RELATED DOCUMENTATION

[Setting Up High Availability | 32](#)

[Associating an SRX Series Device With Spotlight Secure Connector | 36](#)

## Setting Up High Availability

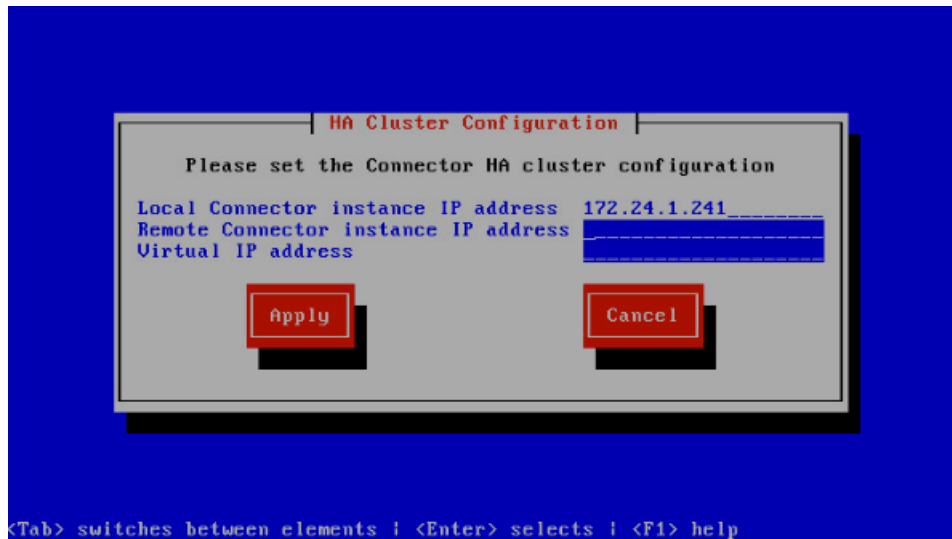
Depending on your requirements, you can configure Spotlight Secure Connector for High Availability (HA) or failover. When the primary node fails, the secondary node automatically takes over without any manual intervention.

To set up HA:

1. During the setup process, define the HA network configuration settings.
2. Add both spotlight connectors as specialized nodes into Junos Space.

During the setup process, you define the primary node (Local Connector instance IP address), the secondary node (Remote Connector instance IP address) and the virtual IP address to send to the SRX Series device. See [Figure 21 on page 33](#).

Figure 21: Defining the HA Network Configuration Settings



When adding a connector as a specialized node to Junos Space, the system reads the network configuration information specified in the setup process. When the secondary node is added to Junos Space, the system recognizes it as the failover node and establishes the relationship with the primary node automatically. See [Figure 22 on page 33](#).

Figure 22: Failover Information Displayed in Security Director

Security Intelligence > Spotlight Secure Connectors							
Spotlight Secure Connectors							
Spotlight Secure Connector is the central connection point between Information Sources and your firewall security devices. You need to have at least one Spotlight Secure Connector configured to leverage these Security Intelligence feeds. You can view the status and manage the configuration of your Spotlight Secure Connectors on this page.							
Name	Management IP	Feed Status	Associated Device	Cluster Status	Virtual IP	Primary	Cluster Members
10.205.51.69	10.205.51.69	OK	2	Yes	10.205.51.80	Yes	10.205.51.69, 10.205.51.79
10.205.51.79	10.205.51.79	OK	2	Yes	10.205.51.80	No	10.205.51.69, 10.205.51.79
10.207.97.201	10.207.97.201	OK	0	No		No	

Because the virtual IP address and not the connector management IP address is sent to the SRX Series device, failover occurs seamlessly.

If you did not configure HA during the setup process and want to configure it after you have already added the connector to Junos Space, follow these steps:

1. On the Junos Space Security Director user interface, select **Security Intelligence > Spotlight Connector**.
2. Select the connector(s) that you want to configure for HA and click **Delete** to remove them as a node.

3. 2. Log in to the connector using SSH (for example, log in to the connector through the VM console) and re-run the setup script.
4. Re-add the connectors as a specialized node in Junos Space.

**NOTE:** If the connectors were already associated with an SRX Series device, you must associate them again. When configured for HA, the SRX Series device talks to the virtual IP and not the individual device's IP address.

#### RELATED DOCUMENTATION

[Configuring Spotlight Secure Connector | 18](#)

[Spotlight Secure Connector General Settings Overview | 34](#)

[Associating an SRX Series Device With Spotlight Secure Connector | 36](#)

## Spotlight Secure Connector General Settings Overview

You can configure general settings for Spotlight Secure Connector. See [Figure 23 on page 35](#). These settings apply to all instances of the connector within Security Director.

**NOTE:** This option is available only if you do not have any spotlight connectors selected. If this option is disabled, deselect all spotlight connectors and try again.

Figure 23: Spotlight Secure Connector General Settings

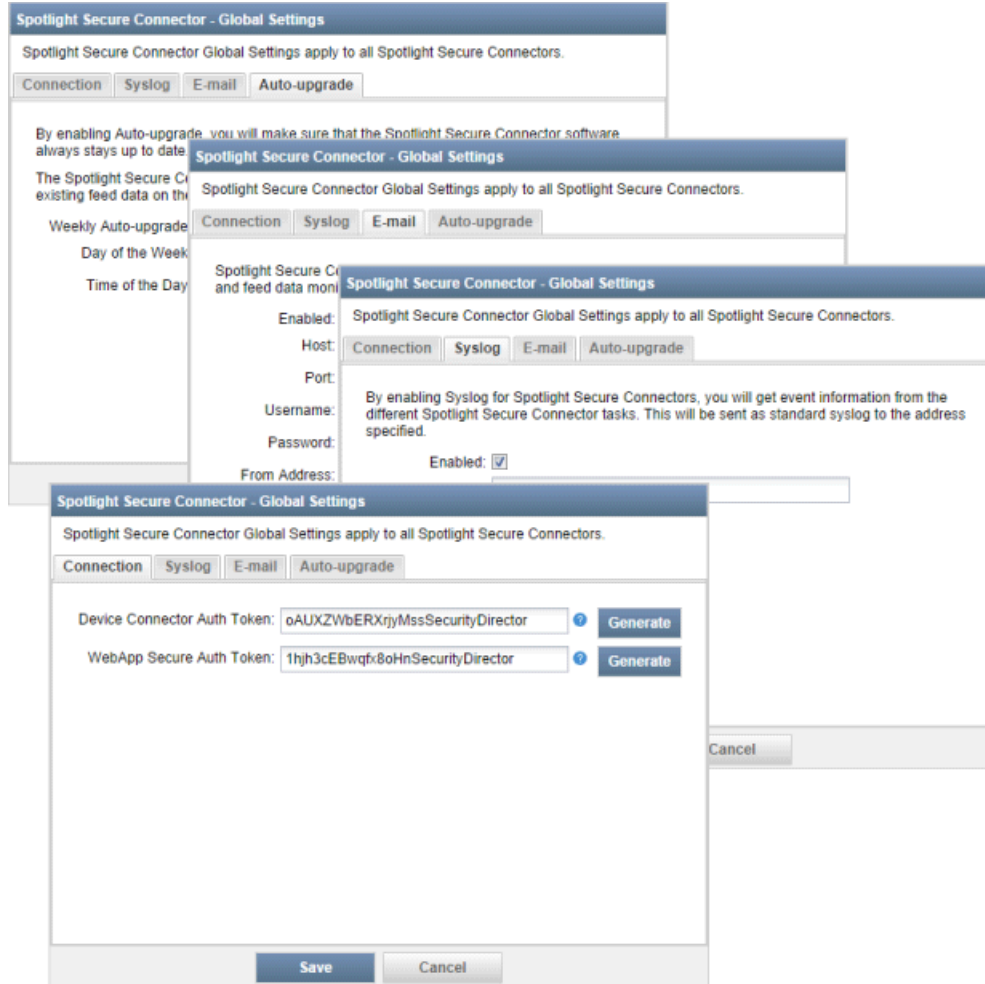


Table 3 on page 35 briefly describes the settings in each tab.

Table 3: Spotlight Secure Connector General Setting Options

Settings Tab	Description
Connection	<p>Defines the tokens used for authentication between Spotlight Secure Connector and other devices, such as WebApp Secure.</p> <p><b>NOTE:</b> Generate these tokens before associating an SRX Series device or WebApp Secure. You must enter the same token when configuring WebApp Secure. The device auth token is pushed to the SRX Series device when associating the SRX Series device.</p>
Syslog	Defines the severity level of log messages to report.
E-mail	Defines e-mail settings for sending error log reports.

Table 3: Spotlight Secure Connector General Setting Options (*continued*)

Settings Tab	Description
Auto-upgrade	Defines when to check for updates to the Spotlight Secure Connector firmware and software packages. Updates are located in the Spotlight Cloud.

#### RELATED DOCUMENTATION

[Configuring Spotlight Secure Connector](#) | 18

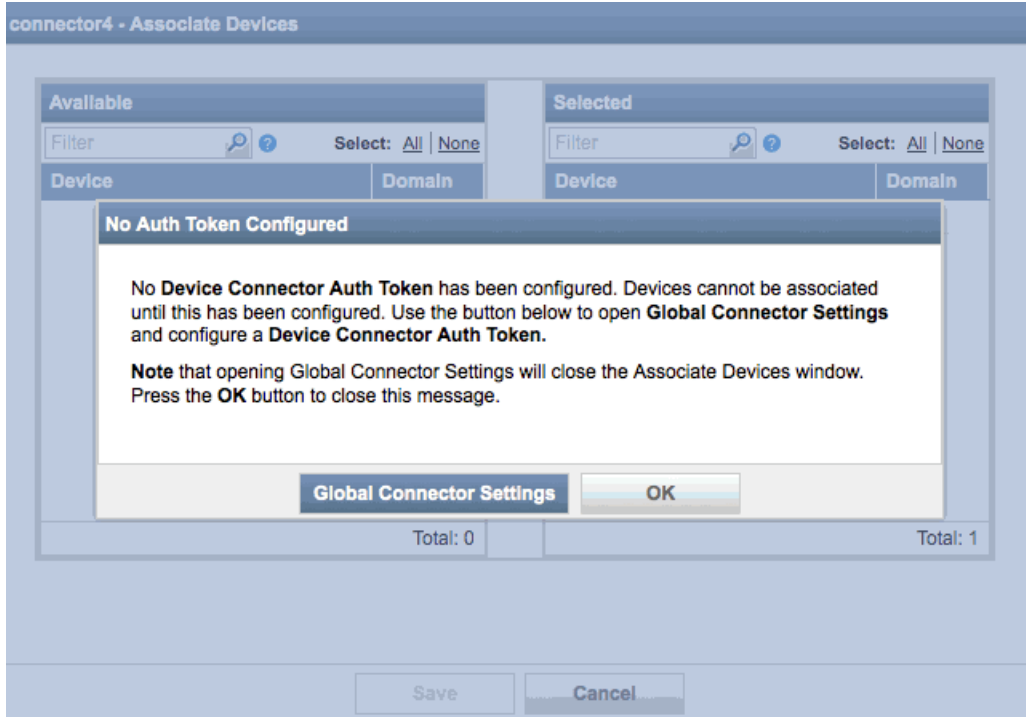
## Associating an SRX Series Device With Spotlight Secure Connector

After the connector is added as a fabric to Junos Space, you can associate an SRX series device to that connector. You can associate multiple SRX devices to each connector.

**NOTE:** Spotlight Secure does not support Logical System (LSYS) devices.

Before associating an SRX Series device, you must first generate the device auth token in the Global Connector Settings page. An alert appears if no auth token is present. See [Figure 24 on page 37](#).

Figure 24: Associating an SRX Series Device Without a Device Auth Token



If your SRX device is already managed by the Security Director, skip to 5. If you have not already associated an SRX Series device with a connector, follow these steps:

1. On the Junos Space Security Director user interface, select **Devices > Device Discovery > Device Targets** and then click the **Add Device** icon (+). See [Figure 25 on page 38](#).

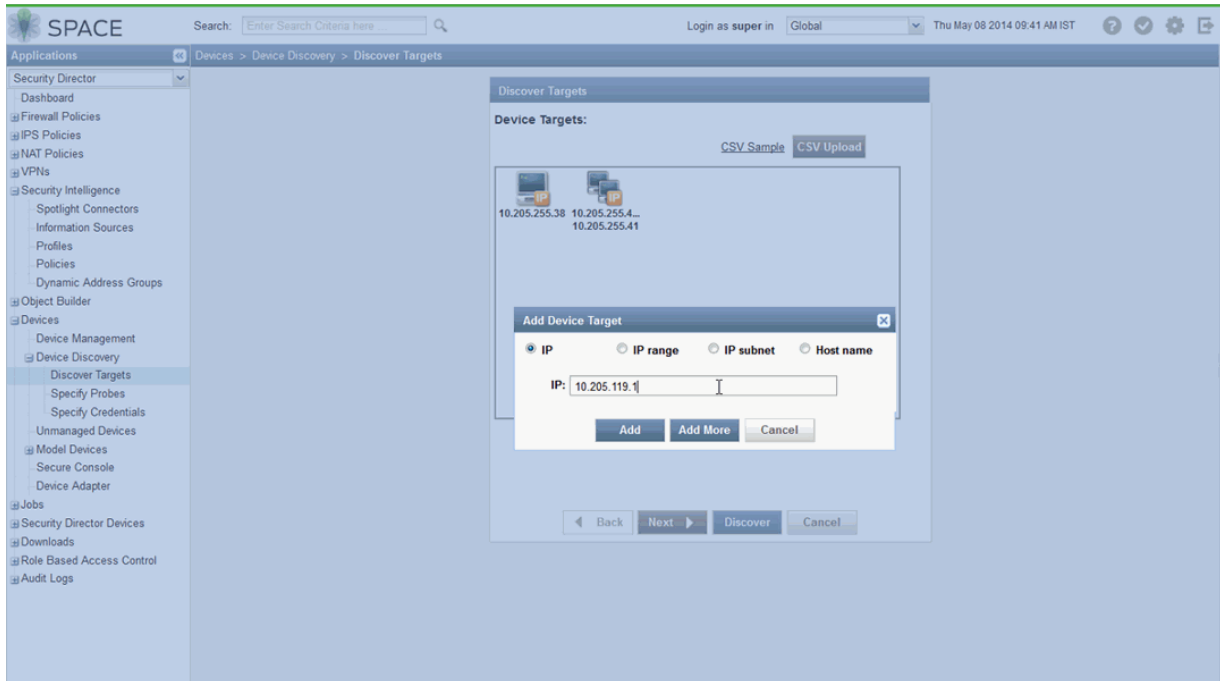
**Figure 25: Adding a New Device Target**



2. Enter the IP address of the SRX Series device that you want to associate with the connector and click **Add**. See [Figure 26 on page 39](#).

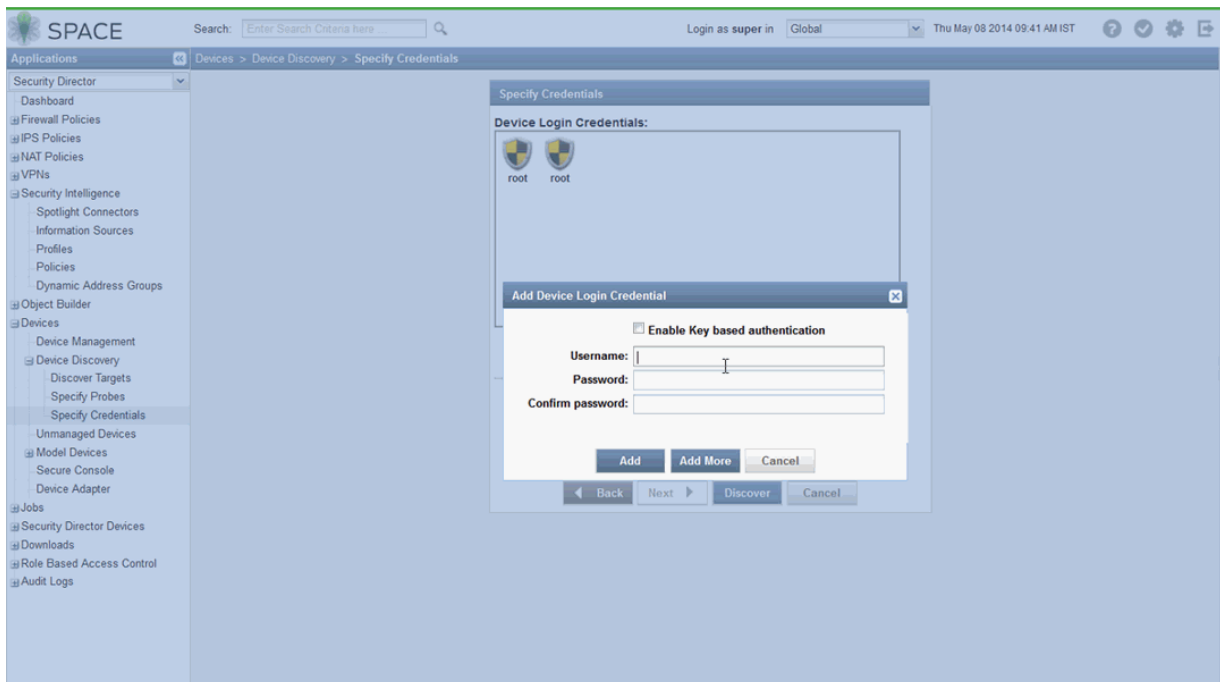


Figure 26: Specifying the SRX Series IP Address



3. Enter the SRX Series device login credentials and click **Add**. See [Figure 27 on page 39](#).

Figure 27: Entering SRX Device Login Credentials



- On the Junos Space Security Director user interface, select **Jobs > Job Management** to view the progress of adding the SRX Series device. When done, a **Discovery succeeded** message appears. See [Figure 28 on page 40](#).

Figure 28: Viewing the Discovery Status

The screenshot shows the 'Jobs > Job Management' interface. A table lists jobs, with job ID 229419 selected. Below the main table, a detailed view for job ID 229419 is shown, including a table of discovered devices. In this table, the 'Status' column for the first device (10.205.119.1) is circled in red, showing 'Discovery succeeded'.

ID	Name	Percent	State	Job Type	Parameters	Summary	Scheduled Start ...	Owner
229419	Discover Network Elements-229419	50.0	Inprogress	Discover Network Elements	IP Address(es): 2 IP Range(s): 10.205.255.40 to 10.205.255.41		May 8, 2014 9:42:00 AM IST	super

Job ID: 229419 Job Type: Discover Network Elements Scheduled Start Time: May 8, 2014 9:42:00 AM IST			
IP Address	Hostname	Status	Description
10.205.119.1		Discovery succeeded	Device discovered successfully
10.205.255.38	secintel-38	Already Managed	Device is already managed
10.205.255.40	clust-40-node0	Already Managed	Device is already managed
10.205.255.41	clust-41-node1	Already Managed	Device is already managed

- On the Junos Space Security Director user interface, select **Security Intelligence > Spotlight Connectors**.
- Right-click the connector you want to associate with SRX Series devices and select **Device Association**. See [Figure 29 on page 41](#).

**NOTE:** If you do not see the SRX Series device, make sure the SRX Series device's release number and schema match that supported by Spotlight Secure. See the *Spotlight Secure Supported Platforms Guide*.

Figure 29: Selecting the Connector to Associate Devices

The screenshot shows the SPACE Security Intelligence console. The left sidebar contains a navigation tree with categories like Applications, Security Director, Alerts, Reports, Firewall Policies, IPS Policies, NAT Policies, VPNs, Security Intelligence, and Object Builder. The main pane displays the 'Spotlight Secure Connectors' page. A table lists three connectors. The connector with IP 10.205.51.79 is selected, and a context menu is open over it, showing the following options:

- Delete Spotlight Secure Connector
- Associate Devices
- Update Spotlight Secure Connector Configuration
- Clear All Selections

Name	Management IP	Feed Status	Associated Devi...	Cluster Status	Virtual IP	Primary	Cluster Members
10.205.51.69	10.205.51.69	Warning	2	Yes	10.205.51.80	No	10.205.51.79, 10.205.51.69
10.205.51.79	10.205.51.79	Warning	2	Yes	10.205.51.80	Yes	10.205.51.79, 10.205.51.69
10.207.97.201	10.207.97.201	Unknown	0	No		No	

7. Select the SRX Series devices to associate with this connector and click **Save**. See [Figure 30 on page 41](#).

Figure 30: Selecting the SRX Series Devices to Associate

The screenshot shows the '10.205.51.79 - Associate Devices' dialog box. The dialog has two panes: 'Available' and 'Selected'. The 'Available' pane lists two devices: 'clust-41-node1' and 'Node-119.2'. The 'Selected' pane lists two devices: 'SRX550-51.45-Srikant' and '10.205.255.38-Secintel'. The 'Save' button is highlighted.

Device	Domain
clust-41-node1	Global
Node-119.2	Global

Device	Domain
SRX550-51.45-Srikant	Global
10.205.255.38-Secintel	Global

**NOTE:** Spotlight Secure requires a specific DMI schema. If you do not see your SRX Series device, make sure the correct DMI schema is installed. See [“Updating the Schema” on page 43](#) and the [Spotlight Secure Supported Platforms Guide](#).

A configuration commit is done on the device after it is associated. On the SRX550 and SRX650 devices, memory allocation is updated and the device is rebooted.

To verify the device association, run the **show configuration** CLI command on the SRX Series device or the **Device Configuration View** in Network Management Platform and look for the following entry:

```
services {
  security-intelligence {
    url https://10.189.240/api/v1/manifest.xml;
    authentication{
      auth-token 7qgxe0VnlQxVphbdFMkEItgL5MpmqTN1;
    }
  }
}
```

The URL and auth-token entries will be unique to your configuration.

## RELATED DOCUMENTATION

[Configuring Spotlight Secure Connector | 18](#)

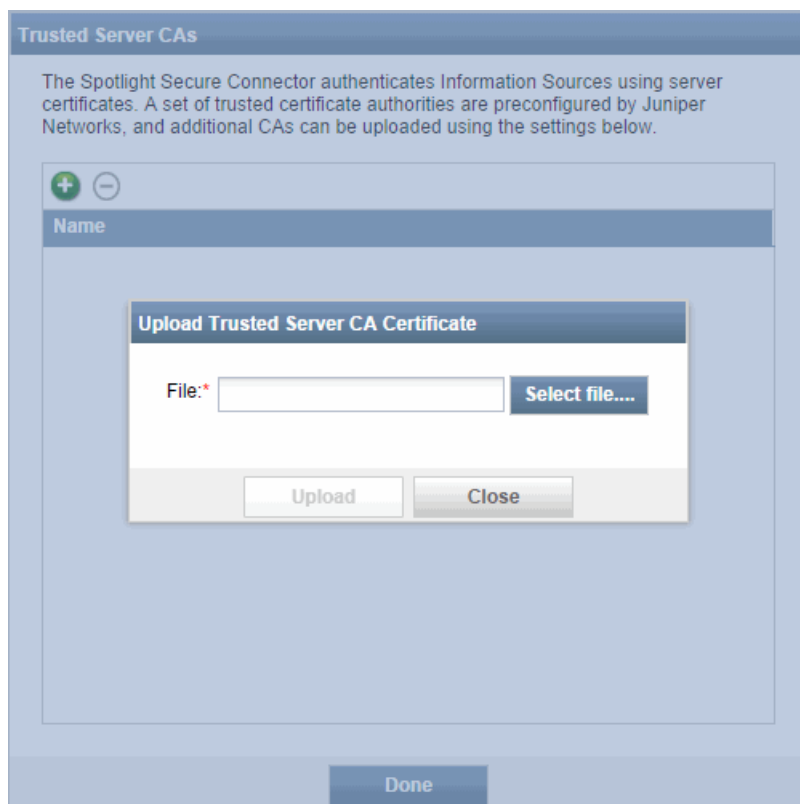
[Setting Up High Availability | 32](#)

[Updating the Schema | 43](#)

## About Trusted Server CAs

Spotlight Secure Connector uses server certificate authorities (CAs) when communicating with any https server, such as those hosting information sources. A set of trusted CAs are pre-installed but you can install additional certificates. See [Figure 31 on page 43](#).

Figure 31: Uploading Additional Trusted Server CA Certificates.



## RELATED DOCUMENTATION

| [Spotlight Secure Connector Information Source Overview](#) | 54

## Updating the Schema

Security Intelligence requires specific versions of the DMI schema. See the [Spotlight Secure Supported Platforms Guide](#) for detailed information. Depending on your current installed versions, you may be required to update your DMI schema. This topic presents an overview of the steps. It assumes you have already downloaded the schema file to your local system. See [Updating a DMI Schema](#) for complete instructions.

To update a DMI schema:

1. From the Junos Space Network Management Platform, select **Administration > DMI Schemas** and click the **Update Schema** icon.
2. Check the **Archive (tgz) option** radio button.

3. Click **Browse**, select the .tgz file and click **Open**.
4. Click **Upload**.
5. Select the desired schema and click **Install**.

The DMI Schemas inventory landing page displays the newly installed schema.

## RELATED DOCUMENTATION

| [Associating an SRX Series Device With Spotlight Secure Connector](#) | 36

## Managing Spotlight Secure Connectors

### IN THIS SECTION

- [Adding Spotlight Secure Connector Global Settings](#) | 45
- [Uploading Trusted Server CAs](#) | 46
- [Associating Devices to Spotlight Secure Connectors](#) | 47
- [Updating Spotlight Secure Connector Configuration](#) | 49
- [Deleting Spotlight Secure Connectors](#) | 50
- [Viewing Spotlight Secure Connector Feed Status](#) | 50
- [Upgrading Spotlight Secure Connector Software or Package](#) | 51

To open the Spotlight Secure Connectors page:

- Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connector.

- Right-click the spotlight secure connector to manage it, or select the required options from Actions.

You can perform the following management tasks on the Spotlight Secure Connectors page:

## Adding Spotlight Secure Connector Global Settings

To add spotlight secure connector global settings:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Click the Spotlight Secure Connector - Global Settings icon in the toolbar.

The Spotlight Secure Connector - Global Settings page appears, as shown in [Figure 32 on page 45](#).

**Figure 32: Global Connector Settings**

Spotlight Secure Connector - Global Settings

Spotlight Secure Connector Global Settings apply to all Spotlight Secure Connectors.

Connection Syslog E-mail Auto-upgrade

Device Connector Auth Token: JqrYXLVbW31VZv0yuoTkt9Up6vM3Ta6 ? Generate

WebApp Secure Auth Token: hXU5SbWMusL0d6rN2puqSyqaQfzAmxst ? Generate

Save Cancel

3. Under the Connection tab, configure the following parameters:

- To generate a 32-character token for the Device Connector Auth Token field, click **Generate**.
- To generate a 32-character token for the WebApp Secure Auth Token field, click **Generate**.

You can edit the auto-generated token; however, make sure that it still contains 32 characters.

4. Under the Syslog tab, configure the following parameters:

- Select the **Enabled** check box to enable the syslog collection.
- In the Address field, provide the address to use to collect the syslog data.
- In the Log Verbosity drop-down list, select the required option. The available options are:

- Error
  - Warning
  - Info
  - Debug
5. Under the E-mail tab, configure the following parameters:
    - Select the **Enabled** check box to enable the E-mail functionality.
    - In the Host field, enter the hostname.
    - In the Port field, select the required port number.
    - In the Username field, enter the username.
    - In the Password field, enter the password information.
    - In the From Address field, enter the From address.
    - in the To Address field, enter the To address.
    - Select the **Use TLS** check box.
  6. Under the Auto-upgrade tab, you can configure the following parameters:
    - To automatically upgrade the spotlight secure connector once a week, select the **Weekly Auto-upgrade** check box.
    - From the Day of the Week drop-down list, select the required day to perform the automatic upgrade.
    - From the Time of the Day drop-down list, select the time.
  7. Click **Save** to save the spotlight secure connector settings.

## Uploading Trusted Server CAs

To upload the trusted server CA certificates:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Click the Trusted Server CAs icon.

The Trusted Server CAs page appears, listing the already uploaded certificates.

3. To upload the new certificate, click the plus sign (+).

The Upload Trusted Server CA Certificate pop-up window appears.



4. To select the certificate file to upload, click **Select file**.
5. To upload the certificate files, click **Upload**.

## Associating Devices to Spotlight Secure Connectors

To associate a device with a spotlight secure connector:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

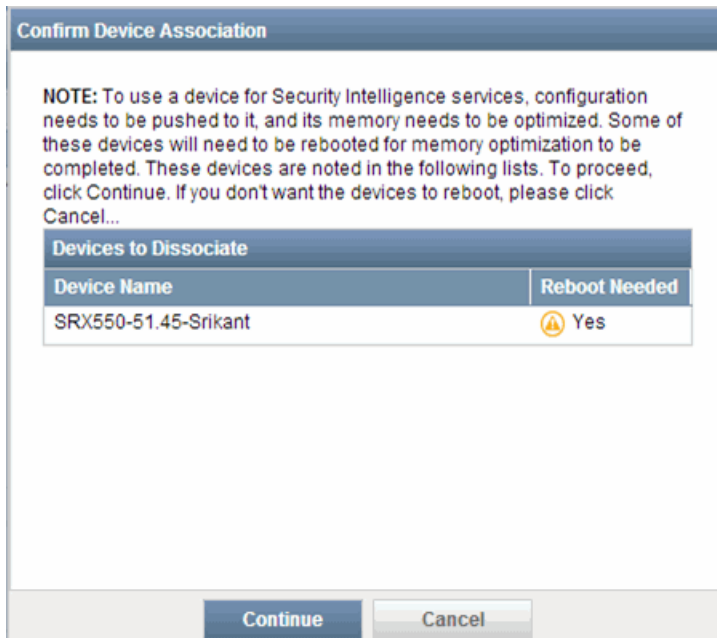
2. Right-click the spotlight secure connector, or, from the Actions, select **Associate Devices**.

The Device Association page appears.

3. Select the required devices from the Available column, and move them to the Selected column.

If you assign a SRX550 or SRX650 device, the following message about the memory optimization is shown, as shown in [Figure 33 on page 47](#).

**Figure 33: Confirm Device Association**



4. To associate the selected devices with the spotlight secure connector, click **Save**.

When a device is associated with a spotlight secure connector or disassociated from a spotlight secure connector, a job is created in Security Director to push the spotlight secure connector configuration information to the device.


You can view the associated devices on the Spotlight Secure Connectors landing page. Click the Associated Devices column for the respective spotlight secure connector, and all the devices are listed, as shown in [Figure 34 on page 48](#).

**Figure 34: Connector-Device List**

Connector-SD-QA - Device List				
The following devices are configured to retrieve Security Intelligence from Connector-SD-QA.				
<input type="checkbox"/>	Security Device Name	Connection Status	Feed Update Status	Last Connection Time
<input checked="" type="checkbox"/>	Node-119.2	Down	Failure	Sep 11, 2014 05:46:49 AM UTC
<input type="checkbox"/>	10.205.255.38-Secintel	Up	OK	Sep 11, 2014 09:38:15 AM UTC
<input type="checkbox"/>	clust-41-node1	Up	OK	Sep 11, 2014 09:38:12 AM UTC
<input type="button" value="Update Feed"/>				
<input type="button" value="Done"/>				

You can view the feed update status of the security device. Select the required device and click the Feed Update Status. A window appears showing the feed status of the device, as shown in [Figure 35 on page 49](#).

Figure 35: Security Device Feed Status

10.205.255.38 - Secintel - Feed Status				
Feed Name	Category	Status	Detailed Status	Last update time
TEST	BLACKLIST	✓ OK	Store succeeded	2014-09-10 10:31:34.0
WL1	BLACKLIST	✓ OK	Store succeeded	2014-09-10 10:31:34.0
BL2	WHITELIST	✓ OK	Store succeeded	2014-09-10 10:31:34.0
JWAS1.cookie	JWAS	✓ OK	Store succeeded	2014-09-10 10:41:31.0
JWAS1.ip_addr	JWAS	✓ OK	Store succeeded	2014-09-10 10:41:31.0
 Refresh Status				
Done				

You can update the feed to any listed device. Select the required Security Device, and click Update Feed option provided in the bottom of the Device List page, as shown in [Figure 34 on page 48](#).

A job window appears showing the status of the feed update. Click **View** under the Message column to view the update feed message.

## Updating Spotlight Secure Connector Configuration

If the configuration of a spotlight secure connector is out of sync from Security Director, administrator can choose to push or update the latest configuration to a spotlight secure connector.

To update the configuration:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Right-click the spotlight secure connector, or, from the Actions, select **Update Spotlight Secure Connector Configuration**.

A confirmation message appears confirm the update.

3. Click **Continue**.

The Job Details page appears, showing the spotlight secure connector update details.

4. In the Message column, click **View** to view the spotlight secure connector configuration.

When Device connector auth-token changes, both Update connector and Update connector settings to device jobs begin. The later job updates the auth-token information alone in the device.

## Deleting Spotlight Secure Connectors

To delete a spotlight secure connector:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Right-click the spotlight secure connector and select **Delete Spotlight Secure Connector**, or click the minus sign (-).
3. You cannot directly delete a spotlight secure connector from the Security Intelligence workspace. A pop-up window appears to enable you to delete the spotlight secure connector.
4. Go to Network Management Platform > Administration > Fabric.  
Select the required node, and click the minus sign (-).
5. The required spotlight secure connector is deleted.

## Viewing Spotlight Secure Connector Feed Status

To view the feed status of a spotlight secure connector:

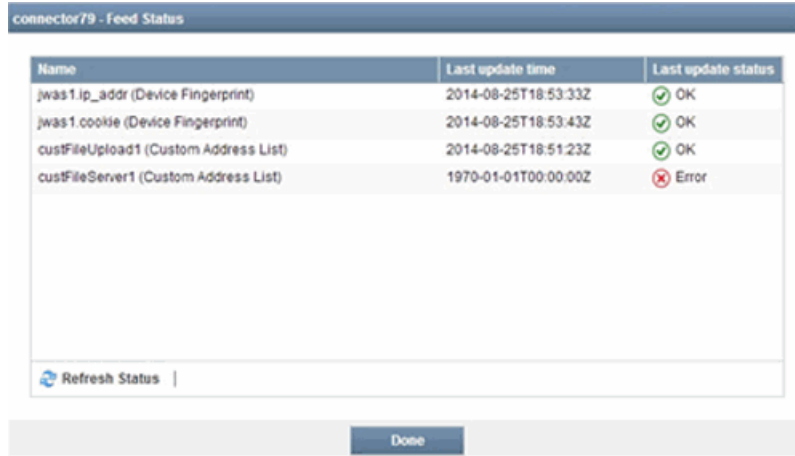
1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Click the **Feed Status** column for the required spotlight secure connector.

A Feed Status page appears showing the feed name, last updated time, and the last updated status, as shown in [Figure 36 on page 51](#).

Figure 36: Spotlight Secure Connector Feed Status



The screenshot shows a window titled "connector79 - Feed Status". Inside, there is a table with three columns: "Name", "Last update time", and "Last update status". The table contains four rows of data. Below the table, there is a "Refresh Status" button with a circular arrow icon. At the bottom of the window, there is a "Done" button.

Name	Last update time	Last update status
jwas1.ip_addr (Device Fingerprint)	2014-08-25T18:53:33Z	OK
jwas1.cookie (Device Fingerprint)	2014-08-25T18:53:43Z	OK
custFileUpload1 (Custom Address List)	2014-08-25T18:51:23Z	OK
custFileServer1 (Custom Address List)	1970-01-01T00:00:00Z	Error

3. To close the window, click **Done**.

## Upgrading Spotlight Secure Connector Software or Package

To upgrade the new spotlight secure connector software package:

1. Enable the auto upgrade option for the spotlight secure connector. Ensure the spotlight secure connector has connectivity to the spotlight secure connector software repository.
2. If a spotlight secure connector does not have the latest software version and the spotlight secure connector has connectivity to the spotlight secure connector software package, administrator can upgrade the spotlight secure connector from the update link of the spotlight secure connector listing page.
3. If Step 1 and Step 2 options are not available, administrator can upload the software image and apply to spotlight secure connectors for upgrade. In the first release, administrator must SCP the upgrade package to spotlight secure connector VMs and invoke the upgrade process by executing a set of specific commands. You require an active internet connection because the command downloads the latest spotlight secure connector release from the Juniper Networks cloud package server.

## RELATED DOCUMENTATION

| *Creating a Spotlight Secure Connector*

## Creating a Backup or Restoring the Connector Settings

You can create a backup of the connector configuration and restore the connector settings. To create a backup:

1. Select **Security Intelligence > Backup/Restore**.

The Backup/Restore page appears, listing the current versions.

2. To create a backup of the connector configuration, click the plus sign (+).

The Backup Connector Setting page appears.

3. In the Description field, enter a description of the new version.

4. Click **Backup**.

5. The Snapshot Policy page appears, showing the status of the backup. Click **Close**.

A new version is created and listed on the Backup/Restore page.

To restore the connector configuration:

1. On the Backup/Restore page, select a version and right-click, or, from Actions, select **Restore**.

The Connector Settings - Restore Summary page appears. This page shows a summary of the connector settings before you restore the configuration.

2. Click **Restore**.

The selected version is rolled back to the previous version, and the Rollback Policy page lists a summary of the rollback.

3. To view the summary of the rolled-back version, click **Summary Report**.

You can also delete the versions.

### RELATED DOCUMENTATION

| [Security Intelligence Overview](#)

# 3

PART

## Configuring Spotlight Secure Connector in Security Director

---

Configuring the Information Sources | 54

Configuring Profiles and Policies | 71

Applying Spotlight Secure to Security Rules | 87

---

# Configuring the Information Sources

## IN THIS CHAPTER

- [Spotlight Secure Connector Information Source Overview | 54](#)
- [Information Source Update Interval | 65](#)
- [Creating an Information Source | 66](#)
- [Managing Information Sources | 68](#)

## Spotlight Secure Connector Information Source Overview

## IN THIS SECTION

- [Allowlist and Blocklists | 55](#)
- [Geolocation IP Address | 57](#)
- [Command and Control Lists | 59](#)
- [WebApp Secure Threats | 61](#)
- [About Custom Address Lists | 64](#)
- [Feed Status | 64](#)

The first step in configuring the connector is to set up your data feeds or information sources. Spotlight Secure Connector supports three information sources:

- Custom files
- Spotlight Cloud
- WebApp Secure



The following data categories can be obtained from one or more of the information sources.

Information Source	Data Feed
Custom files	Allowlist and blocklists
Spotlight Cloud	GeoIP, C&C
WebApp Secure	WebApp Secure threats

## Allowlist and Blocklists

Generally speaking, a allowlist is simply a list of known IP addresses that you trust and a blocklist is a list that you don't trust. See [Example Blocklist on page 55](#). Depending on your requirements, you can set up the connector to either allow what's on the allowlist and prevent everything else, or prevent what's on the blocklist and allow everything else. You can create your own list or obtain a list from a third-party vendor.

### Example Blocklist

```
239.102.121.28
10.39.38.38-10.39.134.41
140.156.140.116
10.101.88.97-10.101.153.218
48.36.103.130/28
39.187.114.224/14
6.30.10.43/2
233.194.172.81
99.139.153.226
10.169.130.35-10.169.178.129
10.83.5.148-10.83.28.167
10.183.194.58-10.183.210.220
96.15.111.63
10.23.57.20-10.23.97.40
156.79.137.86
99.188.94.107/32
55.96.230.38
```

These lists can be stored locally on a system or posted on a webserver. See [Figure 37 on page 56](#). Spotlight Secure Connector periodically polls the webserver and dynamically updates the security device with the addresses. Or, the list can be assigned to a dynamic address group and used for source or destination match in the security policy.

Allowlist and blocklists must be an ASCII text file with each entry on a separate line. See [Example Blocklist on page 55](#).

Figure 37: Using the Custom File Source for Allowlist and Blocklists

The image displays two overlapping 'Add Information Source' dialog boxes. The background dialog is for a 'Custom File Upload' source, with fields for 'Source' (set to 'Custom File Upload'), 'Name' (set to 'My Blacklist'), 'Description' (empty), and 'File' (set to 'demo-blacklist.txt'). It has a 'Create' button at the bottom. The foreground dialog is for a 'Custom File Server' source, with fields for 'Source' (set to 'Custom File Server'), 'Name' (set to 'My Blacklist'), 'Description' (empty), 'Address' (set to 'http://my.juniper.net'), 'Username' (set to 'admin'), 'Password' (masked with '\*\*\*\*'), 'Update Interval' (set to 'Weekly'), and buttons for 'Create' and 'Cancel' at the bottom.

With this release, Spotlight Secure Connector supports only IP record format.

The IP record format can be any of the following:

- IP Address—Supports only IPv4 address with this release; for example, 172.16.254.1.
- IP Range—IP addresses can also be shown as a range; for example, 172.16.0.0 – 172.31.255.255 or 122.140.201-205.\*
- CIDR—Classless Interdomain Routing (CIDR) notation specifies an IP address and its associated routing prefix; for example, 192.168.0.1.0/24.

Once created, you can add your list to the Global Allowlist or Global Blocklist profile. See [Figure 38 on page 57](#). You can also these lists in dynamic address groups.

Figure 38: Creating a Global Blocklist Profile

**Modify Security Intelligence Profile - Global Black List**

Name: Global Black List

Description: This global profile applies to all Security Intelligence Policies and can be used as a black list, permitting traffic and taking priority over the actions of other profiles

Feed Category: CustomAddressList

Actions: REJECT

Custom Address Lists:

**Available Address Lists**
Filter    Select: [Page](#) | [None](#)

**Black Lists**
Filter    Select: [Page](#) | [None](#)

My Blacklist

Total: 1

**Modify** **Cancel**

## Geolocation IP Address

Geolocation software uses the IP address to determine a person's geographic location by identifying what country or organization is assigned to that IP address. This technology is widely used by several industries, such as banking, travel, health care, and so forth for preventing fraud, serving targeted marketing content and other functions.

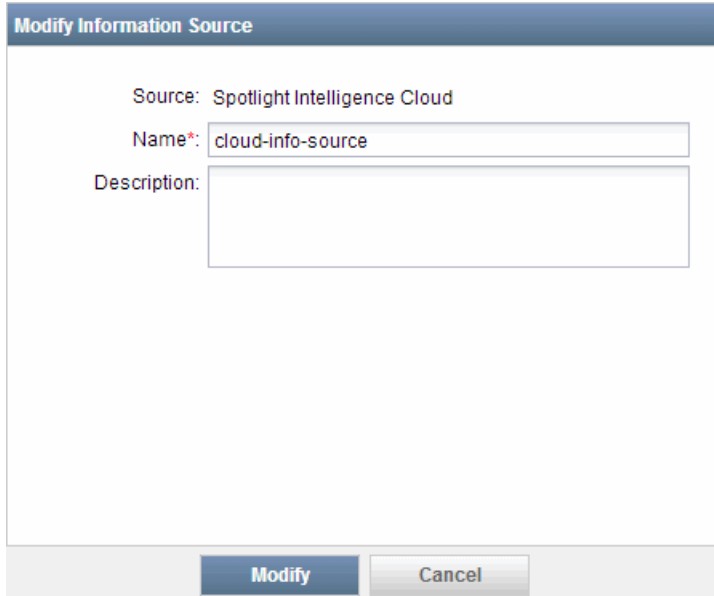
With Security Intelligence, you can use geolocation IP (GeoIP) address to allow or deny traffic to or from a particular geographic region. GeoIP feeds are created with dynamic address groups or from the Spotlight Cloud. You can create a list of allowed countries or a list of countries to exclude with dynamic address groups. See [Figure 39 on page 58](#).

Figure 39: Creating a GeolIP Dynamic Address Group

The image shows two overlapping 'Create Dynamic Address' dialog boxes. The background dialog has fields for Name (My Dynamic Address Group), Description, Feed (GeolIP), and Countries (Pick one or more countries...). The foreground dialog is identical but has a red circle around the 'Negate Selected Countries' checkbox, which is currently unchecked. A dropdown menu is open for the 'Countries' field in the foreground dialog, showing a list of countries including Afghanistan, Åland Islands, Albania, Algeria, American Samoa, Andorra, Angola, Anguilla, Antarctica, Antigua and Barbuda, Argentina, Armenia, Aruba, and Australia.

You can create only one Spotlight Cloud information source. Once created, all available Spotlight Cloud feeds are automatically downloaded to the connector for use. See [Figure 40 on page 59](#).

Figure 40: Example of the Spotlight Cloud Information Source



Modify Information Source

Source: Spotlight Intelligence Cloud

Name\*: cloud-info-source

Description:

Modify Cancel

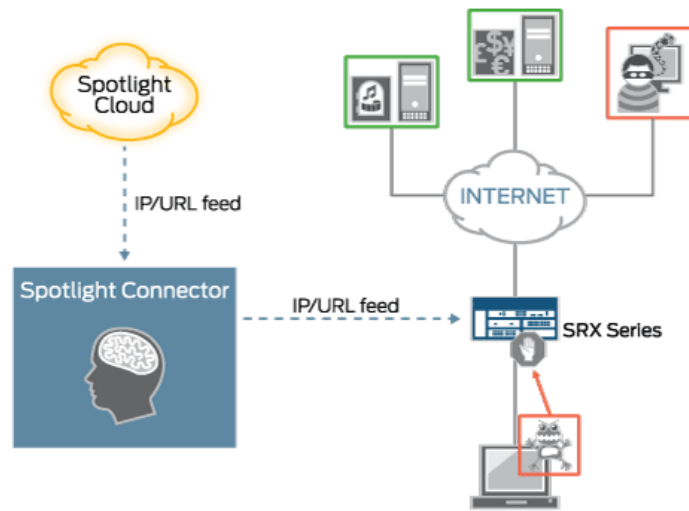
Unlike static address groups where you specify the host's network address, dynamic address groups let you define fields or tags as identifiers. With dynamic address groups you can add or remove hosts in the list without having to reconfigure the security device.

## Command and Control Lists

A bot, also called a web robot, is a program that runs automated tasks over the Internet. After a computer is taken over by a bot, it can steal personal information, send spam e-mail, launch distributed denial of service (DDOS) attacks, and perform other malicious actions. Bots are usually part of a collection of infected computers, ranging from a few computers to several thousand, called botnets. Botnets are controlled by a central system called the Command and Control (C&C) server.

With Security Intelligence, the SRX Series device can mitigate traffic when an infected device attempts to contact a known C&C server by comparing IP addresses and URLs feeds. See [Figure 41 on page 60](#).

Figure 41: Security Intelligence and Infected Host Detection



8042324

You can download C&C feeds only from the Spotlight Cloud. You cannot create your own C&C feed, but you can create custom blocklists to block specific IP addresses or URLs. Once you create a Spotlight Cloud information source, all Spotlight Cloud feeds are automatically downloaded to the connector for use. See [Figure 42 on page 60](#).

Figure 42: Specifying the C&amp;C Source in Security Director

The screenshot shows a dialog box titled 'Modify Information Source'. It contains the following fields:

- Source:** Spotlight Intelligence Cloud
- Name\*:** cloud-info-source
- Description:** (An empty text area)

At the bottom of the dialog box are two buttons: 'Modify' and 'Cancel'.

Then you can create a profile and policy to mitigate C&C threats. See [Figure 43 on page 61](#). You can also use C&C lists in dynamic address groups.

Figure 43: Creating a C&amp;C Profile in Security Director

**Create Security Intelligence Profile**

Name\*:

Description:

Feed Category:

? Blocking Threshold:

*Custom allows you to block traffic based on the Threat Score*

**Most aggressive**

**Least aggressive**

**Default Security**

- Provides the best balance between increased security and reduced [false positives](#).
- Block malicious or suspicious traffic with a [threat score](#) of 6 or higher.

**Security**

Less More

**False Positive**

Less More

? Block Options: *For all the blocked traffic, take the following action:*

☒ Drop connection silently (recommended)

☐ Close connection

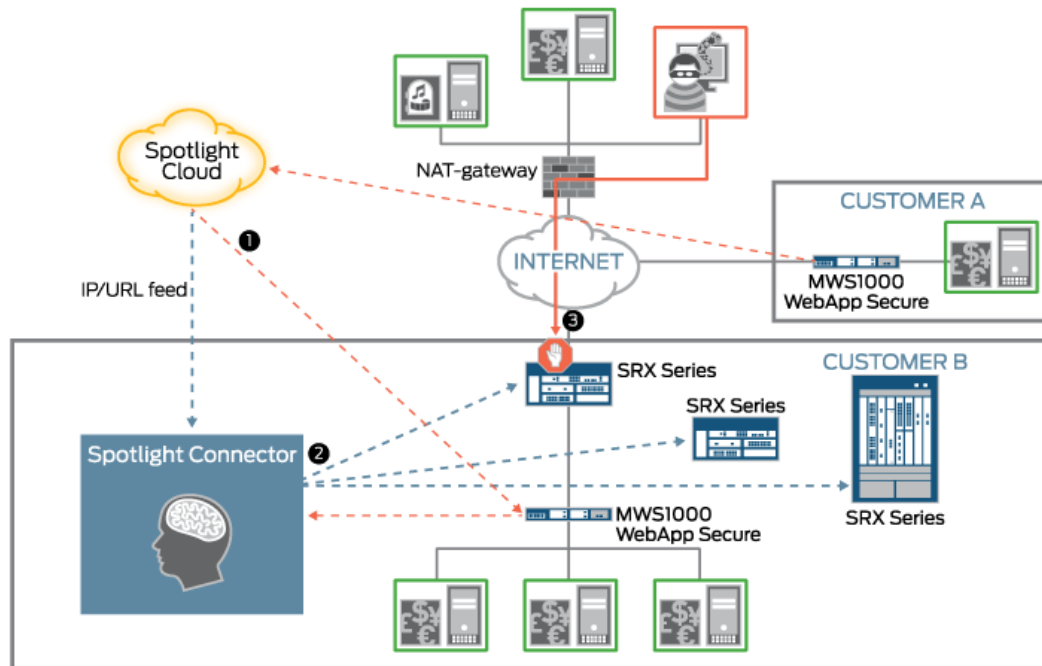
*For all closed HTTP traffic, take the following action:*

☒ No Message

## WebApp Secure Threats

Once an attacker is identified and fingerprinted on a subscriber's network using WebApp Secure, the attacker profile is shared with other subscribers, providing a real-time security solution. This approach provides better accuracy when compared with IP-based reputation feeds. See [Figure 44 on page 62](#).

Figure 44: Example WebApp Secure Deployment



- ❶ Customer B WebApp Secure appliance gets the attacker fingerprint from Spotlight Cloud.
- ❷ Customer B WebApp Secure shares attacker fingerprint with Spotlight Connector that dynamically feeds it into all selected SRX devices.
- ❸ The SRX blocks the attacker based on the device fingerprint and allows all other valid clients, even if they have the same IP as the attacker.

8042325

Figure 45 on page 63 shows the dialog box for adding a WebApp Secure information source. Note that you must also configure the WebApp Secure device with the same information.



Figure 45: Creating a WebApp Secure Information Source

**Add Information Source**

Source:  ?

Spotlight Connector Group Name:

Description:

Adding a Juniper WebApp Secure feed requires the same settings provided above to be configured on each WebApp Secure Appliance that will be part of the group. The following additional information will also be needed:

Connector URL: `https://[Connector Hostname or IP Address]/api/jwas/manifest.json`

WebApp Secure Auth Token: `RfMzYnpgNzaXH4pWbV54G1Vkt5wfitoM` ?

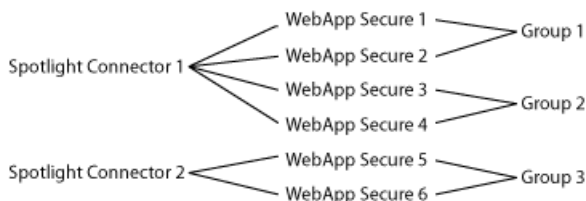
To configure, do the following:

1. Log into the Juniper WebApp Secure Appliance.
2. Navigate to **Security Intelligence** under **Spotlight Secure** in the main menu.
3. Select the **Configure** button in the top right corner.
4. Set **Service Enabled** to **True**.
5. Enter the **Connector URL** and **Group Name** as described above.
6. Copy the **WebApp Secure Auth Token** shown above into the **Auth Token** field.
7. Select the **Test Connection Settings** link to verify the connection was made properly.

You may add multiple WebApp Secure Appliances to the same group.

The group name lets you push feeds to multiple WebApp Secure devices (all devices with the same group name receive the same feed.) In the example in [Figure 46 on page 63](#), connector 1 pushes feeds to WebApp Secure 1 through 4. WebApp Secure 1 and WebApp Secure 2 receive the same feeds because they share the same group name. WebApp Secure 3 and WebApp Secure 4 receive the same feeds because they share the same group name, but receive different feeds than WebApp Secure 1 and WebApp Secure 2 because they are in different groups.

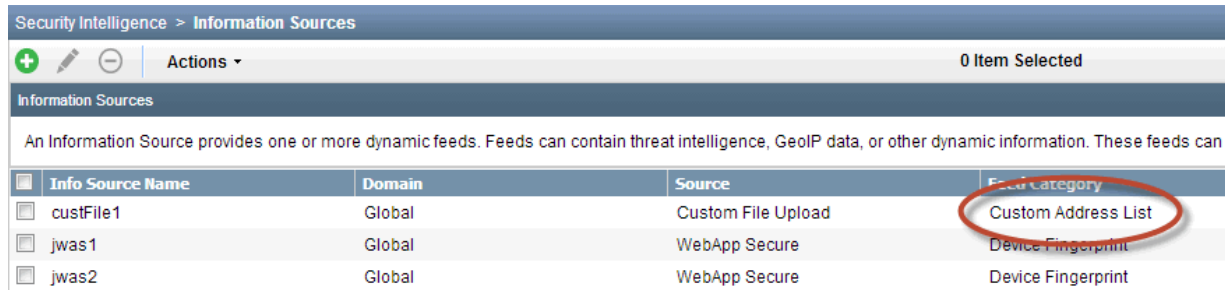
Figure 46: Group Names Receive the Same Feeds



## About Custom Address Lists

When you import a list, either from your local system or from a server, it is categorized as a Custom Address List feed. See [Figure 47 on page 64](#). At this point, Security Intelligence does not know whether this is a allowlist, a blocklist or to be used as a dynamic address group.

Figure 47: Custom Address List Feed Category



Security Intelligence > Information Sources			
Actions ▾			0 Item Selected
Information Sources			
An Information Source provides one or more dynamic feeds. Feeds can contain threat intelligence, GeolP data, or other dynamic information. These feeds can			
Info Source Name	Domain	Source	Feed Category
custFile1	Global	Custom File Upload	Custom Address List
jwas1	Global	WebApp Secure	Device Fingerprint
jwas2	Global	WebApp Secure	Device Fingerprint

If you configure a custom address feed as a blocklist or a allowlist, it becomes a Security Intelligence policy. If you configure it as a dynamic address group, it becomes a firewall policy. This allows flexibility for creating rules. For example, suppose you have a GeolP dynamic address group set up as a firewall policy to block a region. However, there are certain IP addresses within that region that you want to allow. You can create a allowlist and add it as a Security Intelligence policy to that firewall rule to allow those specific IP addresses.


Note that Spotlight Secure policies have priority over firewall policies and the source priorities (in decreasing order) are as follows:

- allowlist
- blocklist
- C&C
- GeolP

## Feed Status

The feed status page indicates the feed's current state on the SRX Series device. The Detailed Status column shows the feed status. Values are **pending**, **storing**, and **store succeeded**. If the status is **store succeeded**, then the feed is active on the SRX Series device and the Last Update Time column shows when the feed was successfully downloaded to the SRX Series device.

Figure 48: Feed Status Information

guavabert - Feed Status				
Feed Name	Category	Status	Detailed Status	Last Update Time
BlacklistFeed1	BLACKLIST	✓ OK	Store succeeded	2014-09-23 10:52:07.0
cc_ip_data	CC	✓ OK	Store succeeded	2014-09-23 10:12:39.0
cc_url_data	CC	✓ OK	Store succeeded	2014-09-23 10:12:44.0
WhitelistFeed1	WHITELIST	✓ OK	Store succeeded	2014-09-23 10:52:37.0
geoip_country	GEOIP	✓ OK	Store succeeded	2014-09-19 11:52:49.0
IPfilterFeed1	IPFILTER	✓ OK	Store succeeded	2014-09-23 10:52:25.0
 Refresh Status				
Done				

## Information Source Update Interval

Spotlight Secure Connector is not a push-enabled application. Instead, it relies on its clients, like the SRX Series device, to query the connector for updates to information sources. See [Table 4 on page 65](#).

Table 4: SRX Series Device Update Interval Time for Information Sources

Information Source	Update Interval
Command and Control	30 minutes
GeoIP	7 days
Custom file	15 minutes

When using the Custom File Server to add an information source, you can specify the interval for polling the server. Custom file information sources are pushed to the connector immediately after being uploaded to Security Director.

## RELATED DOCUMENTATION

## Creating an Information Source

To create an information source:

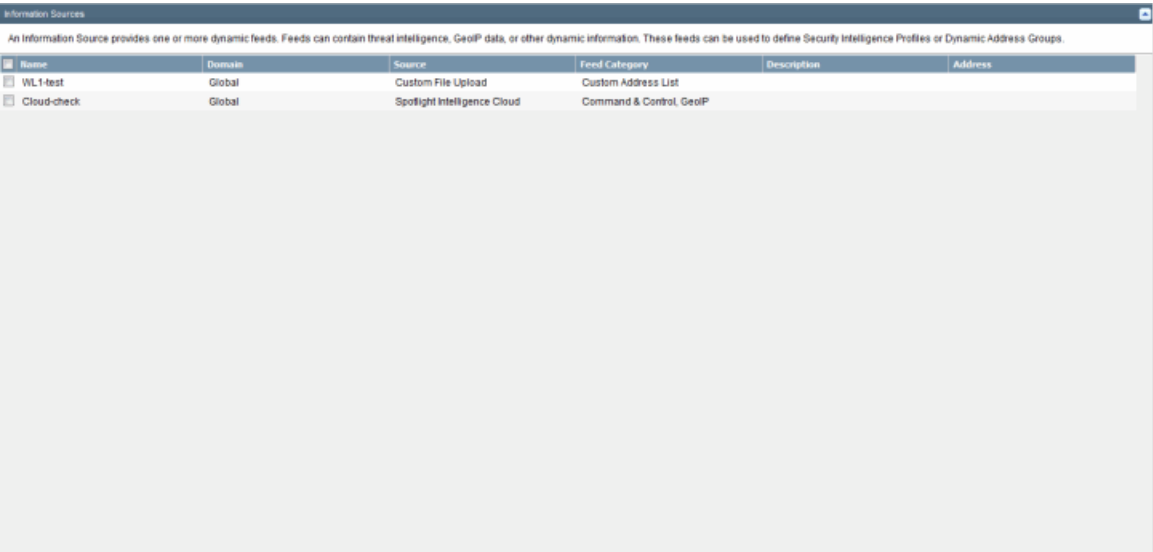
- 1. Select **Security Director > Security Intelligence**.

The landing page appears, showing the feed status of connectors and devices.

- 2. Under Security Intelligence, in the left pane, select **Information Sources**.

The Information Sources landing page appears, as shown in [Figure 49 on page 66](#).

Figure 49: Information Sources Landing Page



- 3. To create a new information source, click the plus sign (+).

The Add Information Source page appears, as shown in [Figure 50 on page 67](#).

Figure 50: Add Information Source

**Add Information Source**

Source:\* WebApp Secure

Group Name:\*

Description:

Adding a Juniper WebApp Secure feed requires the same settings provided above to be configured on each WebApp Secure Appliance that will be part of the group. The following additional information will also be needed:

Connector URL: `https://[Connector Hostname or IP Address]/api/jwas/manifest.json`

WebApp Secure Auth Token: `hXU5SbWMusL0d6rN2puqSyqaQfzAmxst`

To configure, do the following:

1. Log into the Juniper WebApp Secure Appliance.
2. Navigate to **Security Intelligence** under **Spotlight Secure** in the main menu.
3. Select the **Configure** button in the top right corner.
4. Set **Service Enabled** to **True**.
5. Enter the **Connector URL** and **Group Name** as described above.
6. Copy the **WebApp Secure Auth Token** shown above into the **Auth Token** field.
7. Select the **Test Connection Settings** link to verify the connection was made properly.

You may add multiple WebApp Secure Appliances to the same group.

**Create** **Cancel**

4. From the Source drop-down list, select the required source. The following sources are available:

- Spotlight Intelligence Cloud
- WebApp Secure
- Custom File Upload
- Custom File Server

The Spotlight Intelligence Cloud option is available only if the information source of Spotlight Intelligence Cloud type is not defined already. If the administrator has already created an information source of this type, the Spotlight Intelligence Cloud option is not shown in subsequent Add Information Source screen.

5. If you select WebApp Secure as the source, configure the following parameters:

- In the Group Name field, enter the name of the information source.
- In the Description field, enter a description of the information source.

If you select Custom File Upload as the source, configure the following parameters:

- In the Name field, enter the name of the information source.
- In the Description field, enter a description of the information source.
- To upload the custom file, click **Browse...**

You can click **View sample file** to view the sample custom file.

If you select Custom File Server as the source, configure the following parameters:

- In the Group Name field, enter the name of the information source.
- In the Description field, enter a description of the information source.
- In the Address field, enter the address of the customer host file server.
- In the Username field, enter the username of the given address.
- In the Password field, enter the password.
- From the Update Interval drop-down list, select the frequency of the update.

6. To create a new information source, click **Create**.

Once you create, update, or delete the information source, you must push the configuration to all the connected connectors.

## RELATED DOCUMENTATION

| [Managing Information Sources](#) | 68

## Managing Information Sources

### IN THIS SECTION

- [Modifying an Information Source](#) | 69
- [Deleting an Information Source](#) | 69
- [Updating Feeds to Connectors](#) | 69

To open the Information Sources page:

- Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears, listing the existing sources.

- Right-click the information source to manage it, or select the required options from Actions.

You can perform the following management tasks on the Information Sources page:

## Modifying an Information Source

To modify an existing information source:

1. Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears.

2. Select the source and click the pencil icon to modify it.

The Modify Information Source page appears.

3. Modify the required fields, and click **Modify**.

## Deleting an Information Source

To delete an information source:

1. Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears.

2. Select the source, and click the minus sign (-).

A confirmation window appears before you can delete the source.

3. To delete the source, click **Delete**.

## Updating Feeds to Connectors

To update a feed to the connectors:

1. Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears.

2. Select a source that has Spotlight Intelligence Cloud or Custom File Server as the source and right-click, or, from Actions, select **Update Feeds Now**.

All the connectors receive the feeds from the information sources based on the update interval for the feed category. You can use this option to get the feeds immediately.

3. A job is created to view the status of the feeds update.

#### RELATED DOCUMENTATION

| [Creating an Information Source](#) | 66



# Configuring Profiles and Policies

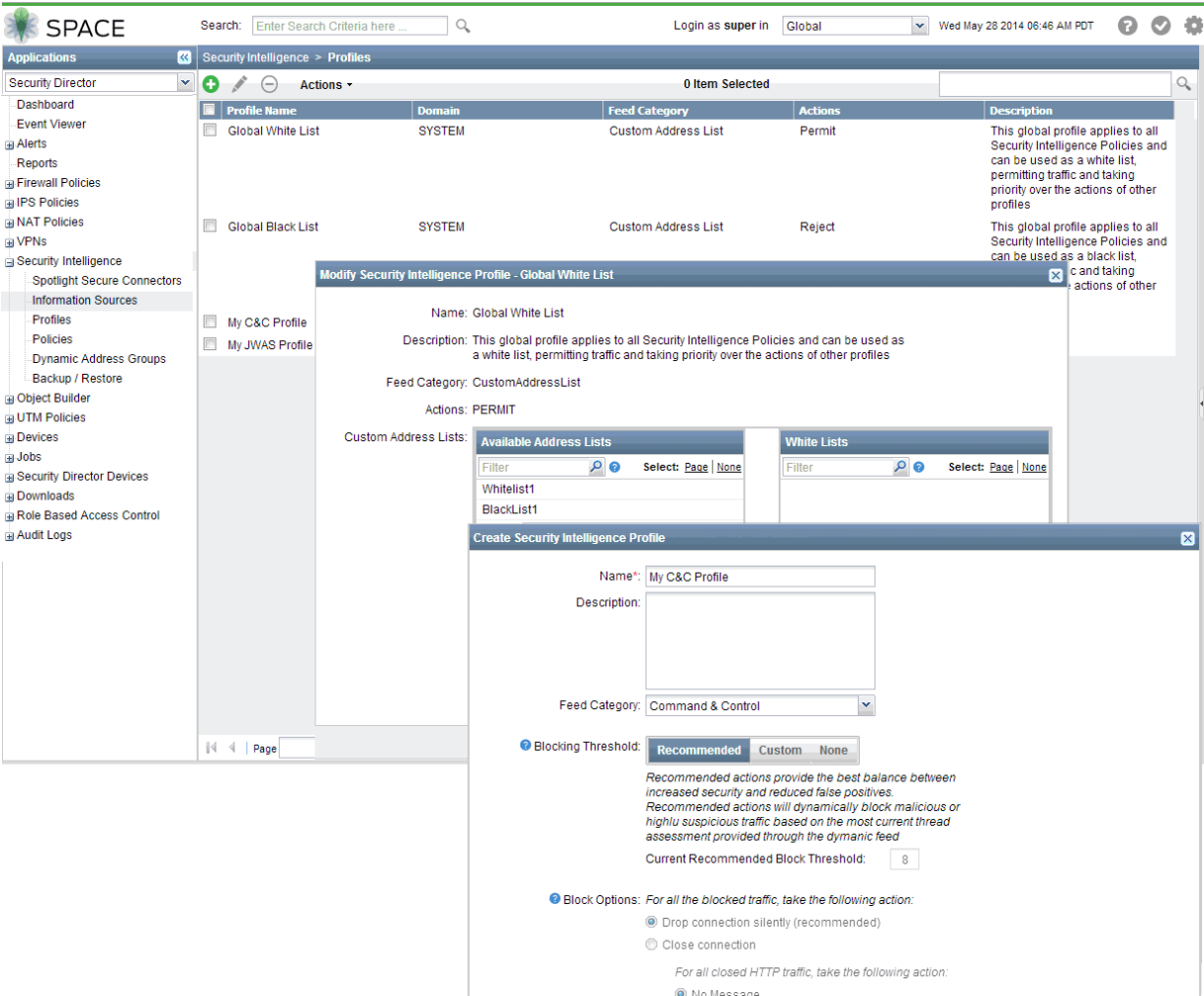
## IN THIS CHAPTER

- [Spotlight Secure Connector Profile Overview | 71](#)
- [Creating Security Intelligence Profiles | 76](#)
- [Managing Security Intelligence Profiles | 80](#)
- [Spotlight Secure Connector Policy Overview | 81](#)
- [Creating Security Intelligence Policies | 83](#)
- [Managing Security Intelligence Policies | 85](#)

## Spotlight Secure Connector Profile Overview

Spotlight Secure Connector profiles are configured on the **Security Intelligence > Profiles** page. See [Figure 51 on page 72](#). Profiles define the actions to take for a specific data feed and for a specific threat level.

Figure 51: Example Spotlight Secure Connector Profiles



By default, a global allowlist and global blocklist are provided.

Allowlist and blocklists have higher priority over other Spotlight Secure profiles and are evaluated first in security rules.

## About Threat Levels

Every attacker is assigned a name and each incident is recorded along with a threat level based on their intent and skill. The severity of the alert matches the threat level; higher severity attacks result in a higher threat level. Spotlight Secure Connector defines default actions but you can customize at what threat level to start logging events and the action to take (permit, reject, redirect) per threat level when creating the profile. See [Figure 52 on page 73](#).

Figure 52: Threat Level Settings

**Create Security Intelligence Profile**

Blocking Threshold:

Custom allows you to block traffic based on the Threat Score.

**Most aggressive**

3 **More Aggressive Security**

- Provides increased security, but a higher likelihood of [false positives](#).
- Block malicious or most suspicious traffic (with a [threat score](#) of 3 or higher).

**Least aggressive**

**Block Options:** For all the blocked traffic, take the following action:

☐ Drop connection silently

☒ Close connection (recommended)

For all closed HTTP traffic, take the following action:

☒ No Message

☐ Default Message

☐ Redirect URL

☐ Custom Message

**Logging:** ☐ Log only blocked traffic

☒ Log all traffic (recommended)

**Security Gauge:** Outcome (Less to More), Security (Less to More)

**False Positive Gauge:** Outcome (Less to More), False Positive (Less to More)

**Create** **Cancel**

Spotlight Secure Connector uses a scale of 1 (most aggressive) to 10 (least aggressive) to define the action to take depending on the threat level. When setting the threat level, attacks with threat numbers equal to and higher than the selected are blocked. For example, if you set the threat level to 4, all threat levels with a score of 4 and higher are blocked. A more aggressive threat level blocks more traffic but also creates more false positives. When you move the slider, the graphs show a general representation of the likelihood of false positives and your security level. The default setting is threat level 6.

As part of the overall Spotlight Secure solution, WebApp Secure sends information on malicious cookies and IP addresses to Spotlight Secure Connector. WebApp Secure also recommends a threat level for the session cookie or IP address, based on a set of criteria, including how malicious the associated attacker is deemed to be. Note that not all sessions are sent to the connector--only those marked as malicious.


Table 5: Mapping WebApp Secure Threat Levels to Spotlight Secure Connector Threat Levels

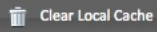
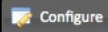
WebApp Secure Threat Level	Description	Spotlight Secure Connector Threat Level
Low	Low threat levels incorporate IP addresses and hosts where the threat is not as severe, the malicious activity has not been seen for a long period of time, or there is evidence of both malicious and non-malicious activity on the same host. For example, requesting server configuration files, non-standard HTTP requests, attempting to locate files not linked by the web server.	4-5
Medium	Medium threat levels represent a moderate threat and are unlikely to be non-malicious. For example, tampering with cookies, attempting to defeat tracking techniques, manipulating honeypot code.	6-7
High	High threat levels represent severe threats at a very high level of certainty. For example, attempting to crack passwords, session spoofing attacks, attempting to defeat WebApp Secure counter-responses.	8-10

To view session cookies and locations sent to the connector, in the WebApp Secure Web UI, navigate to **Juniper Spotlight > Spotlight Connector**. There you will find a Session Cookies tab and a Locations tab. See [Figure 53 on page 75](#).

Figure 53: Spotlight Secure Connector Session Cookies in WebApp Secure

Spotlight Secure » Security Intelligence

 **Status:** Disabled  
**Last Cookie Sync Time:** 1mo, 18d ago  
**Last Cookie Sync Status:** Failed (?)  
**Last IP Address Sync Time:** 1mo, 21d ago  
**Last IP Sync Status:** Succeeded

**Session Cookies (299)** **Locations (0)**

1 - 15 of 299

Description	Threat	Data	Last Update	Expires
Chrystal 376	8.0	qstoken=K9CWAU7iJ0N6CI2janan/g	1mo, 18d ago	1mo, 17d ago
Jacquelyn 8146	8.0	qstoken=8vsF15D/el3dufM1bgCIWg	1mo, 18d ago	1mo, 17d ago
Herman 5823	8.0	qstoken=2VqT2AwfhxILBXI4Zqo5ag	1mo, 18d ago	1mo, 17d ago
Nellie 4548	8.0	rid=f8DI9s0CXiL5M7QuIO/rrg	1mo, 18d ago	1mo, 18d ago
Martha 9831	8.0	rid=Kz/ShDaqhQUt6H5o3b79PA	1mo, 18d ago	1mo, 18d ago
Alex 5120	8.0	qstoken=MKXanGlnW99YyOCN9eRLeg	1mo, 18d ago	1mo, 18d ago
Leon 3706	8.0	qstoken=kj2Vcnx/xkxPpdxzQTumWg	1mo, 18d ago	1mo, 17d ago
Daphne 3134	8.0	qstoken=KXrKHsEmIm94k9JH23OgaA	1mo, 18d ago	1mo, 17d ago
Jo 4309	8.0	rid=5BeYgeWcVtaJp9QjUSOw3A	1mo, 18d ago	1mo, 18d ago
Victoria 4037	8.0	qstoken=UaYh48CnpBOC56VpeBRElg	1mo, 18d ago	1mo, 17d ago
Adrian 5460	8.0	qstoken=nB7A1FwFcbeHTHEaSkilbw	1mo, 18d ago	1mo, 17d ago
Lakisha 624	8.0	rid=6nvNkY3MQpOCUbMixCKFDw	1mo, 18d ago	1mo, 18d ago
Leon 3706	8.0	rid=P5EmUeE2e1BrLgsT+CXp8g	1mo, 18d ago	1mo, 18d ago
Mollie 9904	8.0	rid=eYqvXj7zgGmrfrnJVDelZrw	1mo, 18d ago	1mo, 18d ago

## Verifying Profiles On the SRX Series Device

Use the **show configuration** CLI command or the **Device Configuration View** in Network Management Platform to verify profiles are pushed to the SRX Series device. A profile section is created as shown in the following example.

```
profile JWAS-Fingerprints {
  category JWAS;
  rule Rule-1 {
    match {
      threat-level [1 2 3 4 5 6 7 8 9 10];
    }
    then {
      action {
        recommended;
      }
    }
  }
}
```

```
    log;
  }
}
```

In the example above, a profile named **JWAS-Fingerprints** now resides on the SRX Series device and uses the default recommended actions.

RELATED DOCUMENTATION

- Using Spotlight Secure Connector Policies in Security Rules | 87
- Example: Pushing a Allowlist, Blocklist, C&C, and GeoIP to a Security Device | 101

## Creating Security Intelligence Profiles

To create a profile:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles, as shown in [Figure 54 on page 76](#).

Figure 54: Profiles Page

Profiles					
Security intelligence profiles define what actions you wish to take in response to various threats. All feeds that include Threat Scores can be used in Security intelligence profiles. These profiles are used within Security Intelligence Policies. Global white and black lists are automatically applied across all Security Intelligence policies.					
Profile Name	Domain	Feed Category	Threshold Summary	Address List	Description
<input type="checkbox"/> Global White List	Global	Custom Address List			This global profile applies to all Security Intelligence Policies and can be used as a white list, permitting traffic and taking priority over the actions of other profiles
<input type="checkbox"/> Global Black List	Global	Custom Address List			This global profile applies to all Security Intelligence Policies and can be used as a black list, blocking traffic and taking priority over the actions of other profiles
<input type="checkbox"/> df-reco	Global	Device Fingerprint	Block Threshold Type: Recommended Actions Block Threshold Level: 5 Block Option: Close server & client connection Log Option: Log all traffic		
<input type="checkbox"/> cc-reco	Global	Command & Control	Block Threshold Type: Recommended Actions Block Threshold Level: 5 Block Option: Drop connections silently Log Option: Log all traffic		

2. To create a new Security Intelligence profile, click the plus sign (+).

The Create Security Intelligence Profile page appears, as shown in [Figure 55 on page 77](#).

Figure 55: Create Security Intelligence Profile Page

**Create Security Intelligence Profile**

Name:\*

Description:

Feed Category: Device Fingerprint

Blocking Threshold: Recommended Custom None

*Recommended actions provide the best balance between increased security and reduced false positives. Recommended actions will dynamically block malicious or highly suspicious traffic based on the most current threat assessment provided through the dynamic feed.*

Current Recommended Block Threshold: 6

Block Options: For all the blocked traffic, take the following action:

☐ Drop connection silently

☒ Close connection (recommended)

*For all closed HTTP traffic, take the following action:*

☒ No Message

☐ Default Message

☐ Redirect URL

☐ Custom Message

Logging: ☐ Log only blocked traffic

☒ Log all traffic (recommended)

Create Cancel

3. In the Name field, enter the name of the profile.
4. In the Description field, enter a description of the profile.
5. From the Feed Category drop-down list, select a required feed category.  
The available categories are Device Fingerprint and Command & Control. By default, the feed category is set to Device Fingerprint.
6. Configure the Blocking Threshold field to either for the recommended values, or configure your own parameters.

Recommended actions provide the best balance between increased security and reduced false positives. Recommended actions dynamically blocks malicious or highly suspicious traffic based on the most current threat assessment provided through the dynamic feed

7. If the feed category is Device Fingerprint:

- The recommended action for all the blocked traffic under Block Options is Close connection (recommended). When closing the HTTP traffic, the recommended action is not send any message to the user.
- The recommended action for log events under Logging is Log all traffic (recommended).

You can customize the data to block traffic based on the threat score, as shown in [Figure 56 on page 78](#).

Figure 56: Create Security Intelligence Profile-Custom Values

**Create Security Intelligence Profile**

Blocking Threshold:

*Custom allows you to block traffic based on the Threat Score.*

**Most aggressive**

**Default Security**

5

**Least aggressive**

- Provides the best balance between increased security and reduced [false positives](#).  
- Block malicious or suspicious traffic with a [threat score](#) of 5 or higher.

**Outcome**

Less More

**Security**

**False Positive**

Less More

Block Options: For all the blocked traffic, take the following action:

☐ Drop connection silently

☒ Close connection (recommended)

For all closed HTTP traffic, take the following action:

☒ No Message

☐ Default Message

☐ Redirect URL

☐ Custom Message

Logging: ☐ Log only blocked traffic

☒ Log all traffic (recommended)



Under Blocking Options, you can customize the following action to be taken for all the closed HTTP traffic:

- No Message
- Default Message
- Redirect URL
- Customer Message

Under Logging section, you can customize the following log events:

- Log only blocked traffic
- Log all traffic (not recommended)
- Don't log any traffic

8. If the feed category is Command & Control:

- Under the Block Options, the recommended action for all the blocked traffic is log all traffic (recommended).
- Under Logging section, the recommended action is Log only blocked traffic.

You can customize Blocking Options and Logging fields to the required values.

9. Click **Create**.

A new profile is created and added to the Profiles page.

**NOTE:**

- On the Profiles page, the Global Blocklist and Global Allowlist profiles are created by default.
- The Security Intelligence profiles can be assigned only to the firewall policies.

## RELATED DOCUMENTATION

| [Managing Security Intelligence Profiles](#) | 80

## Managing Security Intelligence Profiles

### IN THIS SECTION

- [Modifying a Security Intelligence Profile | 80](#)
- [Deleting a Security Intelligence Profile | 81](#)
- [Modifying a Global Allowlist or Global Blocklist | 81](#)

You can modify and delete the profiles that are listed on the Profiles main page.

To open the Profiles page:

- Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

- Right-click a profile to manage it.

You can perform the following management tasks on the Profiles page:

### Modifying a Security Intelligence Profile

To modify a profile:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

2. Select the profile that you want to modify, and click the pencil icon or right-click and select **Modify Security Intelligence Profile**.

The Modify Security Intelligence Profile page appears.

3. On the Modify Security Intelligence Profile page you can modify the name, description, actions, and threat levels for the Custom Actions.
4. To modify the profile, click **Modify**.

## Deleting a Security Intelligence Profile

To delete a profile:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

2. Select the profile that you want to delete, and click the minus sign or right-click and select the **Delete Security Intelligence Profile(s)** option. A confirmation window appears before you can delete the profile.

3. To delete the profile, click **Delete**.

You can delete more than one profile at a time.

## Modifying a Global Allowlist or Global Blocklist

To modify a global allowlist or a blocklist:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

2. Select Global Allowlist or Global Blocklist, right-click and select **Modify Security Intelligence Profile**.

The Modify Intelligence Profile window appears for a particular list.

3. Select the custom addresses available from the Available Address Lists. The Custom Address List feed category is assigned to these profiles.

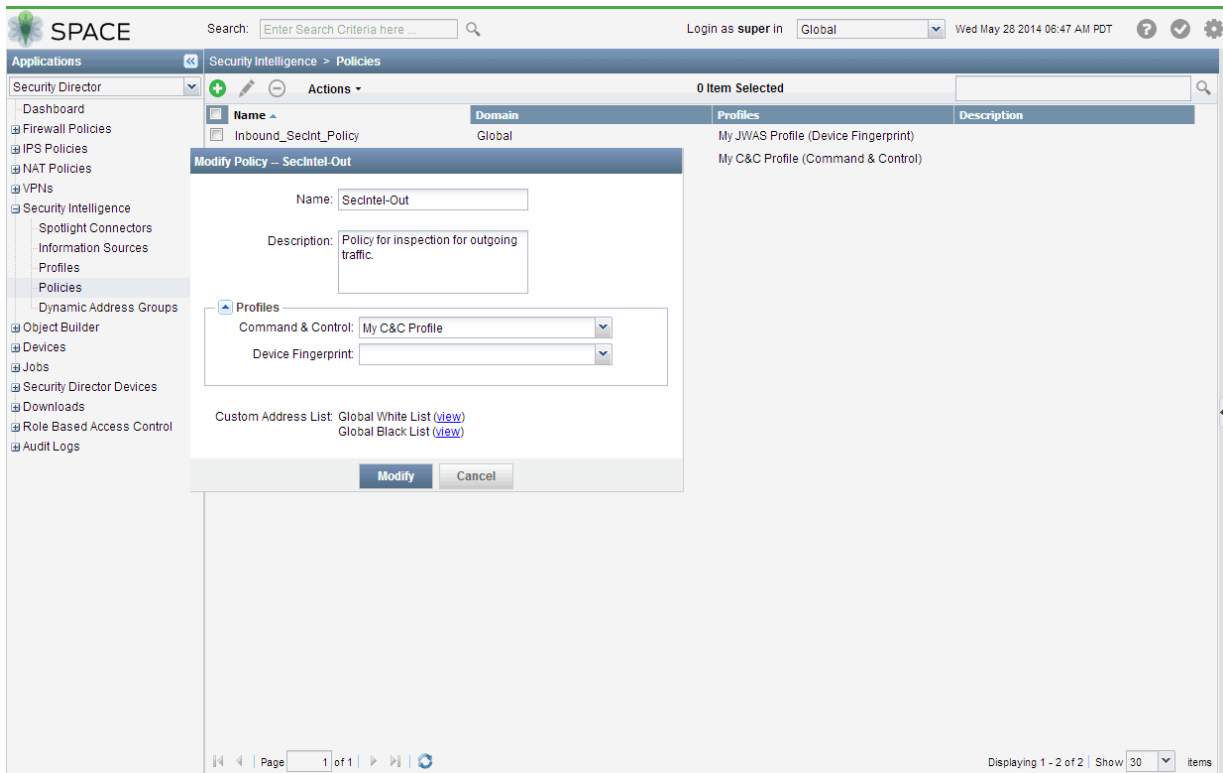
### RELATED DOCUMENTATION

| [Creating Security Intelligence Profiles](#) | 76

## Spotlight Secure Connector Policy Overview

Policies enforce a set of rules for transit traffic, identifying which traffic can pass through the security device and the actions taken on the traffic as it passes through the security device. With Spotlight Secure Connector, you can include one or more profiles to a policy and apply them across multiple security rules. See [Figure 57 on page 82](#). If you want to test a different profile, you can modify it and it will apply across all your security rules where you have referenced this policy.

Figure 57: Example Spotlight Secure Connector Policies



To verify the profiles on an SRX Series device, use the **show configuration** CLI command or the **Device Configuration View** in Network Management Platform. A policy section is added as shown in the following example.

```
policy SecIntel-Policy1 {
  CC {
    Command_and_Control;
  }
  JWAS {
    JWAS-Fingerprints;
  }
}
```

In the above example, a policy named **SecIntel-Policy1** exists and contains C&C and JWAS profiles.

## RELATED DOCUMENTATION

[Spotlight Secure Connector Profile Overview | 71](#)

[Example: Pushing a Allowlist, Blocklist, C&C, and GeoIP to a Security Device | 101](#)

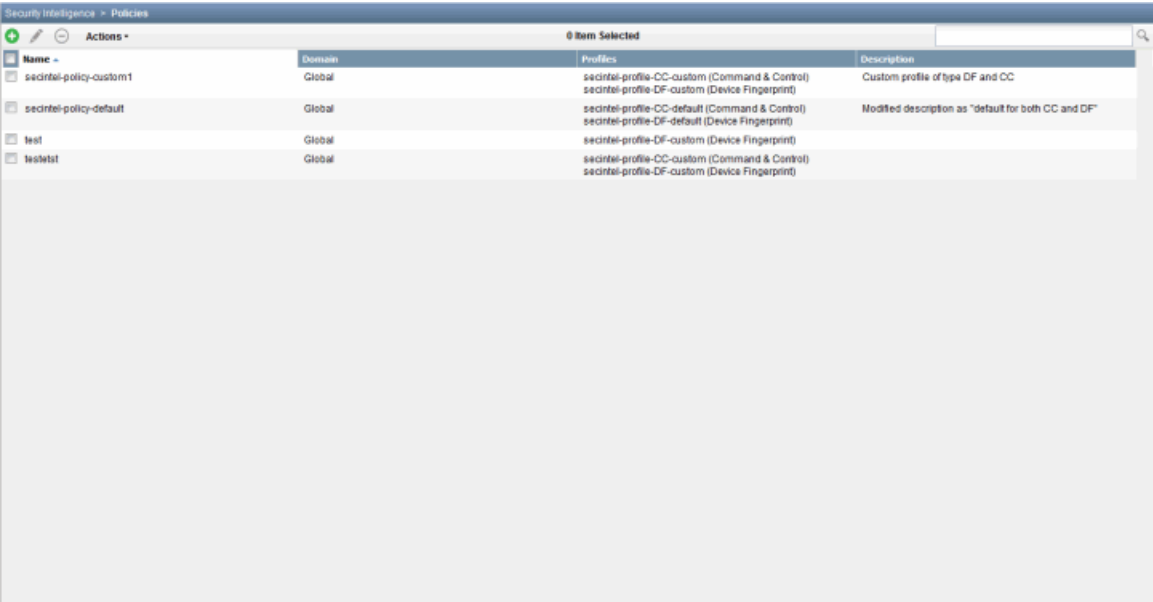
## Creating Security Intelligence Policies

To create a policy:

1. Select **Security Director > Security Intelligence > Policies**.

The Policies page appears, listing all the existing policies, as shown in [Figure 58 on page 83](#).

Figure 58: Policies Page



Security Intelligence > Policies			
0 Item Selected			
Name	Domain	Profiles	Description
secintel-policy-custom1	Global	secintel-profile-CC-custom (Command & Control) secintel-profile-DF-custom (Device Fingerprint)	Custom profile of type DF and CC
secintel-policy-default	Global	secintel-profile-CC-default (Command & Control) secintel-profile-DF-default (Device Fingerprint)	Modified description as "default for both CC and DF"
test	Global	secintel-profile-DF-custom (Device Fingerprint)	
testtest	Global	secintel-profile-CC-custom (Command & Control) secintel-profile-DF-custom (Device Fingerprint)	

2. To create a new Security Intelligence policy, click the plus sign (+).

The Create Policy page appears, as shown in [Figure 59 on page 84](#).

Figure 59: Create Policy Page

Create Policy

Name:

Description:

Profiles

Command & Control:

Device Fingerprint:

Custom Address List: [Global White List \(view\)](#)  
[Global Black List \(view\)](#)

Create Cancel

3. In the Name field, enter the name of the policy.
4. In the Description field, enter a description of the policy.
5. Under the Profiles section, configure the following profile categories:
  - Command & Control
  - Device Fingerprint
6. To view and modify the custom address list of the Global Allowlist and Global Blocklist profiles, click **View**.

The Modify Security Intelligence Profile page appears to enable you to view or modify the profile.

7. Click **Create**.

A new Security Intelligence policy is created and listed in the Policies page.

## RELATED DOCUMENTATION

Managing Security Intelligence Policies | 85

## Managing Security Intelligence Policies

### IN THIS SECTION

- [Modifying a Security Intelligence Policy | 85](#)
- [Deleting a Security Intelligence Policy | 85](#)

You can modify and delete the policies that are listed on the Policies main page.

To open the Policies page:

- Select **Security Director > Security Intelligence > Policies**.

The Policies page appears, listing the existing policies.

- Right-click a policy to manage it.

You can perform the following management tasks on the Policies page:

### Modifying a Security Intelligence Policy

To modify a policy:

1. Select **Security Director > Security Intelligence > Policies**.

The Policies page appears, listing the existing policies.

2. Select the policy that you want to modify, and click the pencil icon or right-click and select **Modify Policy**.

The Modify Policy page appears.

3. On the Modify Policy page you can modify the name, description, profiles, and custom address list.
4. To modify the policy, click **Modify**.

### Deleting a Security Intelligence Policy

To delete a policy:

1. Select **Security Director > Security Intelligence > Policies**.

The Policies page appears, listing the existing policies.

2. Select the policy that you want to delete, and click the minus sign or right-click and select the **Delete Security Intelligence Policy(ies)** option. A confirmation window appears before you can delete the policy.

3. To delete the policy, click **Delete**.

You can delete more than one policy at a time.

#### RELATED DOCUMENTATION

| [Creating Security Intelligence Policies](#) | 83



# Applying Spotlight Secure to Security Rules

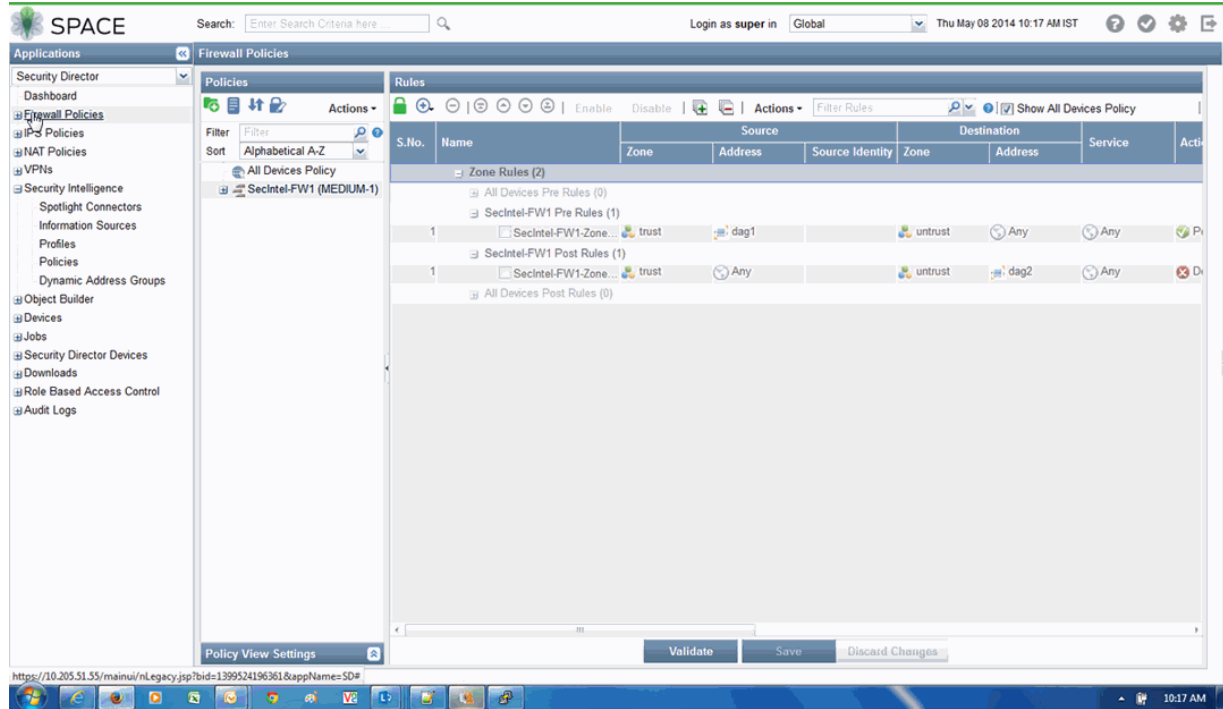
## IN THIS CHAPTER

- Using Spotlight Secure Connector Policies in Security Rules | 87
- Dynamic Address Group Overview | 91
- Creating Dynamic Address Groups | 95
- Managing Dynamic Address Groups | 97

## Using Spotlight Secure Connector Policies in Security Rules

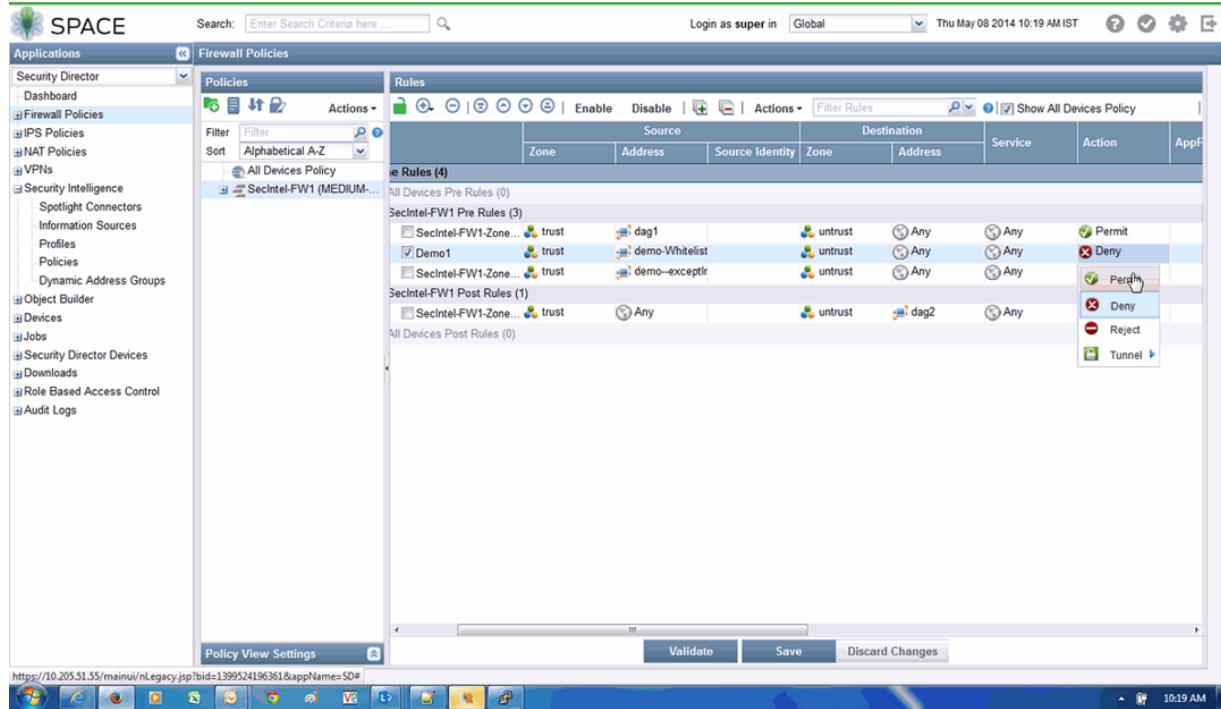
Once you defined your policies, you can assign them to a security rule. See [Figure 60 on page 88](#). The process for adding a Spotlight Secure policy to an SRX Series device is basically the same as any other policy. See [Firewall Policies Overview](#) and [Adding Rules to a Firewall Policy](#).

Figure 60: Assigning Spotlight Secure Policies to a Security Rule



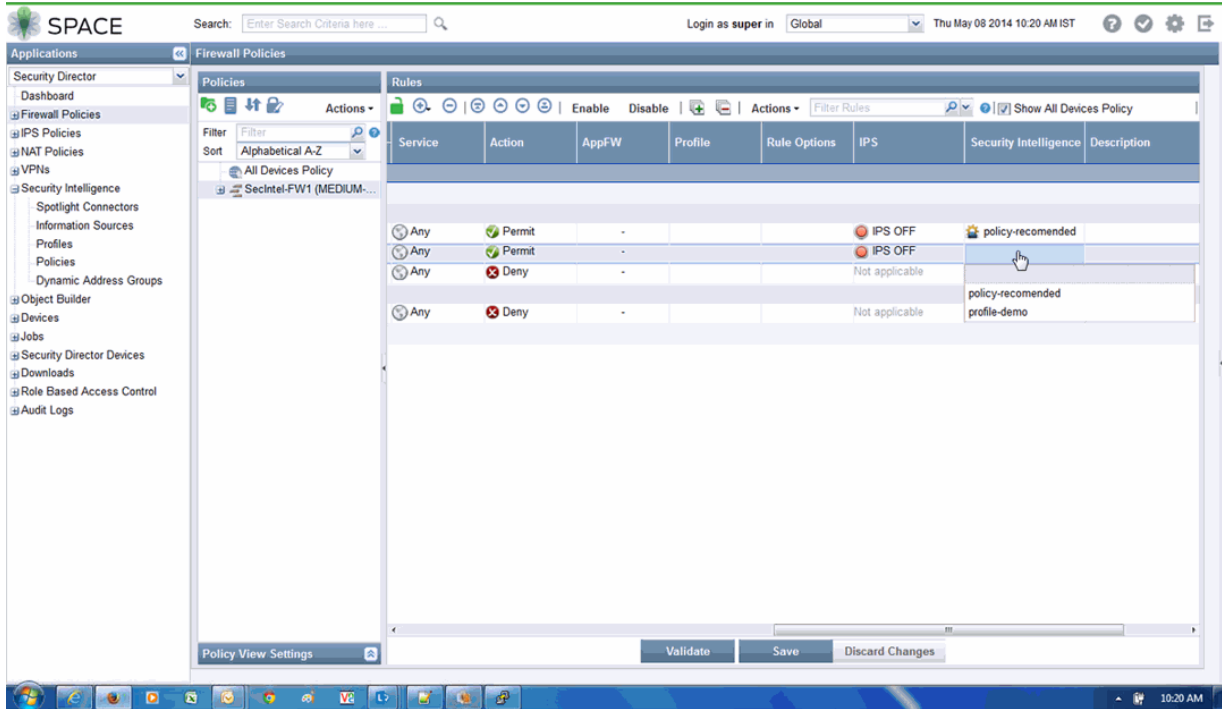
After the rule is added, you define the action (permit, deny, reject, and so forth) taken on the traffic as it passes through the security device. See [Figure 61 on page 89](#).

### Figure 61: Defining the Rule Action



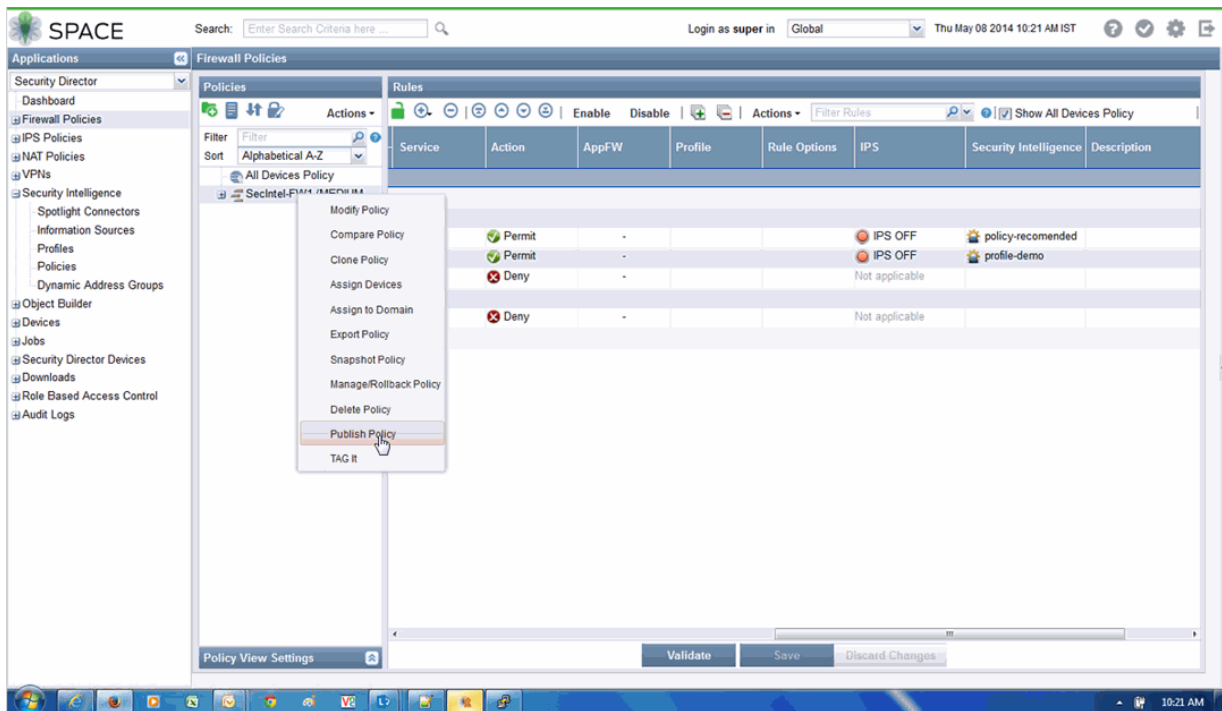
Use the Security Intelligence column to specify the Spotlight Secure policy to attach to this rule. See [Figure 62 on page 90](#).

Figure 62: Assigning the Spotlight Secure Policy to the Rule



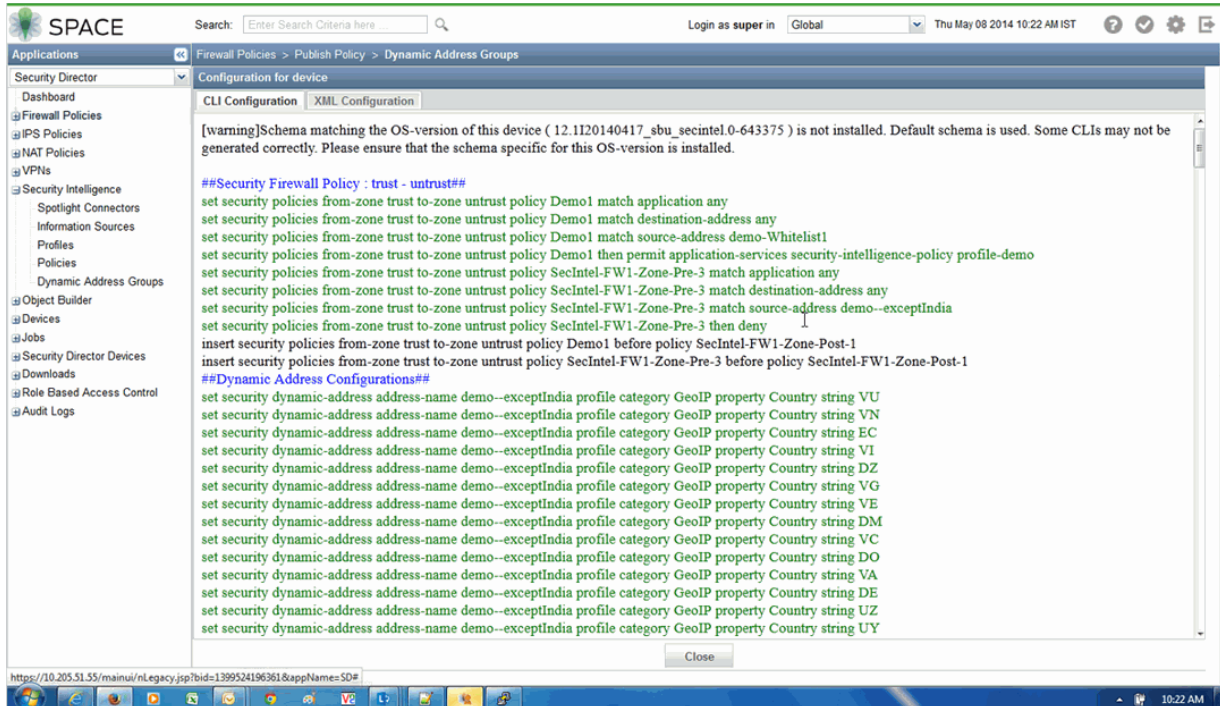
Finally, publish the policy to the SRX Series device. See [Figure 63 on page 90](#).

Figure 63: Publishing a Rule



You can view what is being published to the security device through the CLI Configuration window. See [Figure 64 on page 91](#).

**Figure 64: Viewing the Policies Pushed to the Security Device**



## RELATED DOCUMENTATION

### Dynamic Address Group Overview

Manually adding address entries into a policy can be time consuming. There are external sources that provide lists of IP addresses that have a specific purpose (such as a blocklist) or that have a common attribute (such as a particular location or behavior that might pose a threat). The administrator can leverage this external intelligence in the cloud to identify threat sources by their IP address, then group those addresses into a dynamic address entry, and reference that entry in a security policy, thereby controlling the traffic to and from those addresses. Each such group of IP addresses is referred to as a dynamic address entry.

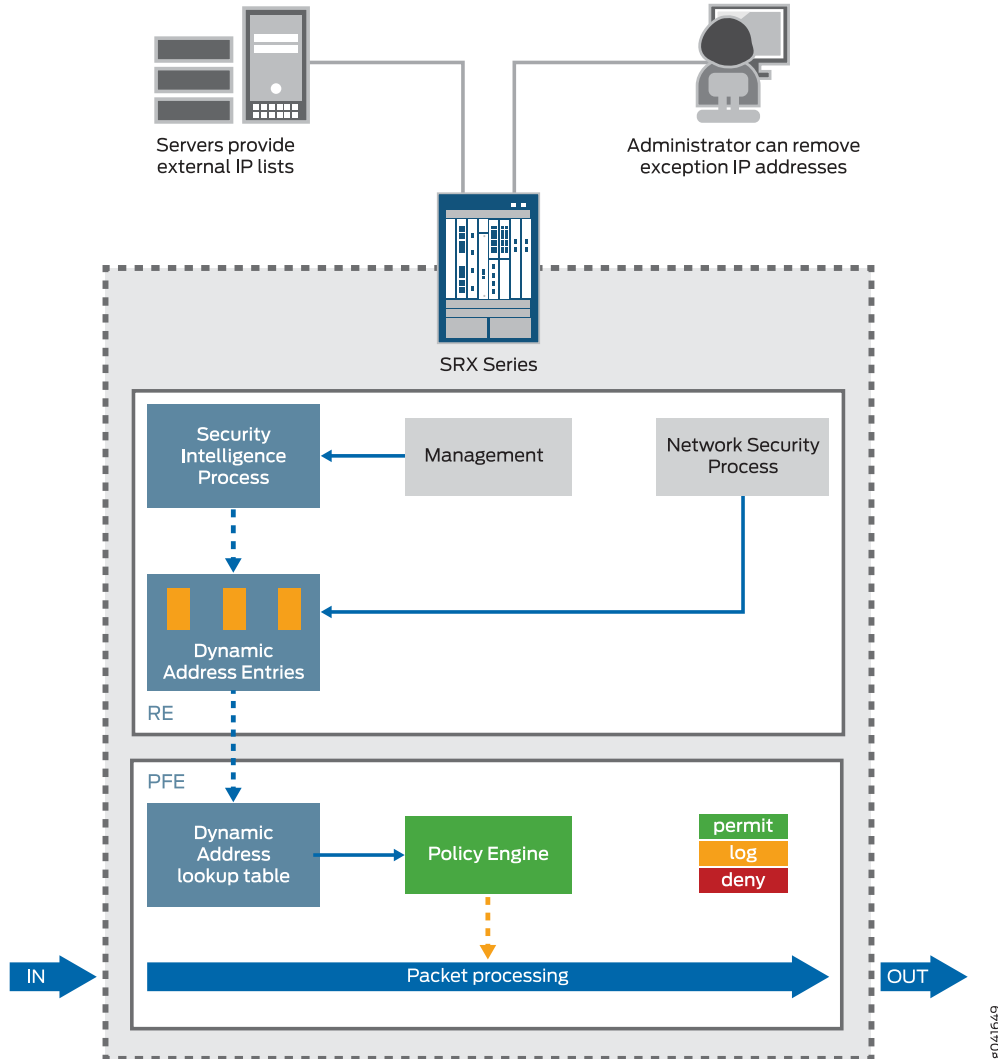
**NOTE:** A dynamic address entry is a group of IP addresses, not a single IP prefix. A dynamic address entry is different from the security address concepts of address books and address entry addresses.

There are major benefits to deploying dynamic address entries in security policies:

- The network administrator has more control over the traffic to and from groups of IP addresses.
- The network administrator can leverage the external intelligence (IP address feeds) that exists in the cloud.
- The external server provides updated IP address feeds to the SRX Series device.
- The administrator's efforts are dramatically reduced. For example, in a legacy security policy configuration, adding 1000 address entries for a policy to reference would require some 2000 lines of configuration. By defining a dynamic address entry and referencing it in a security policy, up to millions of entries could flow into the SRX Series device without much additional configuration effort.
- No commit process is required to add new addresses. Adding thousands of addresses to a configuration through a legacy method takes a long time to commit. Alternatively, IP addresses in a dynamic address entry come from an external feed, so no commit process is required when the addresses in an entry change.

[Figure 65 on page 93](#) illustrates a functional overview of how the dynamic address entry in a security policy works.

Figure 65: Functional Components of the Dynamic Address Entry in a Security Policy

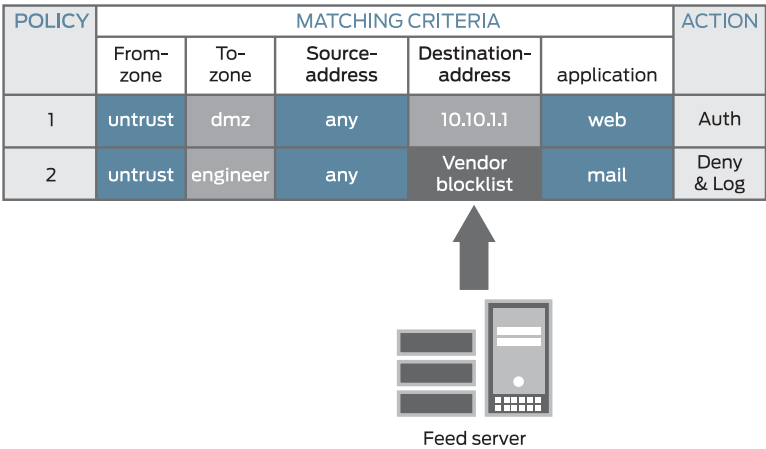


The Spotlight Secure process (daemon) periodically retrieves an IP address feed file or an update to the file from the external source (or server) and decodes the server data into a dynamic address entry. A dynamic address entry contains many IP addresses that share a common purpose or attribute, such as a geographical origin, a threat type, or a threat level.

A security policy then references the dynamic address entry in a source address or destination address field (in much the same way that a security policy references a legacy address entry).

Figure 66 on page 94 illustrates a policy that uses a dynamic address entry in the Destination-address field.

Figure 66: A Dynamic Address Entry in a Security Policy



In [Figure 66 on page 94](#), Policy 1 uses the destination address 10.10.1.1, which is a legacy security address entry. Policy 2 uses the destination address Vendor blocklist, which is a dynamic address entry named by the network administrator. Its content is the list of IP addresses retrieved from an external feed file. Packets that match all five criteria (the From-zone named untrust, the To-zone named engineer, any source address, a destination IP address that belongs to the Vendor blocklist dynamic address entry, and the mail application) are handled according to the policy actions, which are to deny and log the packet.

**NOTE:** The dynamic address entry names share the same name space as legacy security address entries, so do not use the same name for more than one entry. The Junos OS commit process checks that names are not duplicated to avoid a conflict.

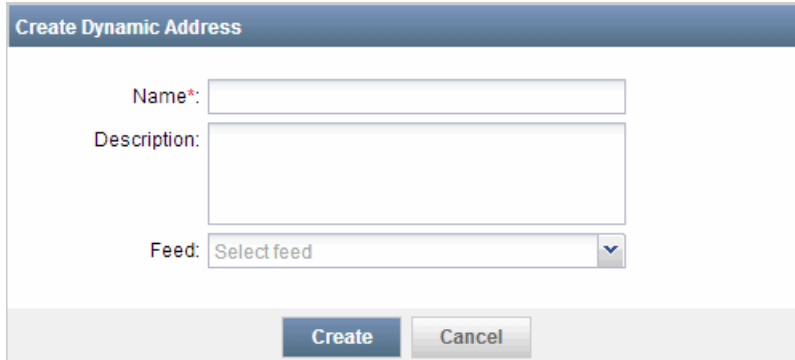
Dynamic address groups support the following data feeds:

- Custom lists (allowlists and blocklists)
- GeoIP

[Figure 67 on page 95](#) shows the dialog box for creating a dynamic address group in Security Director.



Figure 67: Creating a Dynamic Address Group



The screenshot shows a dialog box titled "Create Dynamic Address". It has three input fields: "Name\*" (a single-line text box), "Description:" (a multi-line text box), and "Feed:" (a dropdown menu currently showing "Select feed"). At the bottom of the dialog are two buttons: "Create" and "Cancel".

#### RELATED DOCUMENTATION

## Creating Dynamic Address Groups

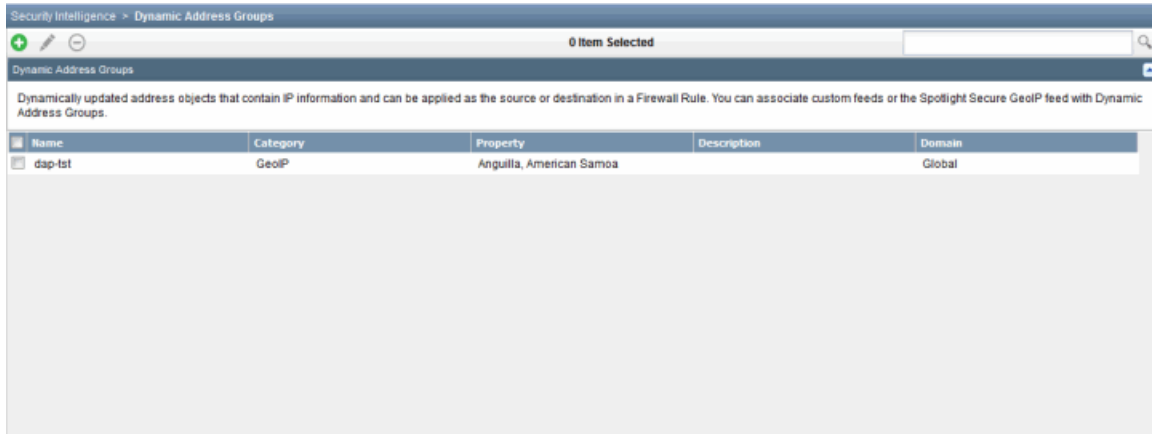
Dynamic address is an infrastructure that serves as a container for a list of IP addresses propagated from an external data feed. In Security Director, it is referenced by the firewall policy in the same way as the security legacy address entry. The only difference is that the content (such as IP addresses, prefixes, or ranges) contained in the Dynamic Address Entry(DAE) changes dynamically based on a periodic update retrieval from an external feed.

To create a dynamic address group:

1. Select **Security Director > Security Intelligence > Dynamic Address Groups**.

The Dynamic Address Groups page appears, as shown in [Figure 68 on page 96](#).

**Figure 68: Dynamic Address Groups Main Page**



2. To create a new dynamic address group, click the plus sign (+).

The Create Dynamic Address Group page appears, as shown in [Figure 69 on page 96](#).

**Figure 69: Create Dynamic Address Page**

**Create Dynamic Address Group**

Name:\*

Description:

Feed:\*

3. In the Name field, enter the name of the dynamic address group.
4. In the Description field, enter a description.

5. From the Feed drop-down list, select the external data feed.

6. Click **Create**.

A new dynamic address is created. This can be used only in the firewall policy.

## RELATED DOCUMENTATION

[Managing Dynamic Address Groups | 97](#)

# Managing Dynamic Address Groups

## IN THIS SECTION

- [Modifying a Dynamic Address Group | 98](#)
- [Deleting an Address from a Dynamic Address Group | 99](#)

You can modify and delete the dynamic addresses that are listed on the Dynamic Address Groups main page.

To open the Dynamic Address Groups page:

- Select **Security Director > Security Intelligence > Dynamic Address Groups**.

The Dynamic Address Groups page appears, listing the existing dynamic addresses.

- Right-click a dynamic address to manage it.

You can perform the following management tasks on the Dynamic Address Groups page:

## Modifying a Dynamic Address Group

To modify a dynamic address group:

1. Select **Security Director > Security Intelligence > Dynamic Address Groups**.

The Dynamic Address Groups page appears.

2. Select the dynamic address that you want to modify, and click the pencil icon or right-click and select **Modify SecIntel Dynamic Address**.

The Modify Dynamic Address page appears, as shown in [Figure 70 on page 98](#).

Figure 70: Modify Dynamic Address Page

Modify Dynamic Address -- dag1

Name: dag1

Description:

Feed: GeoIP

Countries: Albania, Angola, Antigua and Barbuda

☐ Negate Selected Countries

Modify Cancel

3. On the Modify Dynamic Address page, you can modify the name, description, feed, and countries list in addition to modifying the dynamic address.
4. Click inside the Countries field, and select the required countries from the drop-down list.  
The IP addresses shown from the countries in the list are included.
5. If you select the Negate Selected Countries option, the IP addresses from all the countries, except those listed in the Countries field, are included.
6. To modify a dynamic address, click **Modify**.

## Deleting an Address from a Dynamic Address Group

To delete a dynamic address from a dynamic address group:

1. Select **Security Director > Security Intelligence > Dynamic Address Groups**.

The Dynamic Address Groups page appears.

2. Select the dynamic address that you want to delete, and click the minus sign(-) or right-click and select the **Delete SecIntel Dynamic Addresses** option. A confirmation window appears before you can delete the address.

3. To delete the address, click **Delete**.

You can delete more than one dynamic address at a time.

### RELATED DOCUMENTATION

| [Creating Dynamic Address Groups](#) | 95

# 4

PART

## Examples

---

Configuration Examples | **101**

---

# Configuration Examples

## IN THIS CHAPTER

- [Example: Pushing a Allowlist, Blocklist, C&C, and GeoIP to a Security Device | 101](#)

## Example: Pushing a Allowlist, Blocklist, C&C, and GeoIP to a Security Device

### IN THIS SECTION

- [Defining the Information Sources | 101](#)
- [Creating the Profiles | 105](#)
- [Creating the Spotlight Secure Policy | 110](#)
- [Creating the Dynamic Address Groups | 111](#)
- [Associating the SRX Series Device With the Connector | 112](#)
- [Creating the Firewall Policy and Rules | 113](#)

This example describes how to push a allowlist, blocklist, command and control, and geography IP feed to an SRX Series device. This example assumes that the connector is already created and is part of the Security Director fabric and that the SRX Series device is already added as a device to Junos Space Network Management Platform.

### Defining the Information Sources

The first step is to upload the data feeds into the connector. In this example:

- The blocklist and allowlist are uploaded from a file on the local system.
- The command and control feed comes from the Spotlight Intelligence Cloud.
- The geography IP data, which also comes from the Spotlight Intelligence Cloud, is configured as a dynamic address group and is described later.

To define the blacklist, allowlist, and command and control information sources:

1. In the Junos Space Security Director Platform user interface, select **Security Intelligence > Spotlight Connectors > Information Sources**.
2. Click **Add New Information Source**.
3. Select **Custom File Upload** from the Source pull-down menu. Enter **feed\_source\_blacklist** as the name and **Feed for blacklist** as the description.
4. Click **Select File**, locate the blacklist source file and click **Open**. See [Figure 71 on page 102](#).

Figure 71: Defining the Blocklist Information Source

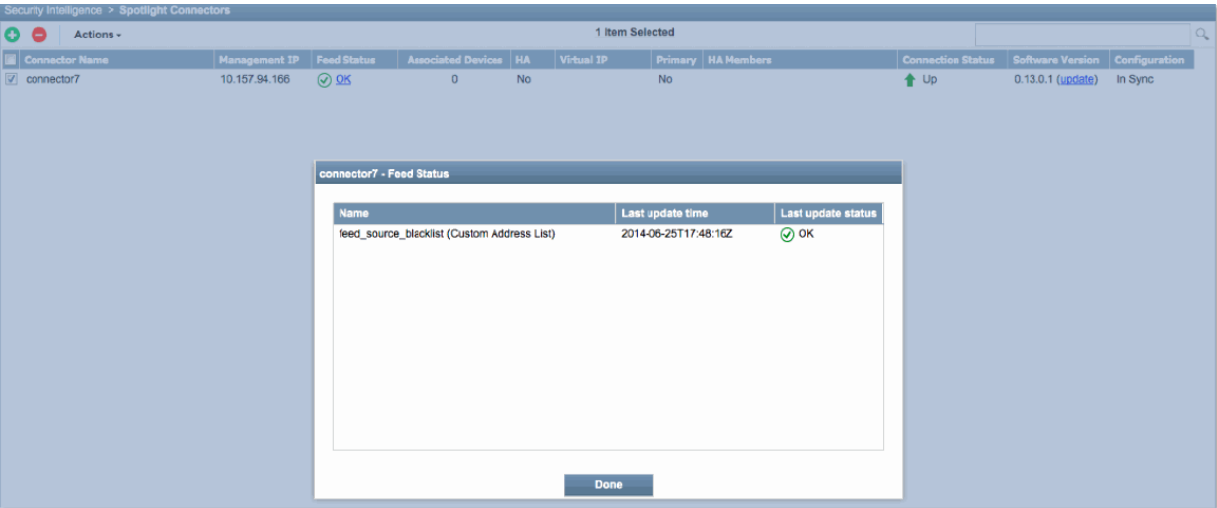
The screenshot shows a web-based form titled "Add Information Source". It contains the following fields and controls:

- Source:** A dropdown menu with "Custom File Upload" selected.
- Name:** A text input field containing "feed\_source\_blacklist".
- Description:** A text area containing "Feed for blacklist".
- File:** A text input field containing "blacklist.dat". To its right is a button labeled "Select file....".
- Buttons:** At the bottom of the form are two buttons: "Create" and "Cancel".

5. Click **Create**.
6. Click the connector feed status to verify the blacklist file is uploaded to the connector. See [Figure 72 on page 103](#).

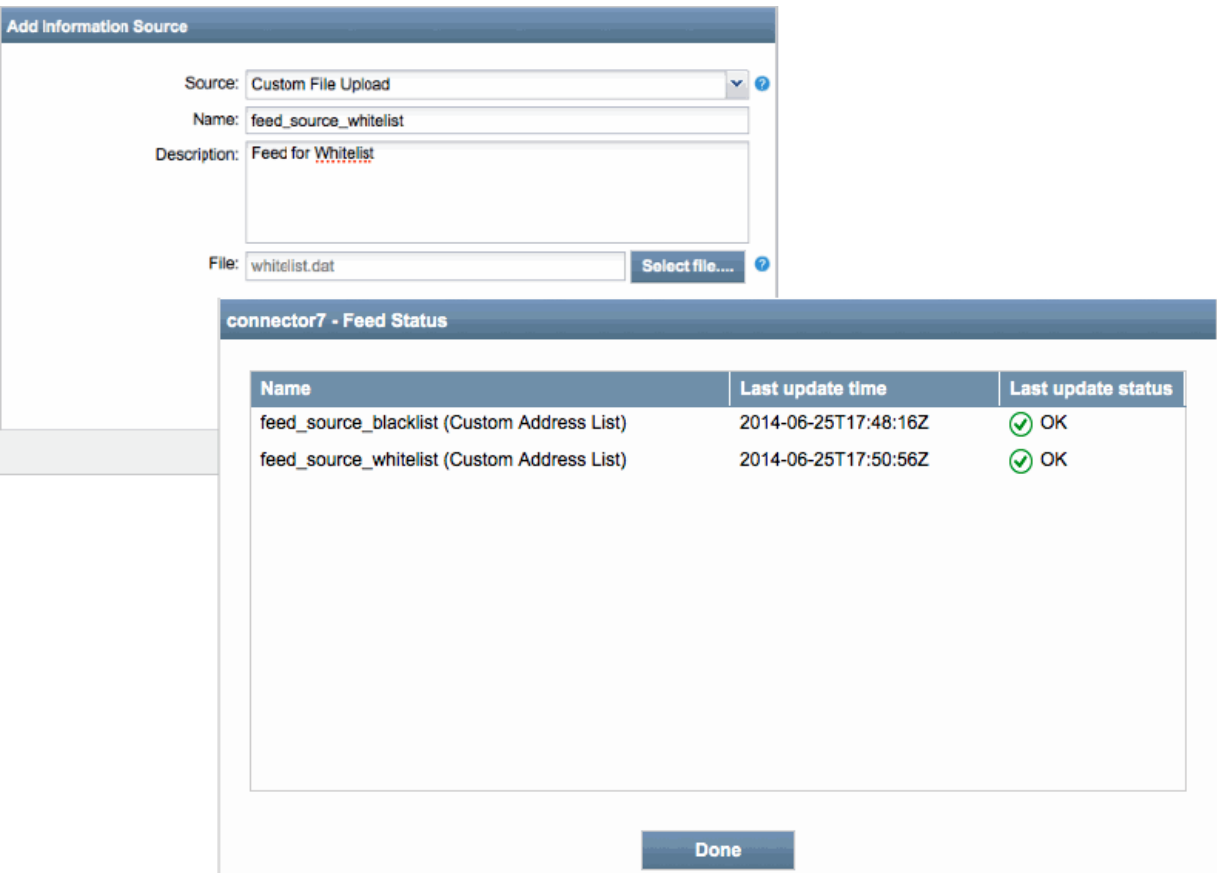


Figure 72: Checking the Feed Status for the Blocklist Update



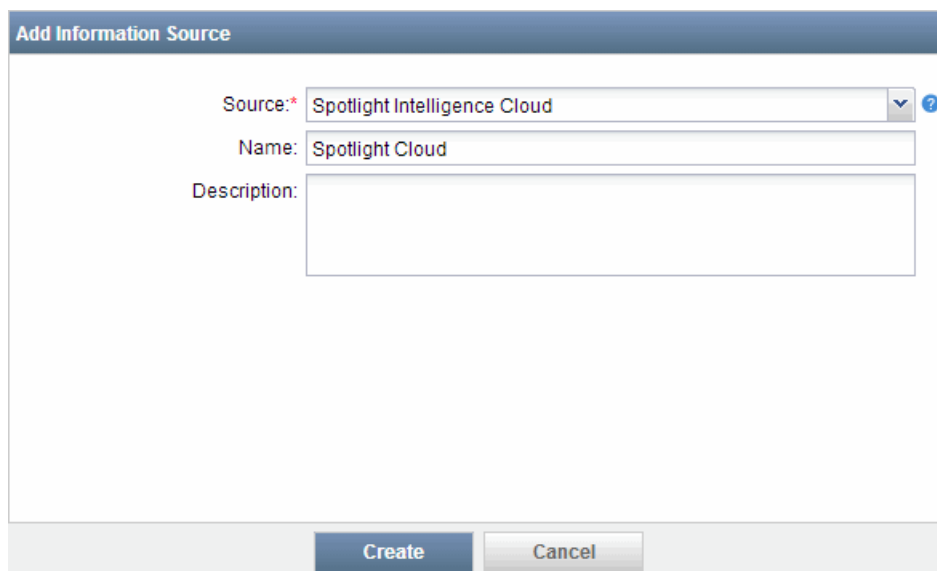
- 7. Repeat Steps 2-5 for the allowlist file. The connector feed status shows the blocklist and allowlist files are both uploaded to the connector. See [Figure 73 on page 103](#).

Figure 73: Defining the Allowlist and Checking the Feed Status



8. Click **Add New Information Source**.
9. Select **Spotlight Intelligence Cloud** from the Source pull-down menu. Enter **Spotlight Cloud** as the name and click **Create**. See [Figure 74 on page 104](#).

**Figure 74: Adding the Spotlight Intelligence Cloud Information Source**



The screenshot shows a dialog box titled "Add Information Source". It contains three input fields: "Source:\*" with a dropdown menu showing "Spotlight Intelligence Cloud", "Name:" with a text box containing "Spotlight Cloud", and "Description:" with an empty text box. At the bottom, there are two buttons: "Create" and "Cancel".

You can create only one Spotlight Intelligence Cloud information source. Once created, the cloud retrieves all subscribed feeds.

10. Click the connector feed status to make sure the feeds have been uploaded. The Spotlight Intelligence Cloud adds a cc\_ip\_data, cc\_url\_data, and geoip\_country feed. See [\[xref target has no title\]](#).

Figure 75: Checking the Feed Status for Spotlight Intelligence Cloud Information Sources

connector7 - Feed Status		
Name	Last update time	Last update status
cc_ip_data (Command & Control)	2014-06-25T17:54:22Z	✓ OK
cc_url_data (Command & Control)	2014-06-25T17:53:51Z	✓ OK
geoip_country (GeoIP)	2014-06-25T17:54:17Z	✓ OK
feed_source_blacklist (Custom Address List)	2014-06-25T17:48:16Z	✓ OK
feed_source_whitelist (Custom Address List)	2014-06-25T17:50:56Z	✓ OK

Done

## Creating the Profiles

Next, add our custom allowlist and blocklist to the global allowlist and global blocklist profiles and create a profile for the command and control feed.

To create the Spotlight Secure profiles:

1. In the Junos Space Security Director Platform user interface, select **Security Intelligence > Spotlight Connectors > Profiles**.

By default a Global White List and a Global Black List profile are provided. See [Figure 76 on page 105](#).

Figure 76: Default Profiles

Security Intelligence > Profiles				
0 Item Selected				
Profile Name	Domain	Feed Category	Actions	Description
<input type="checkbox"/> Global White List	Global	Custom Address List	Permit	This global profile applies to all Security Intelligence Policies and can be used as a white list, permitting traffic and taking priority over the actions of other profiles
<input type="checkbox"/> Global Black List	Global	Custom Address List	Reject	This global profile applies to all Security Intelligence Policies and can be used as a black list, permitting traffic and taking priority over the actions of other profiles

2. Select the Global Blacklist check box and click **Modify Profile**.
3. Select **feed\_source\_blacklist** and move it to the Blocklist column. See [Figure 77 on page 106](#).

Figure 77: Adding the Custom Blocklist to the Global Blocklist

**Modify Security Intelligence Profile - Global Black List**

Name: Global Black List



Description: This global profile applies to all Security Intelligence Policies and can be used as a black list, permitting traffic and taking priority over the actions of other profiles

Feed Category: CustomAddressList

Actions: REJECT



Custom Address Lists:

**Available Address Lists**

Filter   Select: Page | None

feed\_source\_whitelist

**Black Lists**

Filter   Select: Page | None

feed\_source\_blacklist

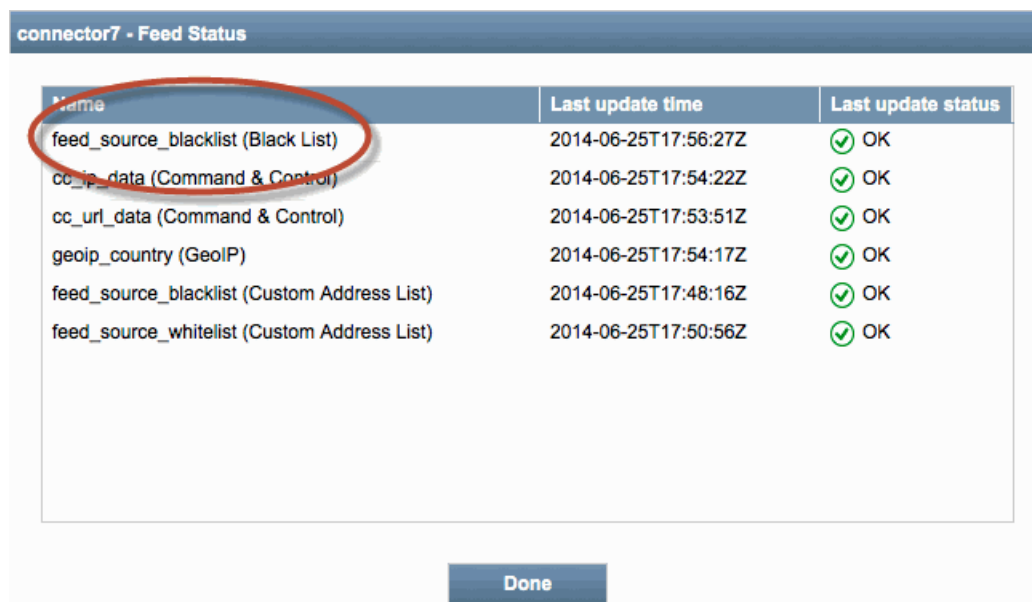
Total: 1

**Modify** **Cancel**

4. Click **Modify**.

View the connector feed status window to verify that the custom blocklist file is uploaded.

Figure 78: Viewing the Feed Status for the Global Blocklist



Name	Last update time	Last update status
feed_source_blacklist (Black List)	2014-06-25T17:56:27Z	✓ OK
cc_ip_data (Command & Control)	2014-06-25T17:54:22Z	✓ OK
cc_url_data (Command & Control)	2014-06-25T17:53:51Z	✓ OK
geoip_country (GeoIP)	2014-06-25T17:54:17Z	✓ OK
feed_source_blacklist (Custom Address List)	2014-06-25T17:48:16Z	✓ OK
feed_source_whitelist (Custom Address List)	2014-06-25T17:50:56Z	✓ OK

Done

5. Select the Global Whitelist check box and click **Modify Profile**.
  6. Select **feed\_source\_whitelist** and move it to the Allowlists column. See [Figure 73 on page 103](#).
- Note that feed\_source\_blacklist is not available as an option since it is already used in the Global Blacklist profile. A file cannot be used for both a allowlist and blacklist profile.

Figure 79: Adding the Custom Blocklist to the Global Blocklist

**Modify Security Intelligence Profile - Global White List**

Name: Global White List

Description: This global profile applies to all Security Intelligence Policies and can be used as a white list, permitting traffic and taking priority over the actions of other profiles

Feed Category: CustomAddressList

Actions: PERMIT

Custom Address Lists:

Available Address Lists	White Lists
Filter [ ] [ ] Select: Page   None	Filter [ ] [ ] Select: Page   None
	feed_source_whitelist
	Total: 1

Modify Cancel

7. (optional) Check the connector feed status to verify that the allowlist is uploaded.
8. Click **Add New Profile**.
9. Enter **cc\_profile** as the name, **Command and Control Profile** as the description, and select **Command & Control** from the Feed Category pull-down menu. In this example, we will use the default recommended actions for the blocking threshold. See [Figure 80 on page 109](#).

Figure 80: Creating the Command and Control Profile

Create Security Intelligence Profile

Name\*:cc\_profile

Description:Command and Control Profile

Feed Category:Command & Control

Blocking Threshold:

Recommended

Custom

None

Recommended actions provide the best balance between increased security and reduced false positives. Recommended actions will dynamically block malicious or highly suspicious traffic based on the most current threat assessment provided through the dynamic feed

Current Recommended Block Threshold:8

Block Options: For all the blocked traffic, take the following action:

Drop connection silently (recommended)

Close connection

For all closed HTTP traffic, take the following action:

No Message

Default Message

Redirect URL

Customer Message

Logging:

Log only blocked traffic

Log all traffic

Create

Cancel

10. Click **Create**.

The Command and Control profile is added to the profiles list. See [Figure 81 on page 109](#).

Figure 81: Command and Control Profile Added to Profile List

Security Intelligence > Profiles				
0 Item Selected				
Profile Name	Domain	Feed Category	Actions	Description
Global White List	Global	Custom Address List	Permit	This global profile applies to all Security Intelligence Policies and can be used as a white list, permitting traffic and taking priority over the actions of other profiles
Global Black List	Global	Custom Address List	Reject	This global profile applies to all Security Intelligence Policies and can be used as a black list, permitting traffic and taking priority over the actions of other profiles
cc_profile	Global	Command & Control		Command and Control Profile

### Creating the Spotlight Secure Policy

In this section, we will create the security intelligence policy for the command and control profile. Spotlight Secure policies are added to firewall rules from the Security Intelligence pull-down menu. See [Figure 82 on page 110](#).

Figure 82: Referencing the Spotlight Secure Policy within the Firewall Rule



To create the Spotlight Secure policy:

1. In the Junos Space Security Director Platform user interface, select **Security Intelligence > Spotlight Connectors > Policies**.
2. Click **Add New Policy**.
3. Enter **secintel\_policy** for the name and **Secintel Policy 1** for the description and select **cc\_profile** from the Command & Control pull-down menu. See [Figure 83 on page 110](#).

Figure 83: Creating the Command and Control Spotlight Secure Policy

A screenshot of the 'Create Policy' form in the Junos Space Security Director Platform user interface. The form has a blue header with the title 'Create Policy'. Below the header, there are two input fields: 'Name\*' with the value 'secintel\_policy' and 'Description' with the value 'Secintel Policy 1'. Below these is a section titled 'Profiles' with a blue arrow icon. Inside this section, there are two dropdown menus: 'Command & Control' with the value 'cc\_profile' and 'Device Fingerprint' with a blank value. Below the 'Profiles' section, there are two links: 'Global White List (view)' and 'Global Black List (view)'. At the bottom of the form, there are two buttons: 'Create' and 'Cancel'.



Note that the global whitelist and blacklist are also part of this policy and are pushed to the SRX Series device along with the command and control information.

4. Click **Create**.

## Creating the Dynamic Address Groups

Next, we will create a dynamic address group for the geography IP address (allowing IP addresses originating from Argentina) and the blacklist. Note that this is the same blacklist file pushed in the section above. Normally you do not need to push the same blacklist again; however, this example shows how to use dynamic address groups to push custom feeds such as allowlist and blocklists.

To create the dynamic address groups:

1. In the Junos Space Security Director Platform user interface, select **Security Intelligence > Spotlight Connectors > Dynamic Address Group**.
2. Enter **Argentina\_ip\_list** as the name, **GeolIP list of Argentina** as the Description, select **GeolIP** from the Feed pull-down menu and select **Argentina** from the Countries list. See [Figure 84 on page 111](#).

Figure 84: Creating the Geography IP Dynamic Address Group

The screenshot shows the 'Create Dynamic Address' form with the following fields and values:

- Name\*:** Argentina\_ip\_list
- Description:** GeolIP list of Argentina
- Feed:** GeolIP (selected from a dropdown menu)
- Countries\*:** Argentina (selected from a list, with a close button 'x' next to it)
- ☐ Negate Selected Countries
- Buttons:** Create, Cancel

3. Click **Create**.
4. In the Junos Space Security Director Platform user interface, select **Security Intelligence > Spotlight Connectors > Dynamic Address Group**.

- 5. Enter **to\_block** as the name, **Blacklist ips** as the description, and select **feed\_source\_blacklist** from the Feed pull-down menu.

Create Dynamic Address

Name\*: to\_block

Description: Blacklist ips

Feed: feed\_source\_blacklist(Custom Address List)

Create

Cancel

- 6. Click **Create**.

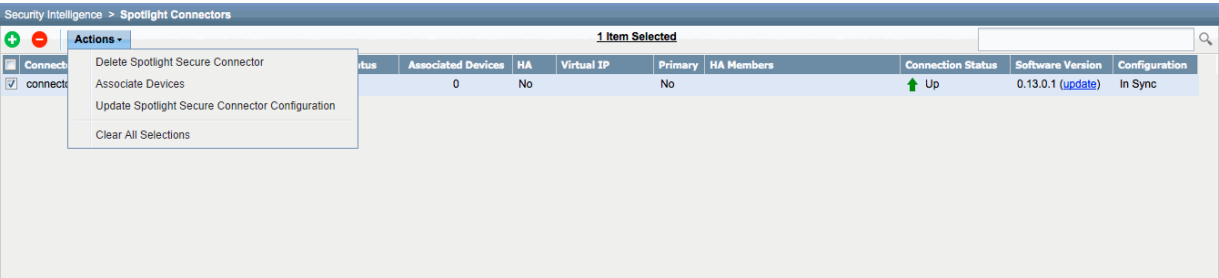
Associating the SRX Series Device With the Connector

In this example, the SRX Series device is not yet associated with the connector. This section describes the association process. You have to do this process only once for each pairing.

To associate the SRX Series device with the connector:

- 1. Select the check box next to connector7 and then select **Actions > Device Association**. See [Figure 85 on page 112](#).

Figure 85: Choosing the Device Association Command



2. Move **guavabert** to the Selected table and click **Save**.

**connector7 - Device Association**

Available		Selected	
Device	Domain	Device	Domain
guavabert	Global		

Total: 1

**Save** **Cancel**

Guavabert is now paired with connector7 and can start receiving data feeds.

## Creating the Firewall Policy and Rules

In this section, we will create the firewall policy and then add the following rules:

- Allow IP addresses that originate from Argentina.
- Block IP addresses based on the blocklist information source through dynamic address groups.
- Allow IP addresses that match the allowlist and block IP addresses based on the command and control source and blocklist through the Spotlight Secure policy.

See [Junos Space Network Management Platform](#) for more information on creating firewall policies and rules.

To create the firewall policy and rules:

1. In the Junos Space Security Director Platform user interface, select **Firewall Policy**.
2. Click **Create Policy** from the left pane.

3. Set the following options:

Option	Value
Type	Device
Name	guavabert_policy
Description	Guavabert FW policy
Manage	Zone Policy
Policy Priority	Medium
Profile	All Logging Enabled
Device	guavabert
IPS Configuration Mode	None

See [Figure 86 on page 115](#).

Figure 86: Creating the Firewall Policy

**Create Policy**

Type: ☐ Group  
☒ Device

Name\*: guavabert\_policy

Description: Guavabert FW policy

Manage\*: ☒ Zone Policy ?  
☐ Global Policy  
☐ Both Zone & Global Policy

Policy Priority\*: Medium - 1 Of 1 ?

Profile: All Logging Enabled

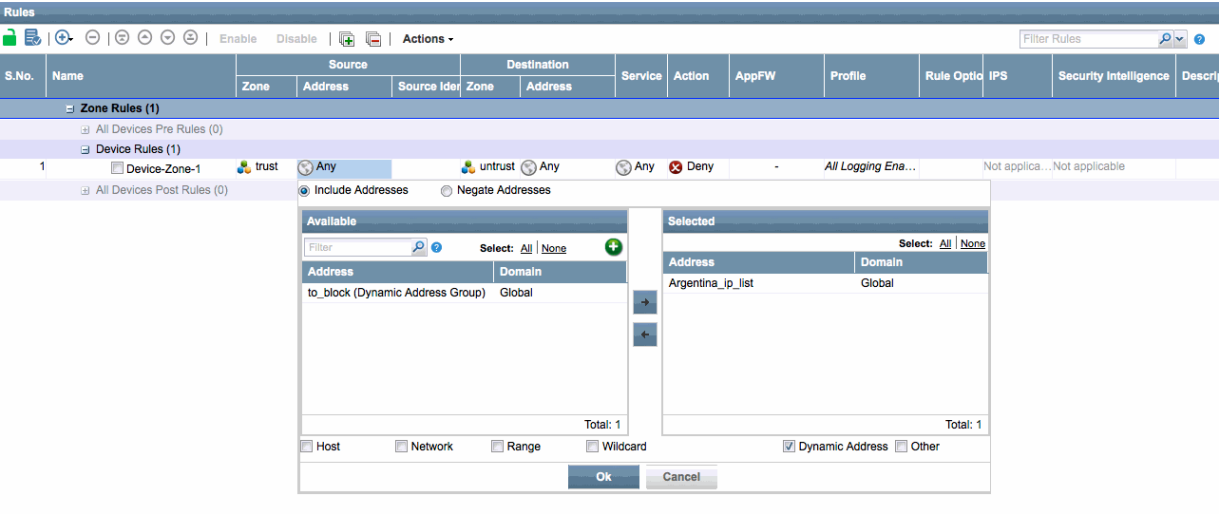
Device: guavabert

IPS Configuration Mode: ☒ None ?  
☐ Basic  
☐ Advanced

**Create** **Cancel**

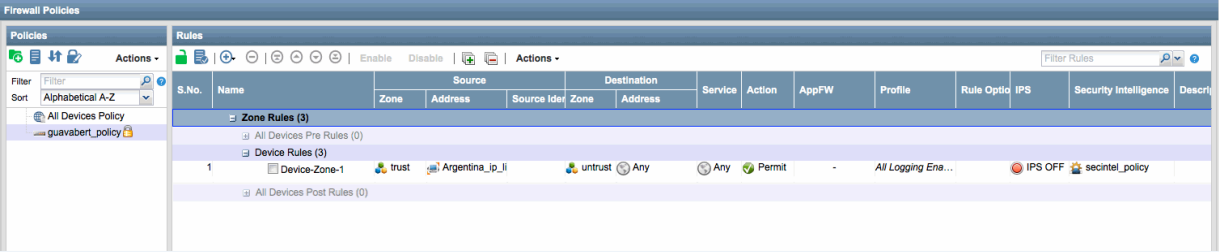
4. Click **Create**.
5. Click the plus (+) icon to add a device pre-rule.
6. Click in the Source Address column and move **Argentina\_ip\_list** to the Selected column. See [Figure 87 on page 116](#).

Figure 87: Configuring the Allow Argentina IP Addresses Firewall Rule



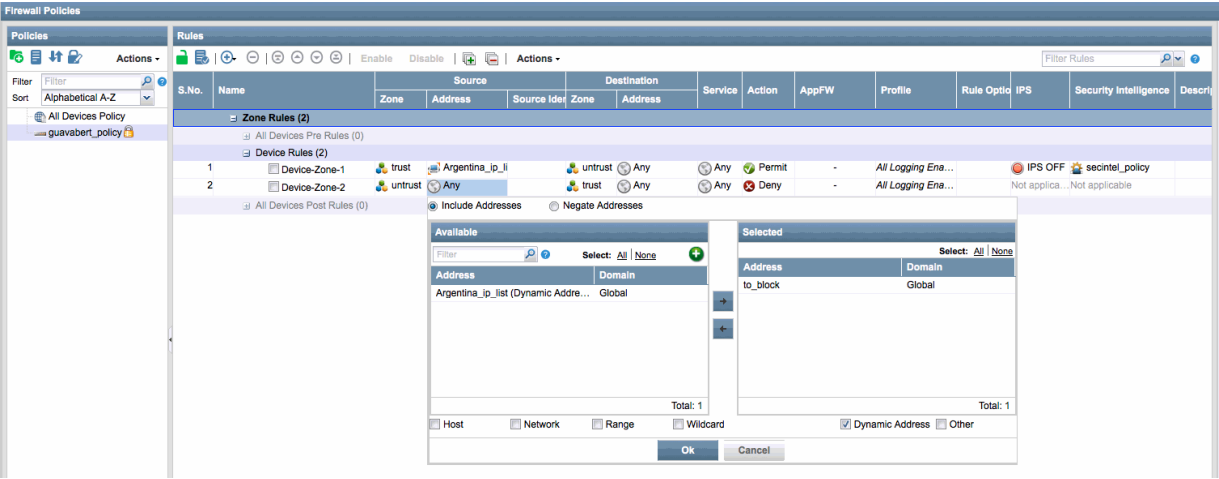
- 7. Click **OK**.
- 8. Click in the Action column and select **Permit**. Then click in the Security Intelligence column and select **secintel\_policy**. See [Figure 88 on page 116](#).

Figure 88: Configuring the Spotlight Secure Firewall Rule



- 9. Click the plus (+) icon to add another device pre-rule.
- 10. Click in the Source Address column and move **to\_block** to the Selected table. See [Figure 89 on page 117](#).

Figure 89: Configuring the Blocklist Firewall Rule



11. Click **OK**.

12. View the job details to see the firewall policies added to the SRX Series device.

Job Details: 262171

User:	super	Actual start time:	Jun 25, 2014 11:24:22 AM PDT
Job ID:	262171	Scheduled start time:	Jun 25, 2014 11:24:22 AM PDT
Job type:	Update Devices	Percentage completion:	100
Job status:	SUCCESS	End time:	Jun 25, 2014 11:24:33 AM PDT

guavabert

```

##Security Firewall Policy : trust - untrust##
delete security policies from-zone trust to-zone untrust policy Device-Zone-1 match source-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-1 match source-address Argentina_ip_list
set security policies from-zone trust to-zone untrust policy Device-Zone-1 then permit application-services security-
intelligence-policy secintel_policy
##Security Firewall Policy : untrust - trust##
set security policies from-zone untrust to-zone trust policy Device-Zone-2 match application any
set security policies from-zone untrust to-zone trust policy Device-Zone-2 match destination-address any
set security policies from-zone untrust to-zone trust policy Device-Zone-2 match source-address to_block
set security policies from-zone untrust to-zone trust policy Device-Zone-2 then log session-close
set security policies from-zone untrust to-zone trust policy Device-Zone-2 then log session-init
set security policies from-zone untrust to-zone trust policy Device-Zone-2 then deny
set security policies from-zone untrust to-zone trust policy Device-Zone-3 match application any
set security policies from-zone untrust to-zone trust policy Device-Zone-3 match destination-address any
set security policies from-zone untrust to-zone trust policy Device-Zone-3 match source-address any
set security policies from-zone untrust to-zone trust policy Device-Zone-3 then log session-close
set security policies from-zone untrust to-zone trust policy Device-Zone-3 then log session-init
set security policies from-zone untrust to-zone trust policy Device-Zone-3 then permit
##Dynamic Address Configurations##
set security dynamic-address address-name Argentina_ip_list description "GeoIP list of Argentina"
set security dynamic-address address-name Argentina_ip_list profile category GeoIP property Country string AR
set security dynamic-address address-name to_block description "Blacklist ips"
set security dynamic-address address-name to_block profile category IPFilter feed feed_source blacklist

```

Back
Close

## RELATED DOCUMENTATION

[Spotlight Secure Connector Information Source Overview | 54](#)

[Spotlight Secure Connector Profile Overview | 71](#)

[Spotlight Secure Connector Policy Overview | 81](#)