

Security Director

FIPS Evaluated Configuration Guide for Security Director

Published
2021-02-18

Release
19.1R1

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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

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

Security Director FIPS Evaluated Configuration Guide for Security Director
19.1R1

Copyright © 2021 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

Understanding Security Director in FIPS Mode | 12

About the Cryptographic Boundary on Security Director | 12

How FIPS Mode Differs from Non-FIPS Mode | 13

Validated Version of Security Director in FIPS Mode | 13

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 13

FIPS Terminology | 14

Supported Cryptographic Algorithms | 14

Weak Digital Certificates | 16

Understanding the Security Director User Interface | 17

Benefits of Junos Space Security Director | 18

Access and Log in | 18

Using Navigational Elements | 19

Banner Overview | 19

About Page | 20

Junos Space Platform Link | 20

Search Utility | 21

Domain Switcher | 21

Notification Center | 21

User Functions Menu | 22

Help Button | 22

Search Overview | 22

| | |
|------------------------------|----|
| Search Patterns | 22 |
| Search Categories | 24 |
| Global Search | 24 |
| ILP Search | 25 |
| Column Search | 25 |
| Item Selector Search | 27 |
| Delimiter Search Limitations | 28 |
| Refresh Search Index | 29 |
| Main Workspace Overview | 30 |
| Dashboard | 30 |
| Monitor | 31 |
| Devices | 32 |
| Configure | 32 |
| Reports | 33 |
| Administration | 34 |
| Global Features | 34 |
| Conclusion | 35 |

| | |
|---|----|
| Setting Up a JA2500 Appliance for Security Director | 36 |
|---|----|

| | |
|--|----|
| Setting Up a Junos Space Virtual Appliance for Security Director | 37 |
|--|----|

2

Understanding Roles and Authentication Methods

| | |
|--|----|
| Understanding Roles in Security Director | 39 |
|--|----|

| | |
|--|----|
| Understanding Password Specifications and Guidelines for Security Director in Junos Space in FIPS Mode | 40 |
|--|----|

3

Deploying Security Director

| | |
|------------------------------|----|
| Installing Security Director | 43 |
|------------------------------|----|

| | |
|---|----|
| Uploading the Junos Space Application | 44 |
| Installing the Uploaded Junos Space Application | 45 |
| Installing and Upgrading Security Director from the Junos Space Store | 47 |

| | |
|----------------------|----|
| Installing Hot Patch | 53 |
|----------------------|----|

Working in Build Mode

Overview of Device Discovery in Security Director | 55

About the Documentation

IN THIS SECTION

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

Use this guide to operate Security Director in Federal Information Processing Standards (FIPS) 140-2 Level 1 environment. FIPS 140-2 defines security levels for hardware and software that perform cryptographic functions.

Documentation and Release Notes

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

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

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

Documentation Conventions

Table 1 on page 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 |
|------------------------------|---|--|
| Bold text like this | Represents text that you type. | To enter configuration mode, type the configure command: user@host> configure |
| Fixed-width text like this | Represents output that appears on the terminal screen. | user@host> show chassis alarms No alarms currently active |
| <i>Italic text like this</i> | <ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. | <ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i> |

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@# set system domain-name <i>domain-name</i> |
| Text like this | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | <ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE. |
| < > (angle brackets) | Encloses optional keywords or variables. | stub <default-metric <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. | broadcast multicast (<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. | rsvp { # Required for dynamic MPLS only |
| [] (square brackets) | Encloses a variable for which you can substitute one or more values. | community name members [<i>community-ids</i>] |
| 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

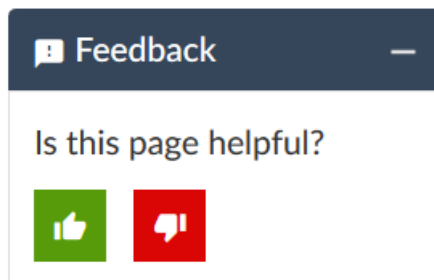
Table 2: Text and Syntax Conventions (*continued*)

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

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. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

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

Self-Help Online Tools and Resources

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

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

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

Creating a Service Request with JTAC

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

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

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

1

CHAPTER

Overview

Understanding Security Director in FIPS Mode | **12**

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | **13**

Understanding the Security Director User Interface | **17**

Setting Up a JA2500 Appliance for Security Director | **36**

Setting Up a Junos Space Virtual Appliance for Security Director | **37**

Understanding Security Director in FIPS Mode

IN THIS SECTION

- [About the Cryptographic Boundary on Security Director | 12](#)
- [How FIPS Mode Differs from Non-FIPS Mode | 13](#)
- [Validated Version of Security Director in FIPS Mode | 13](#)

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, Security Director complies with the FIPS 140-2 Level 1 standard.

Operating Security Director in a FIPS 140-2 Level 1 environment requires enabling FIPS mode in Junos Space. If FIPS mode is enabled in Junos Space, then Security Director automatically supports FIPS mode.

For regulatory compliance information about FIPS for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

About the Cryptographic Boundary on Security Director

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a device. Junos Space in FIPS mode prevents the cryptographic module from executing any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module by, for example, being displayed on a console or written to an external log file.

Cryptographic boundary is determined by different configurations. For example, you can configure Junos Space with Security Director or Junos Space with Security Director and Network Director.

How FIPS Mode Differs from Non-FIPS Mode

Unlike Junos Space in non-FIPS mode, Junos Space in FIPS mode is a *non-modifiable operational environment*. In addition, Junos Space in FIPS mode differs in the following ways from Junos Space in non-FIPS mode:

- Self-tests of all cryptographic algorithms are performed at Junos Space startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and Message Digest 5 (MD5) are disabled.
- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Administrator passwords must be at least 10 characters.

Validated Version of Security Director in FIPS Mode

To determine whether a Junos OS Evolved release is FIPS 140-2 1 or FIPS 140-3 1 certified, see the compliance page on the Juniper Networks Web site (<https://apps.juniper.net/compliance/fips.html>).

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- [FIPS Terminology | 14](#)
- [Supported Cryptographic Algorithms | 14](#)
- [Weak Digital Certificates | 16](#)

Use the definitions of FIPS terms and supported algorithms to help you understand Security Director in FIPS mode.

Security Director uses the user administration features of the Junos Space platform on which it runs. Use Junos Space for tasks such as adding, deleting, and editing user accounts and roles, and changing user passwords. Refer to the Junos Space documentation for information about user administration.

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects.

Cryptographic module—The set of software that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Super Administrator—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos Space in FIPS mode. For details, see *Understanding Roles and Services for Junos Space in FIPS Mode*.

FIPS—Federal Information Processing Standards. FIPS 140-2 specifies requirements for security and cryptographic modules. Junos Space in FIPS mode complies with FIPS 140-2 Level 1.

SSH—A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for **rlogin**, **rsh**, and **rcp** in a UNIX environment. To secure the information sent over administrative connections, use SSHv2 for CLI configuration. In Junos Space, SSHv2 is enabled by default, and SSHv1, which is not considered secure, is disabled.

Supported Cryptographic Algorithms

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests. Any self-test failure results in a FIPS error state.

BEST PRACTICE: For FIPS 140-2 compliance, use only FIPS-approved cryptographic algorithms in FIPS mode.

The following cryptographic algorithms are supported in FIPS mode. Symmetric methods use the same key for encryption and decryption, while asymmetric methods use different keys for encryption and decryption.

AES—The Advanced Encryption Standard (AES), defined in FIPS PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits.

Diffie-Hellman—A method of key exchange across a nonsecure environment (such as the Internet). The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key independently and send part of that key to the other. Each side then calculates a common key value. This is a symmetrical method—keys are typically used only for a short time, discarded, and regenerated.

ECDH—Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman key exchange algorithm that uses cryptography based on the algebraic structure of elliptic curves over finite fields. ECDH allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret can be used either as a key or to derive another key for encrypting subsequent communications using a symmetric key cipher.

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA uses the P-256, P-384, and P-521 curves that can be configured under OpenSSH.

HMAC—Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos Space in FIPS mode, HMAC uses the iterated cryptographic hash functions SHA-1, SHA-256, and SHA-512 along with a secret key.

SHA-256, SHA-384, and SHA-512—Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest, SHA-384 produces a 384-bit hash digest, and SHA-512 produces a 512-bit hash digest.

3DES (3des-cbc)—Encryption standard based on the original Data Encryption Standard (DES) from the 1970s that used a 56-bit key and was cracked in 1997. The more secure 3DES is DES enhanced with three multiple stages and effective key lengths of about 112 bits. For Junos Space in FIPS mode, 3DES is implemented with cipher block chaining (CBC).

The following [Table 3 on page 15](#) indicates supported algorithms for Security Director in Junos Space:

Table 3: Supported Algorithms for Security Director in Junos Space

| Protocol | Key Exchange | Authentication | Encryption | MAC | Cipher |
|----------|--------------|----------------|-------------|--------|---------------------------|
| TLSv1.2 | DH | RSA | AESGCM(128) | AEAD | DHE-RSA-AES128-GCM-SHA256 |
| TLSv1.2 | DH | RSA | AES(128) | SHA256 | DHE-RSA-AES128-SHA256 |
| TLSv1.2 | DH | RSA | AESGCM(256) | AEAD | DHE-RSA-AES256-GCM-SHA384 |

Table 3: Supported Algorithms for Security Director in Junos Space (*continued*)

| Protocol | Key Exchange | Authentication | Encryption | MAC | Cipher |
|----------|--------------|----------------|-------------|--------|-----------------------------|
| TLSv1.2 | DH | RSA | AES(256) | SHA256 | DHE-RSA-AES256-SHA256 |
| TLSv1.2 | ECDH | RSA | AESGCM(128) | AEAD | ECDHE-RSA-AES128-GCM-SHA256 |
| TLSv1.2 | ECDH | RSA | AES(128) | SHA256 | ECDHE-RSA-AES128-SHA256 |
| TLSv1.2 | ECDH | RSA | AESGCM(256) | AEAD | ECDHE-RSA-AES256-GCM-SHA384 |
| TLSv1.2 | ECDH | RSA | AES(256) | SHA384 | ECDHE-RSA-AES256-SHA384 |

Security Director in Junos Space supports the following third party cryptographic modules, which are FIPS compliance:

- Linux Kernel Crypto
- OpenSSL
- GnuTLS
- Libgcrypt
- Network Security Services
- JDK JCE
- Bouncy Castle

Weak Digital Certificates

Enable the following services only with HTTPS TLSv1.2 configured with SHA256 RSA 2048 signature:

- Log Collector
- Policy Enforcer
- Sky ATP

Understanding the Security Director User Interface

Security Director is a Junos Space management application designed to enable quick, consistent, and accurate creation, maintenance, and application of network security policies. The new GUI provides more isolation from the underlying Junos Space Platform (or Space), allowing security architects, analysts, and operators to focus on security.

Security Director now presents the security-focused administrator with a tabbed interface. The tabs across the top of the GUI provide workspaces in which an administrator can perform specific tasks.

[Table 4 on page 17](#) shows the names of the tabs along with brief descriptions of what is accessible in that workspace.

Table 4: Tabs and What Their Workspaces Access

| Tab Name | Accesses |
|----------------|--|
| Dashboard | Graphical security widgets that can be added, removed, and rearranged on a per user basis. These widgets offer each user a customized view of network security. |
| Monitor | Live threat maps, job management, and visual analysis of: <ul style="list-style-type: none"> • Events received • User activity • Alerts and alarms |
| Devices | Device discovery and device management. |
| Configure | Security-related policy management including: <ul style="list-style-type: none"> • Firewall policies • IPS policies • NAT policies • UTM policies • VPN creation and management • Shared object management |
| Reports | Predefined security reports and the ability to create custom reports. |
| Administration | User and role management, logging management, and infrastructure management. |

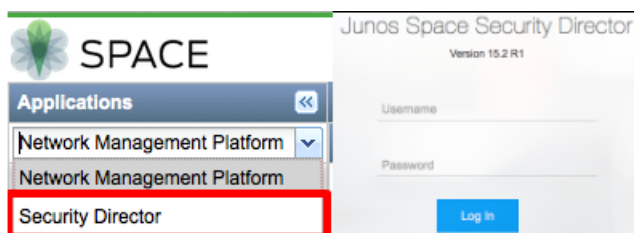
Benefits of Junos Space Security Director

- Provides greater visibility, simplified management, and actionable security intelligence on applications, users, IP addresses, and threats that help network managers make better security decisions.
- Scalable and automated solution with a single centralized management interface provides actionable intelligence to reduce business risk.
- Action-oriented design enables the network administrator to detect risky applications and threats across the network as they occur and apply immediate remedial action with a single click.
- Reduces risk of compromise and human error by allowing network administrators to focus on maximizing the security and accelerating operations with a simple and concise rule set.
- Offers the best search speed in the industry when correlating petabyte of data across hundreds of nodes.
- Enables effective threat management while producing detailed data access and user activity reports.
- Remote mobile monitoring capabilities provide visibility and enhanced flexibility.
- Simple user interface allows new users to quickly become proficient.

Access and Log in

If you are working in the Space Platform, you can access Security Director by selecting Security Director from the Applications drop-down list at the upper left corner of the Space GUI, as shown on the left side of [Figure 1 on page 18](#).

Figure 1: Security Director Access and Log in



After you log out of the Security Director GUI (or the login timer expires while in Security Director), the next time you log in the Security Director login screen will appear, as shown on the right side of [Figure 1 on page 18](#). Once you use the Security Director login screen, that will remain your default login location unless and until you navigate to the Space Platform URL or return to the Space Platform GUI and either log out from there or let the login timer expire.






When the Security Director application is accessed for the first time, a getting started guide will overlay the Security Director Dashboard page. The guide is designed to assist new and longtime users by providing

a quick reference to where functions are located within the new GUI. The guide can be dismissed for subsequent logins and accessed later through the help button on the right side of the banner.

Using Navigational Elements

For a more personal, helpful, and customizable user experience, Juniper Networks has provided some aids within the GUI. Table 2 shows a sample of navigation, customization, and help icons.

Table 5: Navigational Elements

| Element | Icon | Location |
|---|---|---|
| Breadcrumbs—Trace your location in the GUI. The breadcrumbs provide a path back to one of the six starting tabs: Dashboard, Monitor, Devices, Configure, Reports, and Administration. |  | Upper left part of main screen below the Monitor tab. Not visible on the Dashboard. |
| Info Tips—Hover your mouse over any available question mark icon for quick pop-up guidance. |  | Various places around the GUI. |
| Show and Hide Left-Nav—Click the hamburger icon to show or hide the left-nav section. |  | Left side of tab bar, below the Juniper Networks logo. |
| Show Hide Columns—In tabular displays, you can choose which columns are visible by clicking the icon and then selecting the check boxes on the menu. |  | Upper right corner of some tabular display windows such as the Reports tab and Devices tab. |
| Table Search—You can click this magnifying glass icon, within large tabular views, to search for specific text within any of the visible fields in the display. |  | Upper right corner of tabular views. Next to the Show Hide Columns icon. |

Banner Overview

The dark gray bar at the top of the screen is called the Banner. It provides access to system-wide utilities such as a link back to Junos Space Platform, a global search utility, a domain switcher, a notification center, a profile management access menu, and a help button.

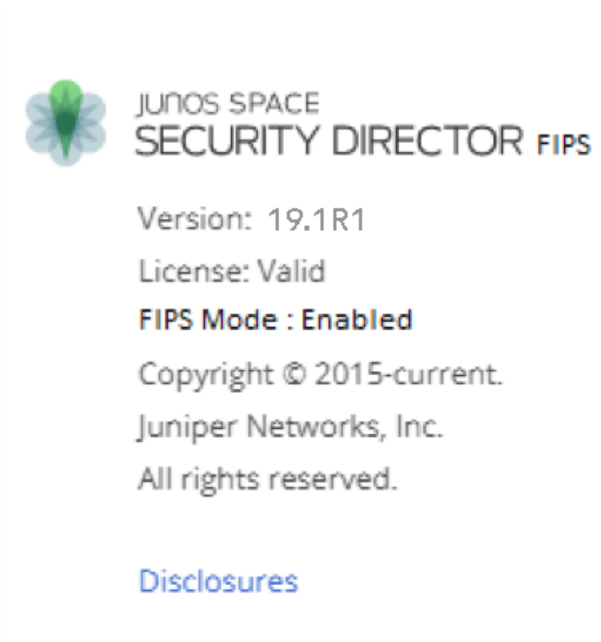
Figure 2: Banner



About Page

Figure 3 on page 20 displays information about Security Director, such as current version and FIPS mode. To view the about page, click **Help** button and select **About Page**.

Figure 3: About Page



Junos Space Platform Link

Figure 4: Junos Space Platform Link



The GUI for Security Director is designed to enhance security focus. Therefore, for administration or other tasks that are not security related, you will need a way to switch back to the Space Platform GUI. In Security Director, this can be accomplished by simply clicking the Juniper Networks logo in the upper left corner of the banner.

Search Utility

Figure 5: Search Utility



Sometimes you just need to search for things. Did I already create an address object for the corporate management network? Is there a URL category for gambling? If you find yourself in need of search capabilities, the Global Search Utility will fulfill your needs. Type a term into the search field and Security Director will show you all of the places where that term is found. The results lists are clickable, so that you can go directly to the found object simply by clicking.

Domain Switcher

Figure 6: Domain Switcher



Security Director supports multitenancy in the form of domains. Domains provide a customizable separation of managed assets and their configuration elements. See Domains Overview for more information.

Notification Center

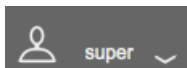
Figure 7: Notification Center



On the right side of the banner is a bell-shaped icon called the Notification Center. Clicking this icon reveals lists of the top alerts and alarms in Security Director. Clicking the View All Alarms or View All Alerts links at the bottom of the drop-down menu takes you to the detail page for the respective topic.

User Functions Menu

Figure 8: User Functions Menu



To the right of the Notification Center, there is a head-and-shoulders icon and a field showing the logged in user. Clicking your user name will allow you to access your user profile or log out of Security Director.

Help Button

Figure 9: Help Button



Access to the online Help system and the Getting Started Guide are available by clicking the right-most icon on the banner, shaped like a question mark. The help system includes access to a list of supported web browsers, user interface assistance, as well as links to technical support and full Security Director documentation.

Search Overview

You can search objects and devices from various tabs using a partial or full name, IP address, or other values. There are different categories of search in Security Director and supported patterns are regular expressions, partial word search, special character search, and so on.

Search Patterns

You can use the following regular expressions to search the objects.

- * (multiple character search)—If you do not know the full name of an object, use * at the start or end of the name.

For example, when you search with test* in addresses, ILP displays the following results as shown in [Figure 10 on page 23](#).

- test-2-SRX

- test_1-SRX

Figure 10: Multiple Character Search

Configure / Shared Objects / Addresses

Addresses ⓘ

More ▾ | + ✎ ✕ | 🔍 ⚙ ⋮

test* × Clear All

| <input type="checkbox"/> | ▲ Name | Type | Hostname | IP Address | Description | Domain |
|--------------------------|------------|------|----------|------------|-------------|--------|
| <input type="checkbox"/> | test-2-SRX | Host | | 1.1.1.1 | | Global |
| <input type="checkbox"/> | test_1-SRX | Host | | 3.3.3.3 | | Global |

2 items

- ? (single character search)—You can replace a single character with ? in search text.
For example, when you search with test?org?net in addresses, ILP displays test.org.net result as shown in [Figure 11 on page 23](#).

Figure 11: Single Character Search

Addresses ⓘ

More ▾ | + ✎ ✕ | 🔍 ⚙ ⋮

test?org?net × Clear All

| <input type="checkbox"/> | ▲ Name | Type | Hostname | IP Address | Description | Domain |
|--------------------------|--------------|------|----------|------------|-------------|--------|
| <input type="checkbox"/> | test.org.net | Host | | 3.3.3.3 | | Global |

1 items

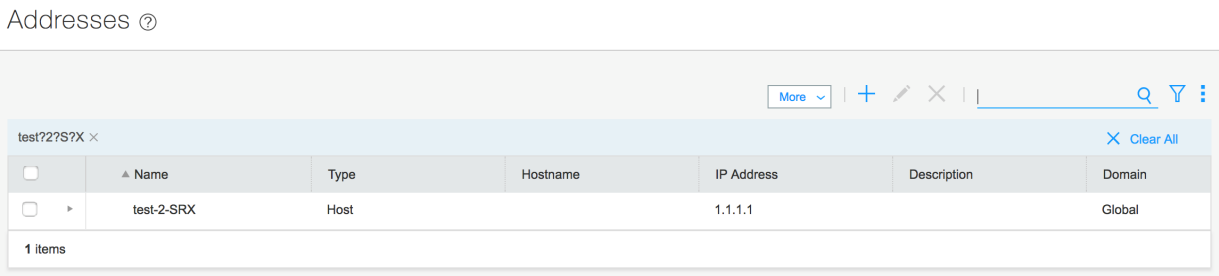
Search limitations

- A partial name search with a single character replacement does not work. If the search text is split by any special character such as - , _ , / , :, . , and ; and if you try to search with a partial name , results will not be displayed.

For example, if address object name is test-2-SRX, and you try to search test?2, then results will not be displayed.

However, you can do a full text search including as many ? in between the name like this: test?2?S?X. See [Figure 12 on page 24](#).

Figure 12: Partial Name Search with Single Character Replacement



Search Categories

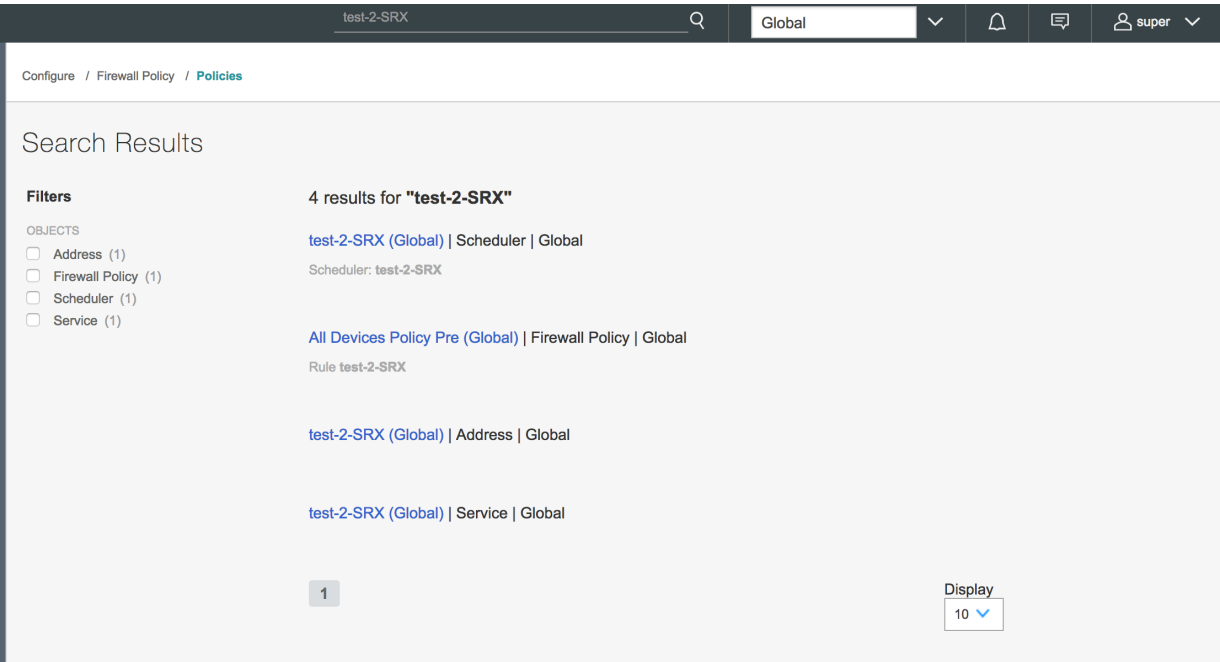
Global Search

Using global search, users can search any Security Director object including SRX Series devices with a name or an IP address. Global search checks the search text or IP address across all objects or devices of Security Director and displays the results in the user interface.

For example, if you create a firewall rule, scheduler, address, and service with same name in Security Director and search that name using the global search text box, the results are displayed with domains.

Global search results are displayed in the format Name of the Object | Type of the Object | Domain Name. See [Figure 13 on page 25](#).

Figure 13: Global Search

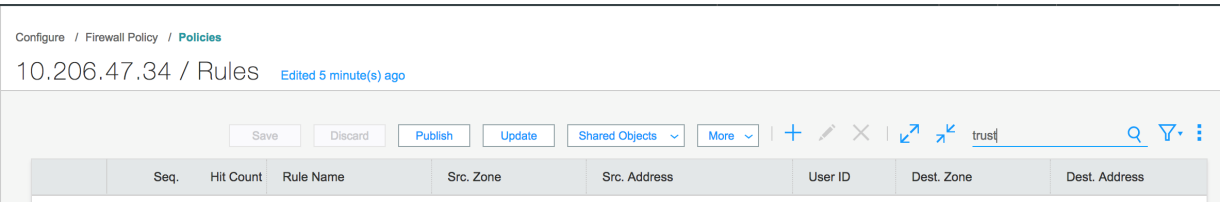


ILP Search

All objects and devices pages such as, address, service, firewall policy, firewall rule, and so on have search boxes at the right corner (ILP search box). You can search using a name, a device IP address, and so on.

For example, in a firewall rules table, you can search the rule by using a name, a zone, an address, a scheduler name, and so on as shown in [Figure 14 on page 25](#).

Figure 14: ILP Search

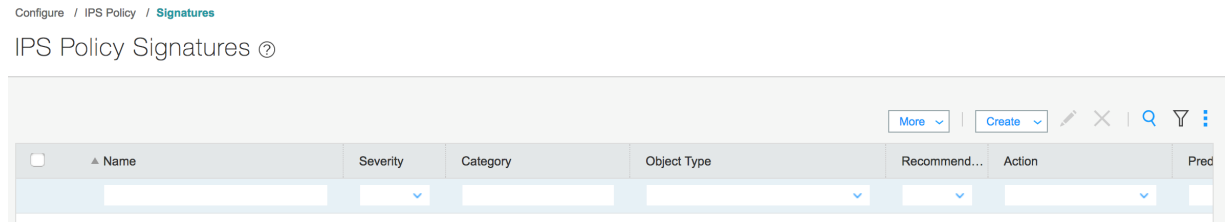


Column Search

You can perform a granular level of search using column level search in the complex tables, which has more data, such as firewall, NAT, IPS, VPN policies, rules table, and devices table.

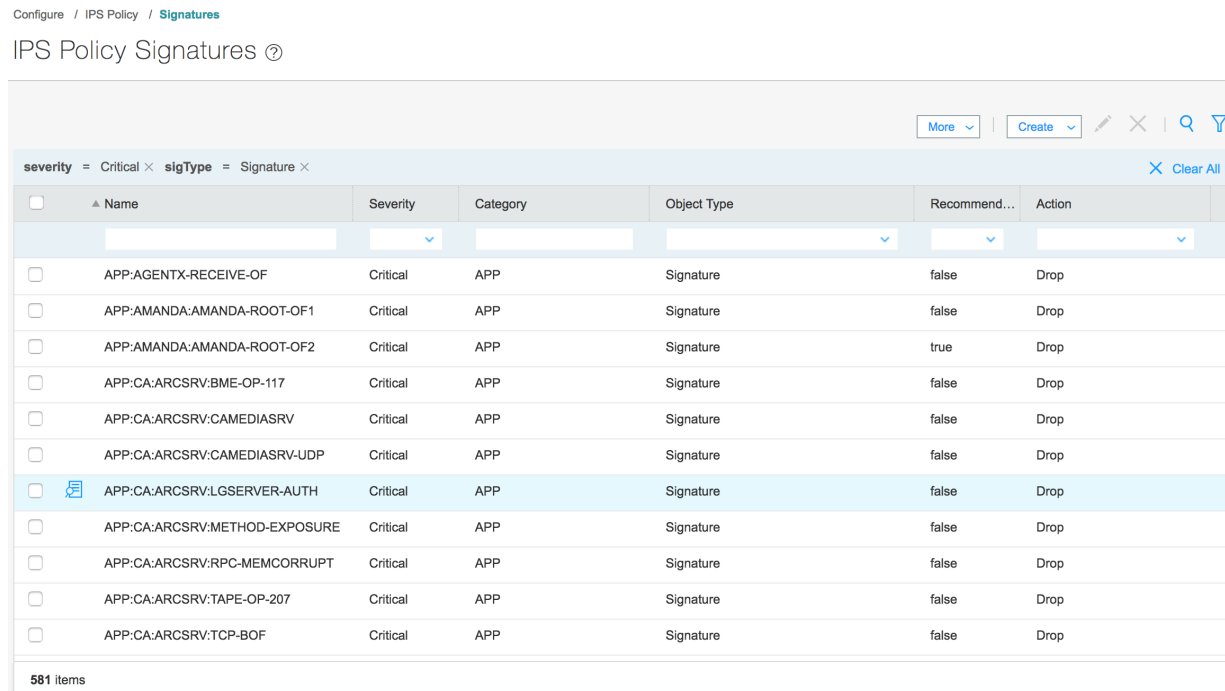
If you click the column search icon placed at the right corner of the table, near the search icon, the column search text box is displayed in the user interface. You can filter records using one or more columns. See [Figure 15 on page 26](#).

Figure 15: Column Search



For example, using the Severity and Object Type columns for IPS signature, obtain your results. See [Figure 16 on page 26](#).

Figure 16: Column Search-Example1



For example, if you want to search with an IP address, the corresponding subnet address and address group will also be listed in the search result. If the IP address of one of the address objects is 2.2.2.2 and it is part of the 2.2.2.0/24 subnet address object and ADDR-G1 is the address group, then both IP address and subnet address are displayed in the result. See [Figure 17 on page 27](#).

Figure 17: Column Search-Example 2

Configure / Shared Objects / Addresses

Addresses

More
+
-
2.2.2.2

| | Name | Type | Hostname | IP Address | Description | Domain |
|--------------------------|---------|---------|----------|------------|-------------|--------|
| <input type="checkbox"/> | ADDR-G1 | Group | | | | Global |
| <input type="checkbox"/> | NET-1 | Network | | 2.2.2.0/24 | | Global |
| <input type="checkbox"/> | test1 | Host | | 2.2.2.2 | | Global |

3 items

2.2.2.2
Clear All

| | Name | Type | Hostname | IP Address | Description | Domain |
|--------------------------|---------|---------|----------|------------|-------------|--------|
| <input type="checkbox"/> | ADDR-G1 | Group | | | | Global |
| <input type="checkbox"/> | NET-1 | Network | | 2.2.2.0/24 | | Global |
| <input type="checkbox"/> | test1 | Host | | 2.2.2.2 | | Global |

3 items

For example, in the Security Devices page, you can filter the devices using the Pending Services column as shown in [Figure 18 on page 27](#). You can filter and push the configuration from Security Director to a specific SRX Series device using the Update operation.

Figure 18: Column Search-Example 3

Devices / Security Devices

Security Devices

Update Changes
Resynchronize with Network
Upload Keys
More
Search
Filter

pending-services = 10.206.47.34
Clear All

| Serial Number | Fab Link Status | Control Link Status | Assigned Services | Pending Services | Installed Services | Domain | Last Rebooted Time | C |
|---------------|-----------------|---------------------|-------------------|------------------|--------------------|--------|---------------------------|---|
| 7b484429050 | N/A | N/A | 10.206.47.34 | 10.206.47.... | N/A | Global | Mon Aug 07 2017 05:23:... | J |

Items
1 of 1
Display 50

Item Selector Search

You can use a search text box to select items for inclusion in a rule or policy.

For example, when creating an address or service group, you can first search for the address or service object. Similarly, in firewall, IPS, and NAT rule creation, source and destination addresses can be searched in the item selector using a regular expression, a full name, and a partial name. See [Figure 19 on page 28](#).

Figure 19: Item Selector Search

Create Address ?

Object Type ?

☐ Address

☒ Address Group

Name * ?

test

Description ?

Addresses ?

Available2 items

test

| <input type="checkbox"/> | Name | Domain |
|--------------------------|-----------------|--------|
| <input type="checkbox"/> | test2 (3.3.3.3) | Global |
| <input type="checkbox"/> | test3 (4.4.4.4) | Global |

Selected0 items

| <input type="checkbox"/> | Name | Domain |
|--------------------------|------|--------|
|--------------------------|------|--------|

>

<

Cancel

OK

Delimiter Search Limitations

The search text should not contain a delimiter that marks the beginning or end, such as a comma, hyphen, and so on. You can search the object by partial word or with * at the end of the text.

For example, if object names are test-SRX, test-SRX-UK, test-SRX_US, and so on, then you cannot search with test-, results will not be displayed as shown in [Figure 20 on page 29](#).

Figure 20: Search with Delimiter

Configure / Shared Objects / Addresses

Addresses ?



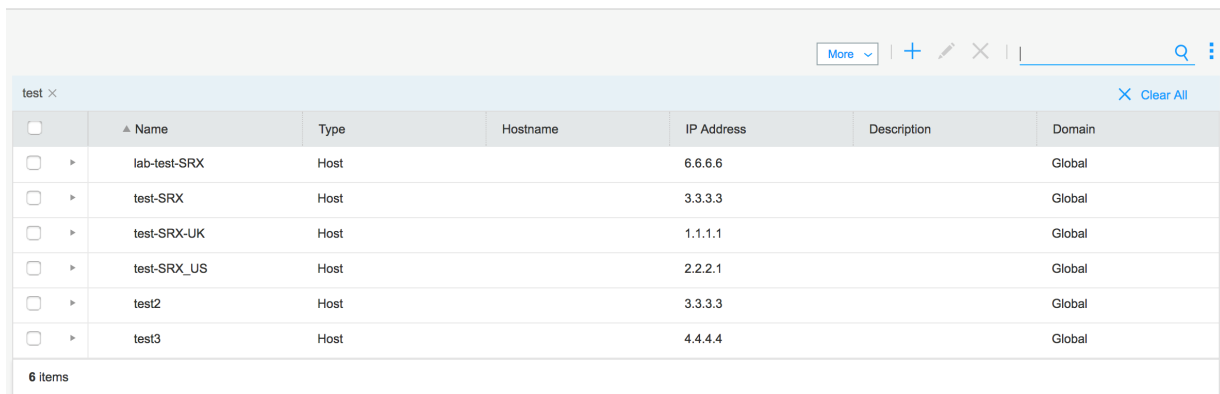
| | Name | Type | Hostname | IP Address | Description | Domain |
|-------------------|------|------|----------|------------|-------------|--------|
| No data available | | | | | | |

However, if you search with the text test, then the object that contains the name as test (either before or after a delimiter) is displayed in the user interface as shown in [Figure 21 on page 29](#).

Figure 21: Search Without Delimiter

Configure / Shared Objects / Addresses

Addresses ?



| | Name | Type | Hostname | IP Address | Description | Domain |
|--------------------------|--------------|------|----------|------------|-------------|--------|
| <input type="checkbox"/> | lab-test-SRX | Host | | 6.6.6.6 | | Global |
| <input type="checkbox"/> | test-SRX | Host | | 3.3.3.3 | | Global |
| <input type="checkbox"/> | test-SRX-UK | Host | | 1.1.1.1 | | Global |
| <input type="checkbox"/> | test-SRX_US | Host | | 2.2.2.1 | | Global |
| <input type="checkbox"/> | test2 | Host | | 3.3.3.3 | | Global |
| <input type="checkbox"/> | test3 | Host | | 4.4.4.4 | | Global |

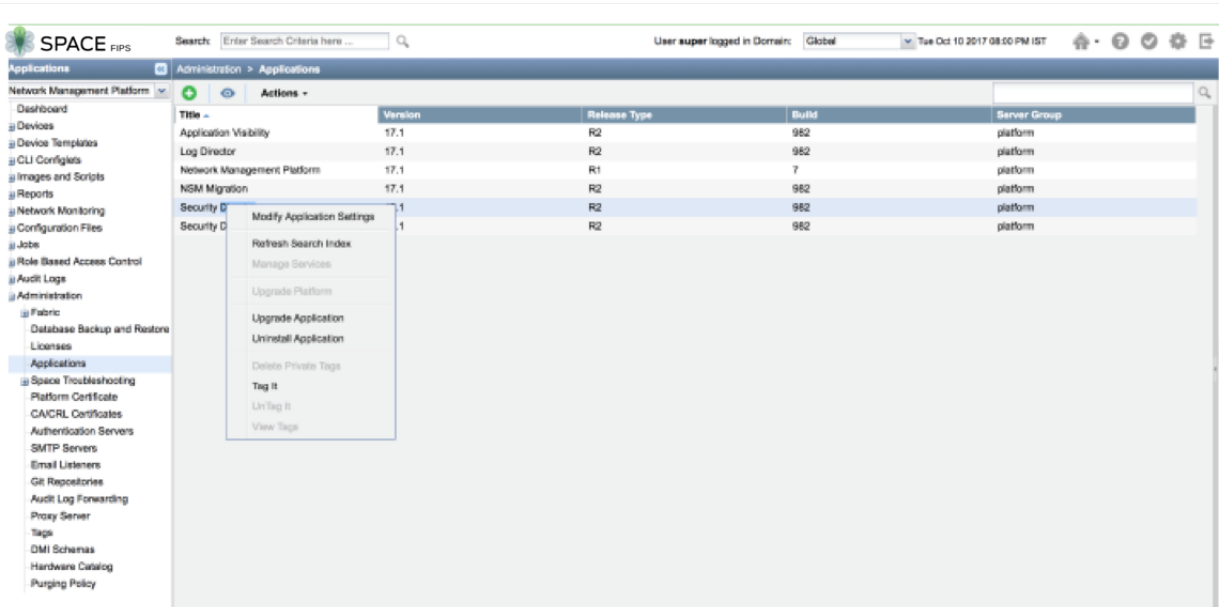
6 items

Refresh Search Index

If you have any issues while searching for newly added or existing object in any category, such as global, ILP, and column search, then you can trigger the refresh search index from the Junos Space Network Management Platform page. Based on the number of objects, such as the number of address, service, and firewall policies in Security Director, the refresh search index might take more or less time.

In Junos Space Network Management Platform page, select **Administrator > Application**. Right-click Security Director and click **Refresh Search Index**. See [Figure 22 on page 30](#).

Figure 22: Refresh Search Index



Wait for about 10-15 minutes, and then try to search objects again in Security Director.

NOTE: This operation should not be performed frequently. This can harm the overall Security Director performance.

Main Workspace Overview

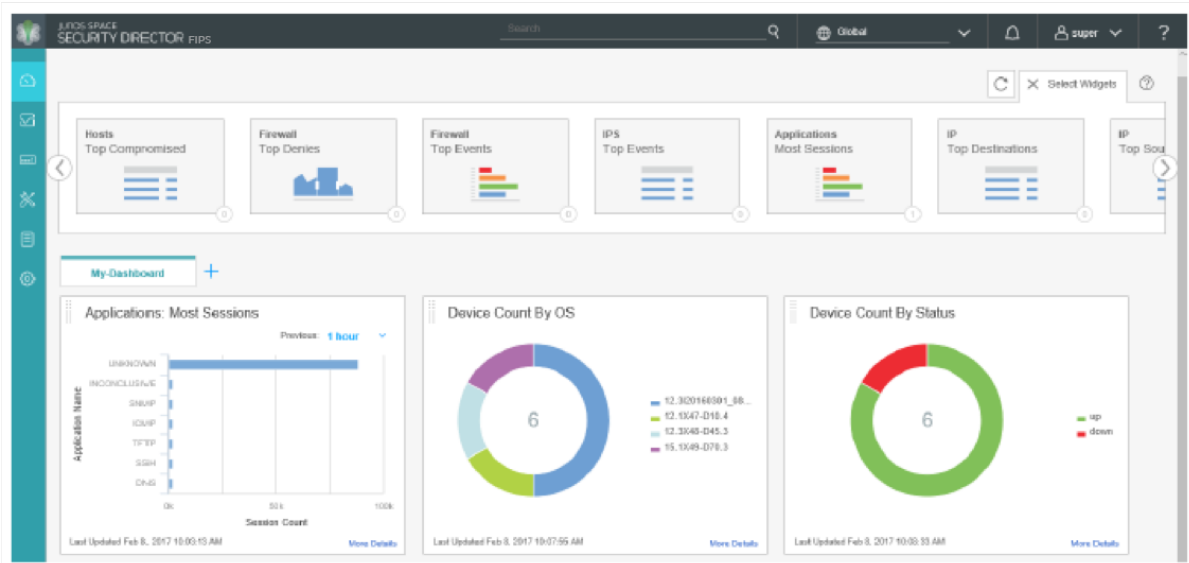
The main workspace of Security Director takes up the remainder of the browser window and is divided by six horizontal tabs just below the Banner. As shown in Table 1, the six tabs are: Dashboard, Monitor, Devices, Configure, Reports, and Administration. Each workspace and its accessible functions are described later in this document.

Dashboard

The Dashboard is the main landing page for Security Director. It is the first thing you will see each time you log in. Therefore, Juniper Networks has provided a means for you to be presented with the network security information that you are most interested in. You can customize the workspace in your Dashboard by adding widgets from the carousel below the banner. The placement of, and settings within, widgets are saved so that anything from device information to firewall event information or from top blocked viruses

to live threat maps can be unique for each user. Once you decide on the widgets that you want to see, you can close the carousel to regain some screen space.

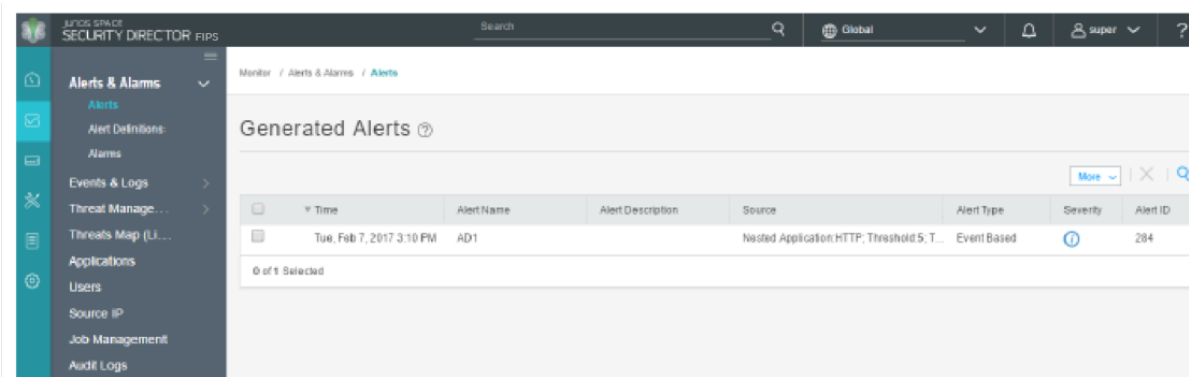
Figure 23: Security Director Dashboard Tab



Monitor

The Monitor tab provides a workspace in which graphical representations of network traffic, firewall events, live threats, and network user data are available. There is also detailed data for alerts and alarms and job management information. In this workspace, you can review the detailed information needed to understand what is happening to the managed security devices and traffic in your network.

Figure 24: Security Director Monitor Tab



Devices

The Devices tab provides a workspace in which you can add and manage Security Director devices. There are several columns of information available by default. This includes live CPU and memory data, and running software version and platform information. Schema mismatches are easily visible so that you can correct them before updating a device.

NOTE: Before working with a particular device in Security Director, ensure that the proper DMI Schema is available. If there is a mismatch between the device's software image and the schema version that Security Director is using to manage the device, unexpected behavior will result. DMI Schema management is performed in the Junos Space Platform Administration workspace.

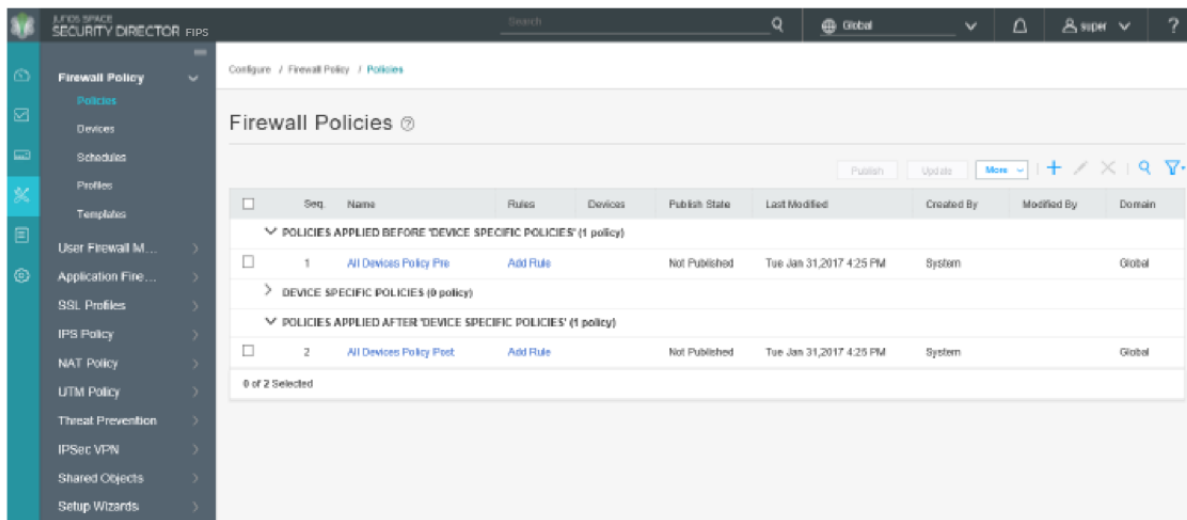
Figure 25: Security Director Devices Tab

| Device Name | IP Address | OS Version | Schema Version | CPU | Storage | Authentication Status |
|--------------------------------|---------------|--------------------------|-------------------------------|-----|---------|-----------------------|
| DC-SRX1400-1 0 LSYs(s) | 10.206.32.245 | 12.3X48-D45.3 | 12.1X46-D35.1 (Mismatch w...) | ... | ... | Credentials Based |
| vsm-75 | 10.207.99.75 | 15.1X48-D70.3 | 15.1X48-D70.3 | ... | ... | Credentials Based |
| vSRX-int | 10.207.98.218 | 12.1X47-D10.4 | 12.1X46-D35.1 (Mismatch w...) | ... | ... | Credentials Based |
| LONGEVITY_1 2 LSYs(s) | 10.206.34.198 | 12.3(20160301_0803_ichen | 12.1X46-D35.1 (Mismatch w...) | ... | ... | Credentials Based |
| interconnected-logical-syst... | 10.206.34.198 | 12.3(20160301_0803_ichen | 12.1X46-D35.1 (Mismatch w...) | ... | ... | NA |
| Is-CityanLogicalSystem ... | 10.206.34.198 | 12.3(20160301_0803_ichen | 12.1X46-D35.1 (Mismatch w...) | ... | ... | NA |

Configure

The Configure tab is the workspace where all of the security configuration happens. You can configure firewall, IPS, NAT, and UTM policies, assign policies to devices, create and apply policy schedules, create and manage VPNs, and create and manage all of the shared objects needed for managing your network security.

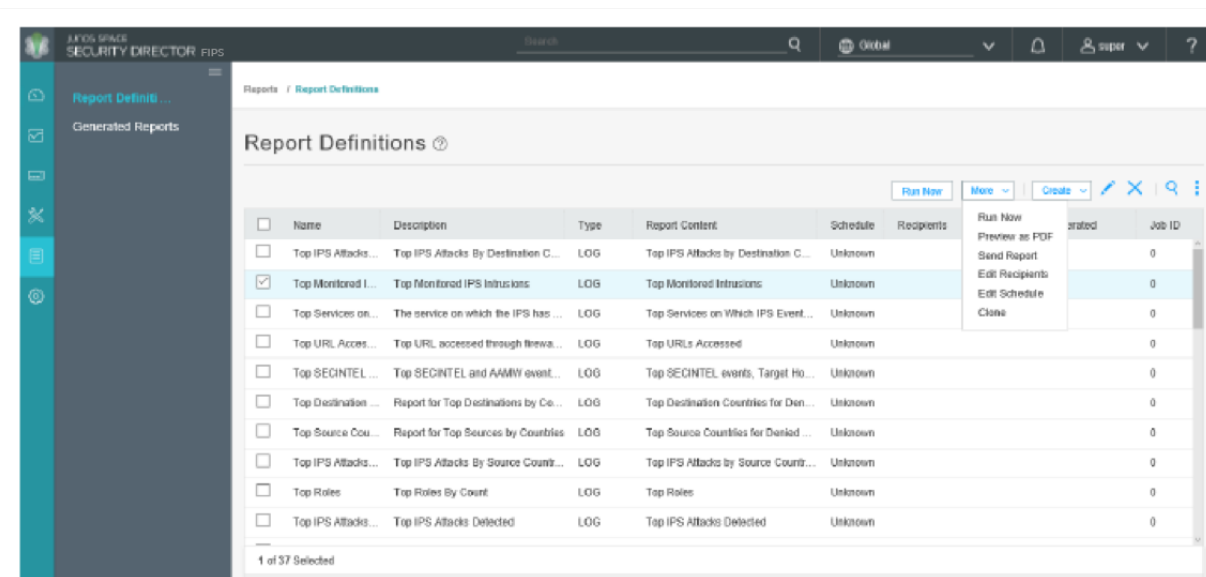
Figure 26: Security Director Configure Tab



Reports

The Reports tab provides a workspace in which you can create and send reports to other interested parties. The reports available on the Dashboard tab are a subset of the reports available here. When run, the report engine provides both graphic and numeric data for a complete visualization of the log data. Security Director comes with a predefined set of reports, and you can add your own customized reports from scratch or by cloning any of the predefined reports.

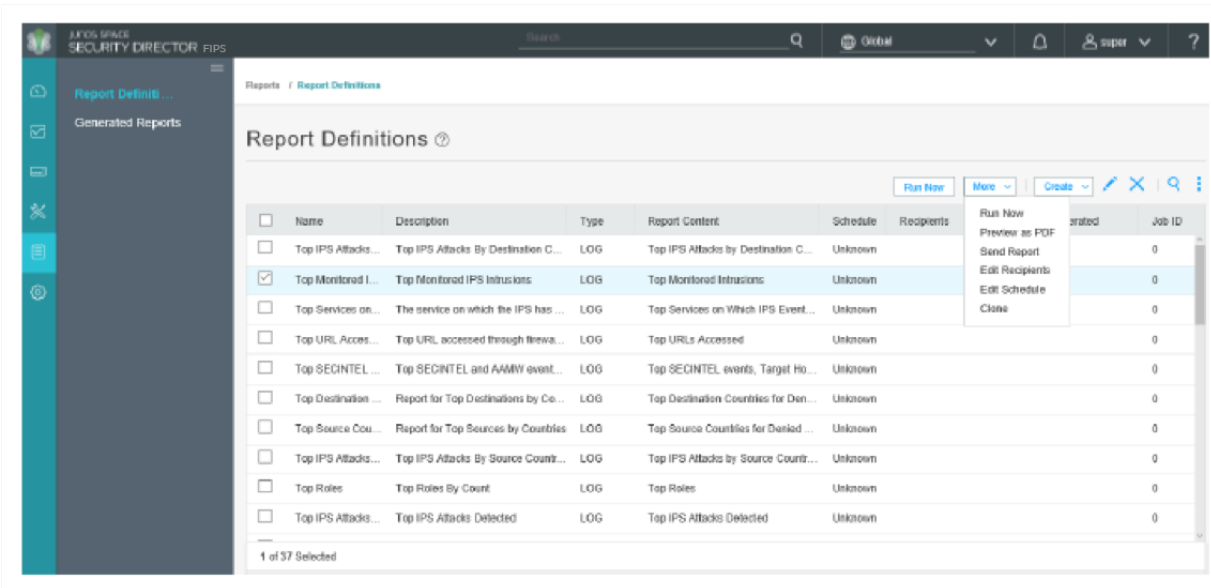
Figure 27: Security Director Reports Tab



Administration

The Administration tab provides a workspace in which you can manage role-based access control (RBAC), review and manage audit logs, manage logging, review and update the IPS signature database, and manage your login profile. Domain RBAC allows system administrators to logically divide Security Director into sections called domains. Policies, objects, logs, and services created for devices within any one domain are available for use only within that domain. User access can also be restricted to individual domains. For more information regarding RBAC, see *Domain RBAC Overview*.

Figure 28: Security Director Administration Tab



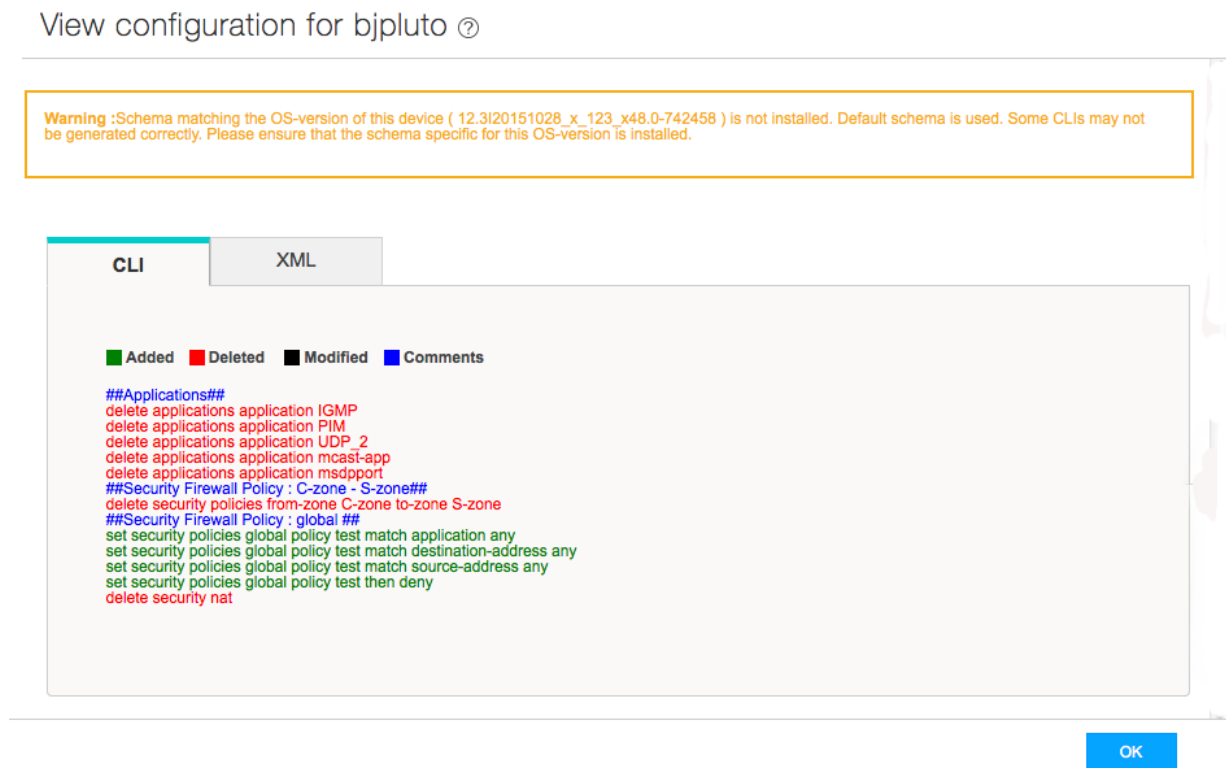
Global Features

Security Director contains assistive workflow wizards that guide you through some of its security functions. These include a rule-creation wizard and an add-device-profile wizard.

The publish workflow allows security configurations to be created or changed, assigned to devices, published and then updated to those devices. Policy changes, whether to IPS, Firewall, or any other managed policy can be staged by network operations center (NOC) personnel, previewed and approved by managers, and updated to the devices individually or all at once during maintenance windows or as often as needed by using the publish workflow. Figure 9 shows a sample of a configuration preview that could be used to review the changes that Security Director would make during the next update.

Cloning allows quick duplication of everything from objects, to rules, to entire policies. When dealing with complex rules or policies, cloning to make changes can ensure that there is a consistent starting point from which to make changes.

Figure 29: Configuration Update Preview



The configuration preview is available as CLI commands or as XML.

Conclusion

Security Director is a security management application designed with speed and scale in mind. Shared objects can be created and used across many security policies and devices. Firewall policies, NAT policies, and others can be created, changed, managed, and applied to individual devices or to groups of devices.

RBAC and domain features enable the Security Director administrator to allow access to many levels of users while restricting the visibility that they have into sensitive security information. Security devices, users, shared objects, and policies in one domain remain inaccessible to users who do not have access to that domain. Thus service provider organizations can provide customer isolation, allowing them to diversify their customer base. User management can be performed locally within Security Director, or remotely using central user management systems such as RADIUS.

And finally, events received by Security Director are logged and correlated in various ways, providing graphical and numerical charts that are understandable and actionable. Reports based on this information can be run and sent directly to stakeholders within an organization. The reports can show security and user trends over time, helping decision makers to craft concise and accurate security policies.

RELATED DOCUMENTATION

[Creating Firewall Policies](#)

[Dashboard Overview](#)

[Overview of Device Discovery in Security Director](#)

Setting Up a JA2500 Appliance for Security Director

The Juniper Networks JA2500 Junos Space appliance is a dedicated hardware device that provides the computing power and specific requirements to run Security Director and the Security Director API as applications.

For detailed steps on installing a JA2500 appliance, see [Juniper Networks JA2500 Junos Space Appliance Hardware Guide](#).

Configuring Basic Settings for a JA2500 Appliance

You must set up the JA2500 appliance to run as a Junos Space node. To configure a JA2500 appliance as a Junos Space node, you must configure basic network and system settings to make the appliance accessible on the network. For complete configuration steps, see [Configuring a Junos Space Appliance as a Junos Space Node](#).

RELATED DOCUMENTATION

[Security Director Installation Overview](#)

Setting Up a Junos Space Virtual Appliance for Security Director

The Junos Space virtual appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is easy to deploy, manage, and maintain.

For more information on installing Junos Space virtual appliance, see [Junos Space Virtual Appliance Installation and Configuration Guide](#).

Configuring the Basic Settings for a Junos Space Virtual Appliance

You must set up the Junos Space virtual appliance to run as a Junos Space node. After you deploy a Junos Space virtual appliance, you must enter basic network and machine information to make your Junos Space virtual appliance accessible on the network. For complete configuration steps, see [Configuring a Junos Space Virtual Appliance as a Junos Space Node](#).

2

CHAPTER

Understanding Roles and Authentication Methods

Understanding Roles in Security Director | **39**

Understanding Password Specifications and Guidelines for Security Director in Junos
Space in FIPS Mode | **40**

Understanding Roles in Security Director

Roles define the functionality or tasks that a user can perform in Junos Space, and they enable you to segregate users based on the functionality that they are allowed to access. You do this by assigning a different set of roles to various user accounts (in the case of local user accounts created in Junos Space) or to remote profiles to be used for remote authorization. When a user logs in to Junos Space, the tasks that they can perform are determined by the roles that have been assigned to that particular user account.

There are two types of roles: predefined roles, which are created by Junos Space, and user-defined (customized) roles, which must be created manually. The list of predefined user roles that Junos Space Security Director supports is available on the Roles page (select **Administration** > **Users & Roles** > **Roles**).

Roles can only be created by users who are assigned the User Administrator or Super Administrator or by a user with the Create Role permission.

The following predefined roles are available for Security Director users:

Security Analyst—Has access to either all the device management tasks or only those device management sub-tasks to which the analyst role is mapped. These users can also view the security director device and read log collector information.

Security Architect—Has access to either all the device management tasks or only those device management sub-tasks to which the analyst role is mapped. These users can also download and install signatures, and create, view, delete, export and publish policies.

Security Director Change Control Approver —A user who has access permission to approve CRs from a requester. For example, a senior administrator or manager can act as an approver, after which a firewall administrator, acting as the requester, can update the changes to the appropriate firewall or NAT policy.

Security Director Change Control Requester—A user who has access permission to make changes to designated policies, submit them for approval, and once approved, update them to the network. For example, an administrator, who provides the required information about the change to the firewall or NAT policy.

Security Operator Read Only—Has access to view all firewall policies and alerts definitions and has access to edit and view dashboards.

Understanding Password Specifications and Guidelines for Security Director in Junos Space in FIPS Mode

Ensure that the device is in FIPS mode before you configure the Super Administrator or any users. All passwords established for users by the Super Administrator must conform to the following Junos Space in FIPS mode requirements. Attempts to configure passwords that do not conform to the following specifications result in an error.

- **Length.** Passwords must contain between 10 and 20 characters.
- **Character set requirements.** Passwords must contain at least three of the following five defined character sets:
 - Uppercase letters
 - Lowercase letters
 - Digits
 - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- **Authentication requirements.** All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size—for example, 20 characters for SHA-1 authentication.

Guidelines for strong passwords. Strong, reusable passwords can be based on letters from a favorite phrase or word and then concatenated with other unrelated words, along with added digits. In general, a strong password is:

- Easy to remember so that users are not tempted to write it down.
- Made up of mixed alphanumeric characters and punctuation. For FIPS compliance include at least one change of case, one or more digits, and one or more punctuation marks.
- Changed periodically.
- Not divulged to anyone.

Characteristics of weak passwords. Do not use the following weak passwords:

- Words that might be found in or exist as a permuted form in a system files such as `/etc/passwd`.
- The hostname of the system (always a first guess).
- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.

- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**root**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

3

CHAPTER

Deploying Security Director

Installing Security Director | 43

Installing Hot Patch | 53

Installing Security Director

IN THIS SECTION

- [Uploading the Junos Space Application | 44](#)
- [Installing the Uploaded Junos Space Application | 45](#)
- [Installing and Upgrading Security Director from the Junos Space Store | 47](#)

In Junos Space Security Director, a single image installs Security Director, Log Director, and the Security Director Logging and Reporting modules. You must deploy the Log Collector and then add it to the Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

NOTE: Both JSA as Log Collector and Security Director Log Collector cannot be added together.

To install the Junos Space Security Director:

1. Download the Junos Space Security Director Release image from the [download site](#).
2. Install the Security Director application using the procedure at [Adding a Junos Space Application](#).

The administrator can add a new Junos Space application while Junos Space Network Management Platform is still running.

Adding an application to the Junos Space Platform server is a two-step process:

1. Upload the application to the Junos Space Platform server.
2. Install the uploaded application.

Uploading the Junos Space Application

To upload a Junos Space application:

1. Ensure that the Junos Space application you want to add is downloaded from the Juniper Networks software download site to the local client file system:

<https://www.juniper.net/support/products/space/#sw>

2. Select **Administration > Applications** and click the Add Application icon.

The Add Application page appears. If you have not uploaded any applications, the page is blank.

3. Upload the new application by performing one of the following steps:

- a. Click **Upload via HTTP**.

The Software File dialog box appears.

- i. Type the name of the application file or click **Browse** to navigate to where the new Junos Space application file is located on the local file system.

- ii. Click **Upload**. This action might take a while. Wait until the application is uploaded.

If you are trying to upload an application that is not supported by Junos Space Platform 19.1R1, then Junos Space Platform displays the following error message:

Current platform version does not support this software version.

The Application Management Job Information dialog box appears. Go to step 4 to confirm whether the application is uploaded successfully.

- b. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. Add the Secure Copy credentials to upload the Junos Space Platform application image from a remote server to Junos Space.

- i. In the **Username** field, enter your username.
- ii. In the **Password** field, enter your password.
- iii. In the **Confirm password** field, enter your password again to confirm the password.
- iv. In the **Machine IP** field, enter the host IP address.

NOTE:

- Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
- The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

- v. In the **Software File Path** field, enter the path name of the Junos Space application file.

For example, `/root/<image-name>.img`.

- vi. Click **Upload**. This action might take a while. Wait until the application is uploaded.

If you are trying to upload an application that is not supported by Junos Space Platform Release 14.1R2, then Junos Space Platform displays the following error message:

Current platform version does not support this software version.

The Application Management Job Information dialog box appears. Go to step 4 to confirm whether the application is uploaded successfully.

4. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the **Jobs > Job Management** inventory page. Wait until the job is completed and ensure that the job is successful.

If the upload is successful, then the new application is displayed by application name, filename, version, release level, and the required Junos Space Platform version on the Add Application page.

Installing the Uploaded Junos Space Application

To install the uploaded application:

1. Select **Administration > Applications** and click the **Add Application** icon.

The Add Application page appears.

2. Select the uploaded application.

3. Click **Install** to install the application or click **Cancel** to exit the Add Application page.

The Application configuration page appears, displaying a list of server groups to which you can deploy the application.



CAUTION: After you select and successfully deploy an application to a server group, it is not possible to move the application from one server group to another from the Junos Space GUI. So choose a server group after careful consideration. To move an application from one server group to another, use the script tool (see the instructions specified in *Running Applications in Separate Server Instances*).

4. Select a server group to which you want to deploy the application.

The default server group is **platform** to which Junos Space Platform is deployed. If you do not select any server group, the selected application is automatically deployed to the default **platform** server group.

5. Click **OK** to proceed.

The Application Management Job Information dialog box appears.

6. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the Job Management page. Wait until the application is fully deployed and ensure that the job is successful.

If the installation of the application is a failure, then the Summary column for the installation job displays the reason for failure. However, the display of messages depends also on the type and version of the application being installed.

NOTE: It is important that you install the applications in the right order: from the primary application to the dependent applications.

7. If the installation is successful, without logging out of Junos Space Platform, select the application from the Application Chooser list (located at the top-left) to view and begin using its workspaces and tasks.

Installing and Upgrading Security Director from the Junos Space Store

The Junos Space store displays a list of applications, which can be installed on the Junos Space Network Management Platform. This topic describes the Security Director installation and upgrade procedure using the Junos Space store.

Before You Begin

- Configure Junos Space Store in Junos Space Network Management Platform. For details on configuring and modifying the Junos Space settings, see [Configuring and Managing Junos Space Store](#).
- You must deploy the Log Collector and Policy Enforcer nodes before installing Security Director.
- Ensure the HDD size (>500GB) of the Junos Space Platform before configuring Log Collector. OpenNMS should be in the disabled state.

For configuring Log Collector component in Junos Space store:

- For distributed deployment of Security Director Log Collector, deploy Log Collector VM on a VMWare ESX server, KVM server, or a JA2500 appliance. To know more about distributed deployment, see *Setting Up Security Director Log Collector*.
- For integrated deployment of Log Collector, install the Integrated Log Collector on a JA2500 Appliance or Junos Space virtual appliance. To know more about the integrated deployment of Log Collector, see, *Setting Up Security Director Log Collector*.
- Deploy and configure JSA for using JSA as Log Collector. See, *JSA Log Collector Overview*.

For configuring Policy Enforcer component in Junos Space Store:

- Deploy and configure Policy Enforcer. See, *Installing Policy Enforcer* in [Administration Guide](#).

To install and upgrade Security Director from the Junos Space Store:

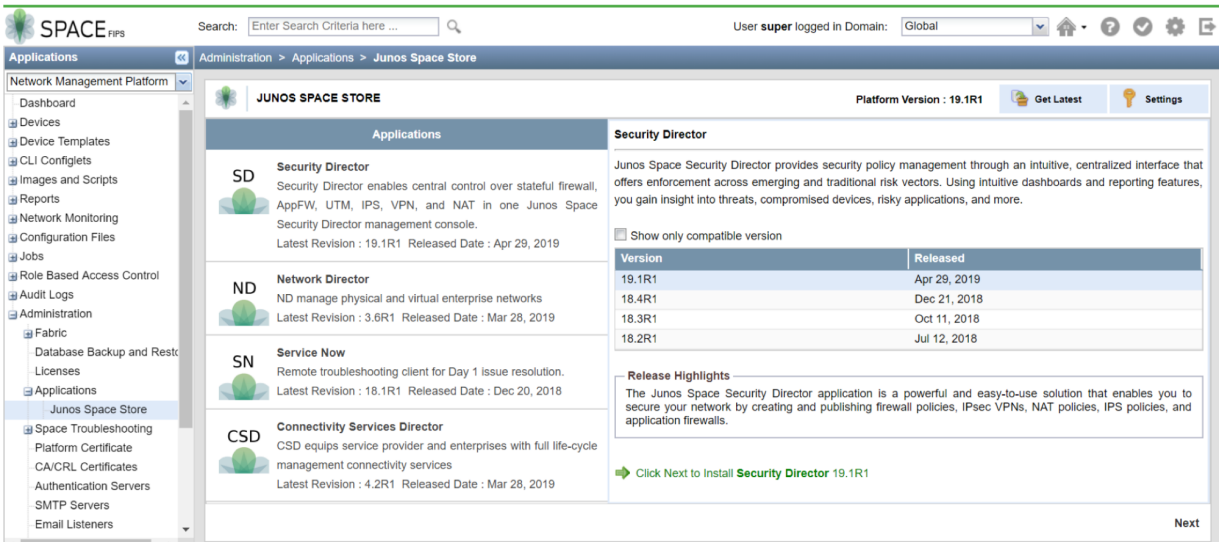
1. Log in to Junos Space Network Management Platform.
2. Select **Administration > Applications > Junos Space Store**.

The Junos Space Store page appears.

NOTE: Click **Get Latest** to refresh the list of applications in Junos Space store.

The Junos Space store with all the applications are displayed as shown in [Figure 30 on page 48](#).

Figure 30: Junos Space Store



3. Select **Security Director**.

The details of the application such as the compatible versions, version release date, and release highlights are displayed.

NOTE: Click **Show only compatible version** option to display only the Security Director versions supported on the current platform version.

4. Select a version to be installed or upgraded and click **Next**

NOTE: If the selected version is not compatible with the Junos Space Network Management Platform version, a warning message is displayed.

The Security Director configuration options are displayed as shown in [Figure 31 on page 49](#).

Figure 31: Security Director Components

JUNOS SPACE STORE

Security Director 19.1R1 Configuration Options

Please select the components to configure.

☒ **Configure Log Collector 19.1R1**

The Junos Space Security Director Logging and Reporting module enables log collection across multiple SRX Series devices and enables log visualization.

Note : If you have a scenario where you require more log reception capacity or events per second, you can configure log collector. Adding log collector provides higher rates of logging and better query performance.

Requirement : For Integrated Log Collector, OpenNMS must be disabled and Disk space should be greater than 500GB in Junos Space Network Management Platform.

Select Deployment Mode:

☒ **Configure Policy Enforcer 19.1R1**

Juniper's Software-Defined Secure Network (SDSN) platform leverages the entire network, not just perimeter firewalls, as a threat detection and security enforcement domain. The Policy Enforcer component of Junos Space Security Director provides the ability to orchestrate policies created by Juniper's Sky Advanced Threat Prevention cloud-based malware detection solution and distributes them to EX Series and QFX Series switches, as well as to Juniper virtual and physical SRX Series firewalls.

Requirement : For Standalone Policy Enforcer, the user should provide details of Policy Enforcer node deployed separately.

Select Deployment Mode:

IP Address:

Password:

Back **Next**

5. Select the components, which you want to configure and complete the configuration according to the guidelines given in [Table 6 on page 50](#).

NOTE: User can configure Log Collector and Policy Enforcer if already deployed and available. The previous method of adding the Log Collector and Policy Enforcer from Security Director is also applicable.

NOTE: Junos Space store allows the component configuration while installing Security Director. Upgrade of components like Log Collector and Policy Enforcer is not handled by Junos Space Store. Therefore, refer the existing method of upgrading Log Collector and Policy Enforcer components after upgrading the Security Director application.

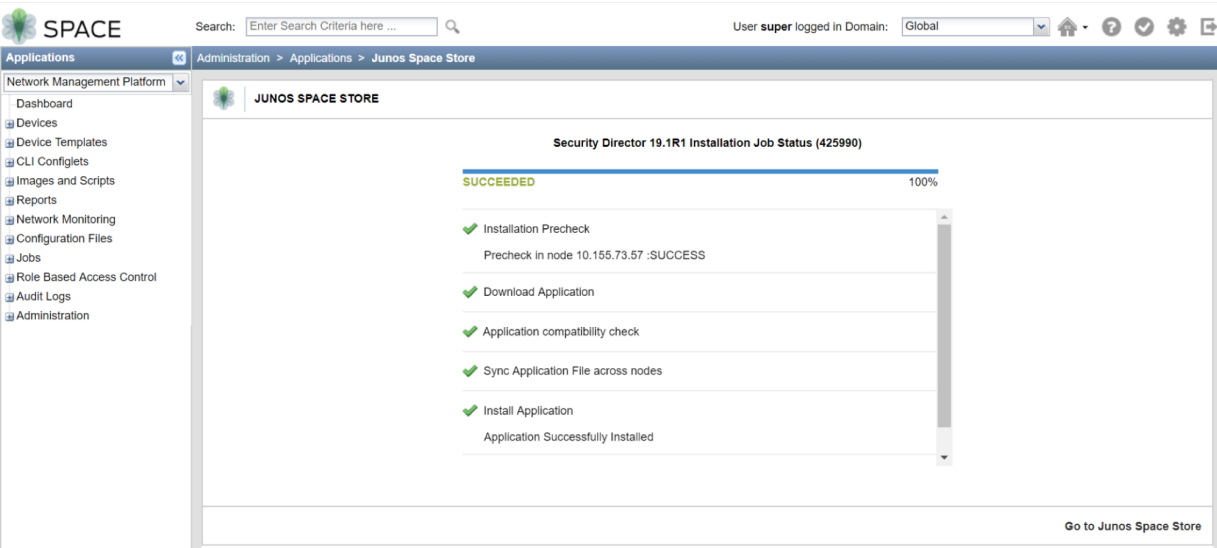
6. Click **Next**.

The Security Director terms and conditions and the license agreement is displayed. Review the license agreement.

7. Click **Accept and Install**.

The job status is displayed as shown in [Figure 32 on page 50](#).

Figure 32: Job Status



8. Click **Go to Junos Space Store**.

The installed or upgraded version of Security Director is displayed in the Junos Space store as shown in [Figure 33 on page 50](#).

Figure 33: Verifying the Installed or Upgraded Version

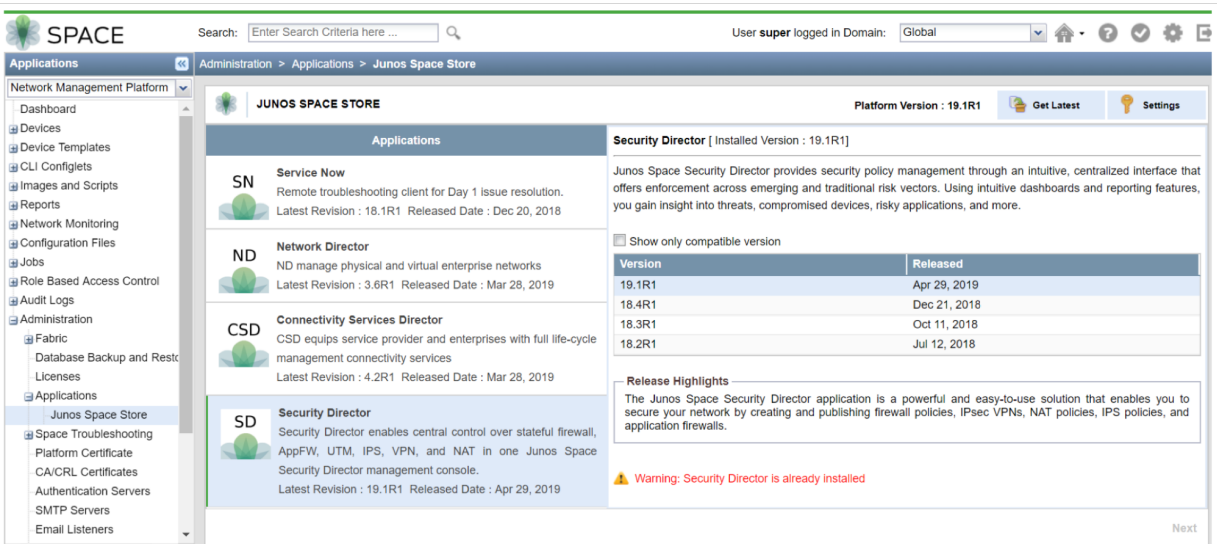


Table 6: Security Director Components Description

| Fields | Description |
|---------------|-------------|
| Log Collector | |

Table 6: Security Director Components Description (*continued*)

| Fields | Description |
|-----------------|--|
| Deployment Mode | <p>Select one of the following:</p> <ul style="list-style-type: none"> • Integrated—The integrated Log Collector is installed on Junos Space node (JA2500 appliance or virtual appliance). Integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance supports only 500 eps. NOTE: For Integrated Log Collector, OpenNMS must be disabled. On the Junos Space Network Management Platform, the disk space must be greater than 500GB. • Standalone—Standalone log collector VM is deployed separately on a VMWare ESX Server, KVM Server, or JA2500 appliance. NOTE: The fields Node Type, Node Name, IP Address, and Username and Password are applicable only if the deployment mode is Standalone. |
| Node Type | <p>Select one of the following:</p> <ul style="list-style-type: none"> • Security Director Log Collector • Juniper Secure Analytics <p>NOTE: You can add only Log Receiver node in Security Director and cannot add Log Storage node.</p> |
| Node Name | Enter the Node name. |
| IP Address | Enter the IPv4 or IPv6 address. |

Table 6: Security Director Components Description (continued)

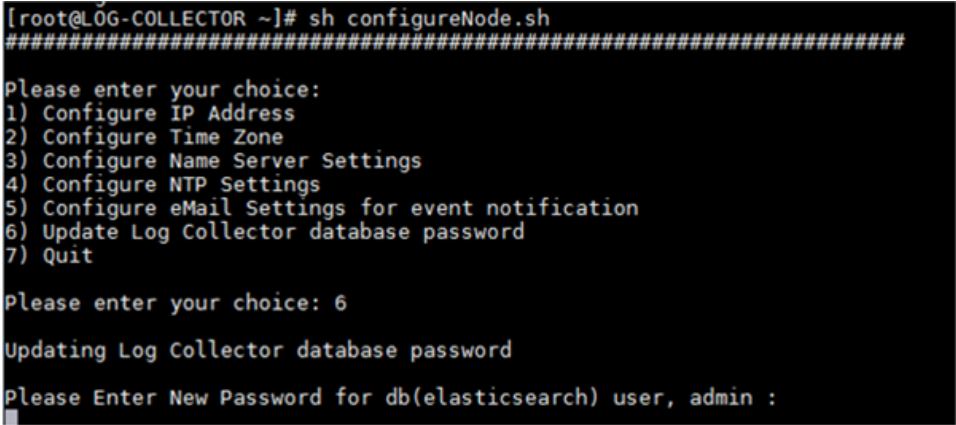
| Fields | Description |
|-----------------------|--|
| Username and Password | <p>For Security Director Log Collector, provide the default credentials; username is admin and password is juniper123. Change the default password using the Log Collector CLI <code>configureNode.sh</code> command as shown in Figure 34 on page 52.</p> <p>Figure 34: Change Password</p>  <pre>[root@LOG-COLLECTOR ~]# sh configureNode.sh ##### Please enter your choice: 1) Configure IP Address 2) Configure Time Zone 3) Configure Name Server Settings 4) Configure NTP Settings 5) Configure eMail Settings for event notification 6) Update Log Collector database password 7) Quit Please enter your choice: 6 Updating Log Collector database password Please Enter New Password for db(elasticsearch) user, admin :</pre> <p>For JSA, provide the admin credentials that is used to login to the JSA console.</p> |
| Policy Enforcer | |
| Deployment Mode | <p>Select Standalone.</p> <p>NOTE: For Policy Enforcer, only Standalone option is available.</p> |
| IP Address | <p>Specify the IP address of the Policy Enforcer virtual machine.</p> |
| Password | <p>Enter the password to login to the virtual machine with the root credentials.</p> |

Table 6: Security Director Components Description (*continued*)

| Fields | Description |
|----------------------------|---|
| Sky ATP Configuration Type | <p>Select one of the following configuration types:</p> <ul style="list-style-type: none"> • Sky ATP—Includes all threat prevention types, but does not include the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer. All enforcement is done through SRX Series Device policies. • Cloud Feeds Only—The prevention types available are command and control server, infections hosts, and Geo IP feeds. Policy Enforcer Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies are also available. All enforcement is done through SRX Series Device policies. • Sky ATP with SDSN—A full version of the product. All Policy Enforcer features and threat prevention types are available. • None—There are no feeds available from Sky ATP, but the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer are available. Infected hosts is the only prevention type available. |
| Network End Point | <p>Polling timers affect how often the system polls to discover endpoints. The timer polls infected endpoints moving within the sites that are a part of Secure fabric. You can set this range from 2 minutes to 60 minutes. The default is 5 minutes.</p> |
| PollSite End Point | <p>Polling timers affect how often the system polls to discover endpoints. The timer polls all endpoints added to the secure fabric. You can set this range between 1 to 48 hours. The default is 24 hours.</p> |

Installing Hot Patch

Security Director hot patches are signed using SHA256 and it should be installed using a script. The script validates the signature of the hot patch and triggers hot patch execution.

Run the following script to install the hot patch:

```
sh /var/www/cgi-bin/installAppHotpatch.sh -f <ND_HOTPATCH_IMAGE> --patch-script
<HOT_PATCH_SCRIPT>] [ARGUMENTS_TO_HOTPATCH_SCRIPT]
```

4

CHAPTER

Working in Build Mode

Overview of Device Discovery in Security Director | 55

Overview of Device Discovery in Security Director

You use the device discovery feature to add devices to Junos Space. Device discovery is the process of finding a device and then synchronizing the device inventory and configuration with the Junos Space database. To use device discovery, Junos Space must be connected to the device.

You discover devices in Junos Space Security Director by creating and using a device discovery profile. A device discovery profile contains information about discovery targets, probes used to discover devices, credentials for authentication, and device SSH fingerprints, and is used to discover, authenticate, and connect to the device.

During discovery, Junos Space connects to the physical device and retrieves the running configuration and the status information of the device. To connect with and configure devices, Junos Space uses the Juniper Networks Device Management Interface (DMI), which is an extension of the NETCONF network configuration protocol.

To discover network devices, Junos Space uses SSH, and (optionally) ping, and SNMP protocols.