

Security Director

Security Director Installation and Upgrade Guide

Published
2023-01-04

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 Security Director Installation and Upgrade Guide
Copyright © 2022 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 | v

Documentation and Release Notes | v

Documentation Conventions | v

Documentation Feedback | viii

Requesting Technical Support | viii

Self-Help Online Tools and Resources | ix

Creating a Service Request with JTAC | ix

1

Installing and Upgrading Security Director

Security Director Installation Overview | 11

Intended Audience | 12

Set Up a Junos Space Virtual Appliance for Security Director | 13

Upgrade Junos Space Network Management Platform | 13

Install Security Director | 14

Upgrade Security Director | 15

Junos Space Store Overview | 19

Install and Upgrade Security Director from the Junos Space Store | 20

2

Setting Up and Upgrading Log Collector

Log Collector 22.3 Overview | 26

Benefits | 26

Log Collector 22.3 – Architecture | 27

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files | 27

Add Security Director Insights as a Log Collector | 33

Upgrade Security Director Insights | 38

JSA Log Collector Overview | 41

Add JSA Log Collector Node to Security Director | 42

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

Use this guide to install and upgrade Security Director application, set up Log Collector, add Log Collector to Security Director, and upgrade Log Collector.

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 vi](#) 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 vi 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.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

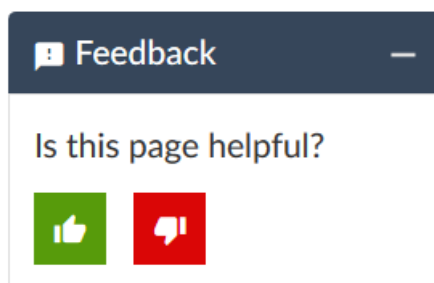
Table 2: Text and Syntax Conventions (*continued*)

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

Installing and Upgrading Security Director

Security Director Installation Overview | 11

Set Up a Junos Space Virtual Appliance for Security Director | 13

Upgrade Junos Space Network Management Platform | 13

Install Security Director | 14

Upgrade Security Director | 15

Junos Space Store Overview | 19

Install and Upgrade Security Director from the Junos Space Store | 20

Security Director Installation Overview

Security Director is a Junos Space management application designed to enable quick, consistent, and accurate creation, maintenance, and application of network security policies. It is a powerful and easy-to-use solution that lets you secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls.

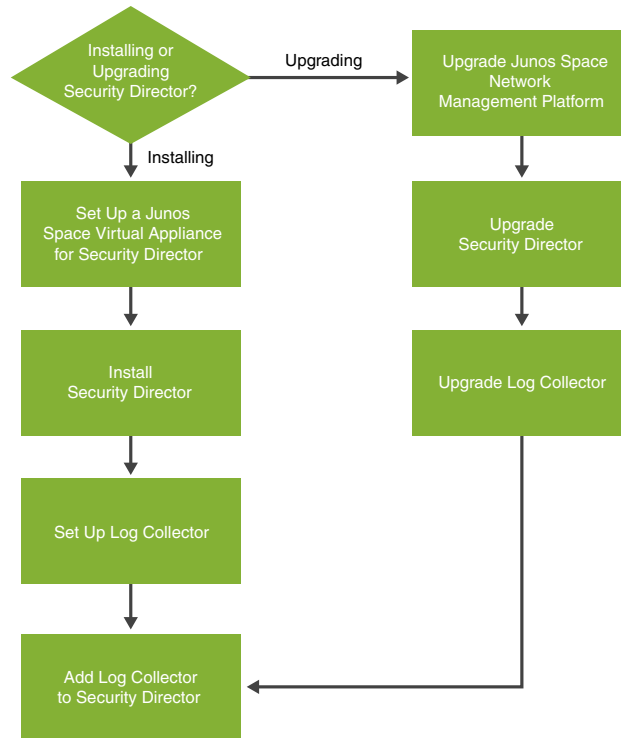
Before you install Security Director, you must configure the Junos Space Appliance as a Junos Space node.

You can install Security Director on Junos Space Virtual Appliance. 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. You must deploy the virtual appliance on a VMware ESX server, VMware ESXi server, or a KVM server which provides a CPU, hard disk, RAM, and a network controller, but requires installation of an operating system and applications to become fully functional.

For information about installing Junos Space virtual appliances on a VMware ESX server, VMware ESXi server, or KVM server, see the [Junos Space Virtual Appliance Installation and Configuration Guide](#).

[Figure 1 on page 12](#) shows the Security Director installation and upgrade flow.

Figure 1: Security Director Installation and Upgrade Flow



Intended Audience

This document is intended for network operators and administrators who install, configure, and manage the network security infrastructure.

RELATED DOCUMENTATION

[Set Up a Junos Space Virtual Appliance for Security Director](#) | 13

Set 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](#).

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](#).

RELATED DOCUMENTATION

| [Security Director Installation Overview](#) | 11

Upgrade Junos Space Network Management Platform

Junos Space Security Director Release can be installed or upgraded only on the supported Junos Space Network Management Platform Release. For example, Security Director Release 22.3R1 is supported only on Junos Space Network Management Platform Release 22.3R1. If your appliance is running the supported version of Junos Space, you can skip this procedure and begin installation of Security Director. For information on supported version of Junos Space Network Management Platform for Security Director, see [“Upgrade Security Director” on page 15](#).

If your appliance is running a Junos Space Network Management Platform release that is earlier than the supported release, you need to upgrade Junos Space Network Management Platform before upgrading Security Director.

To upgrade your Junos Space Network Management Platform:

1. Determine the installed Junos Space Network Management Platform version:
 - a. Log in to Junos Space. The default username is super and password is juniper123. The Dashboard is displayed.

Change the default credentials, when prompted.
 - b. Click the + icon next to Administration to expand the Administration menu.
 - c. Click **Applications** to list all of the applications installed.
 - d. Note the version of the Junos Space Network Management Platform or the Network Application Platform. (Some earlier versions of the Network Management Platform were named Network Application Platform.) If the currently installed release is a supported one, you can skip the upgrade procedure; if not, you must upgrade the Junos Space Network Management Platform to the supported release.
2. Upgrade Junos Space Network Management Platform using the procedure at [Upgrading to Junos Space Network Management Platform Release 22.3R1](#).

NOTE: For more information about application compatibility, see the Knowledge Base article KB27572 at [Junos Space Application Compatibility](#).

RELATED DOCUMENTATION

| [Set Up a Junos Space Virtual Appliance for Security Director](#) | 13

Install Security Director

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 Insights as Log Collector cannot be added together.

NOTE: Upgrade to the supported release of Junos Space Network Management Platform Release. See [“Upgrade Junos Space Network Management Platform”](#) on page 13.

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](#).

NOTE: The applogic service restarts after the application installation job is successful.

RELATED DOCUMENTATION

[Upgrade Junos Space Network Management Platform | 13](#)

[Upgrade Security Director | 15](#)

[Junos Space Store Overview | 19](#)

[Install and Upgrade Security Director from the Junos Space Store | 20](#)

Upgrade Security Director

You can upgrade from a previous Security Director release to the latest Security Director release.

Before You Begin

- If you are upgrading from a previous version of Security Director, clear your browser cache before accessing the Security Director user interface.
- Back up Junos Space Security Director Release that you want to upgrade. You must take the backup before upgrading Junos Space Network Management Platform. Backing up the Junos Space Network Management Platform database before the upgrade helps you to recover the data if the upgrade fails. See [Backing Up the Junos Space Network Management Platform Database](#).
- You must upgrade to the supported Junos Space Network Management Platform Release, before you upgrade the Security Director, Log Director, and Security Director Logging and Reporting modules. See [“Upgrade Junos Space Network Management Platform” on page 13](#).
- The Junos Space Network Management Platform should be active and functioning.

NOTE: The Required Platform Version column in [Table 3 on page 16](#) indicates the supported Junos Space Network Management Platform version. Before upgrading Security Director, ensure that the system is running the supported Junos Space Network Management Platform version. See [“Upgrade Junos Space Network Management Platform” on page 13](#).

Table 3: Upgrade Path

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 22.3R1	22.3R1	<ul style="list-style-type: none"> • 22.2 > 22.3 • 22.1 > 22.3 	You can upgrade from the following releases: <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 22.2R1 and Security Director Release 22.2R1 • Junos Space Network Management Platform Release 22.1R1 and Security Director Release 22.1R1
Security Director 22.2R1	22.2R1	<ul style="list-style-type: none"> • 22.1 > 22.2 • 21.3 > 22.2 	You can upgrade from the following releases: <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 22.1R1 and Security Director Release 22.1R1 • Junos Space Network Management Platform Release 21.3R1 and Security Director Release 21.3R1

Table 3: Upgrade Path (*continued*)

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 22.1R1	22.1R1	<ul style="list-style-type: none"> • 21.2 > 22.1 • 21.3 > 22.1 	<p>You can upgrade from the following releases:</p> <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 21.2R1 and Security Director Release 21.2R1 • Junos Space Network Management Platform Release 21.3R1 and Security Director Release 21.3R1
Security Director 21.3R1	21.3R1	<ul style="list-style-type: none"> • 21.1 > 21.3 • 21.2 > 21.3 	<p>You can upgrade from the following releases:</p> <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 21.1R1 and Security Director Release 21.1R1 • Junos Space Network Management Platform Release 21.2R1 and Security Director Release 21.2R1
Security Director 21.2R1	21.2R1	<ul style="list-style-type: none"> • 21.1R1 > 21.2R1 	<p>You can upgrade from the following releases:</p> <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 21.1R1 and Security Director Release 21.1R1
Security Director 21.1R1	21.1R1	<ul style="list-style-type: none"> • 20.3R1 > 21.1R1 	<p>You can upgrade from the following releases:</p> <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 20.3R1 and Security Director Release 20.3R1
Security Director 20.3R1	20.3R1	<ul style="list-style-type: none"> • 19.3R1 > 20.3R1 • 19.4R1 > 20.3R1 • 20.1R1 > 20.3R1 	<p>You can upgrade from the following releases:</p> <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1 • Junos Space Network Management Platform Release 19.4R1 and Security Director Release 19.4R1 • Junos Space Network Management Platform Release 20.1R1 and Security Director Release 20.1R1

Table 3: Upgrade Path (*continued*)

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 20.1R1	20.1R1	<ul style="list-style-type: none"> • 19.3R1 > 20.1R1 • 19.4R1 > 20.1R1 	<p>You can upgrade from the following releases:</p> <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1 • Junos Space Network Management Platform Release 19.4R1 and Security Director Release 19.4R1
		<p>You can now perform direct upgrade to 20.1R1 from earlier versions of Junos Space Security Director Release 19.1R1 and 19.2R1.</p> <ul style="list-style-type: none"> • 19.1R1 > 20.1R1 • 19.2R1 > 20.1R1 <p>NOTE: You can perform direct upgrade only for Junos Space Security Director. However, you must follow all the supported upgrade paths for Junos Space Network Management Platform and Log Collector to upgrade to 20.1R1.</p>	
Security Director 19.4R1	19.4R1	<ul style="list-style-type: none"> • 19.2R1 > 19.4R1 • 19.3R1 > 19.4R1 	<p>You can upgrade from the following releases:</p> <ul style="list-style-type: none"> • Junos Space Network Management Platform Release 19.2R1 and Security Director Release 19.2R1 • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1

To upgrade from a previous version of Junos Space Security Director:

1. Download the Junos Space Security Director Release image to which you want to upgrade from the [download site](#).
2. Upgrade the Junos Space Security Director application using the procedure at [Upgrading a Junos Space Application](#).

NOTE:

- If you try to upload Junos Space Security Director image of a lower version, an error message **Can only upgrade to newer version** appears. Click **OK** and upload compatible version of Junos Space Security Director.
- If you try to upload incompatible version of Junos Space Security Director image, an error message **Current platform version does not support this software version** appears. Click **OK** and upload compatible version of Junos Space Security Director.

NOTE: The applogic service restarts after the application upgrade job is successful.

RELATED DOCUMENTATION

[Upgrade Junos Space Network Management Platform | 13](#)

[Install Security Director | 14](#)

[Junos Space Store Overview | 19](#)

[Install and Upgrade Security Director from the Junos Space Store | 20](#)

Junos Space Store Overview

The Junos Space store displays the latest compatible versions of the Junos Space applications, which can be installed or upgraded on the current version of Junos Space Network Management Platform. Starting in Junos Space Security Director Release 18.2R1, you can install or upgrade Junos space Security Director application from the Junos Space store on the Network Management Platform.

You must configure the Juniper Networks Software download credentials to connect to Junos Space store. The Junos Space store lists the latest available applications.

The Junos Space Network Management Platform accesses the metadata repository hosted by Juniper Networks to discover the available applications and published versions. When you initiate an install or upgrade for Security Director application or its components, the package path is identified from the metadata file and package is downloaded. This reduces the manual effort of downloading the application package from the download site and then uploading it to the Junos Space Network Management Platform server, thereby enhancing the installation and upgrade process.

You can view whether a Security Director application version is supported on the current Junos Space Network Management Platform version, even before initiating install or upgrade. Junos Space store allows the component configuration while installing Security Director. It limits the component configuration when you try to upgrade Security Director.

NOTE: The earlier method of installing and Upgrading Security Director application documented in [“Install Security Director” on page 14](#) and [“Upgrade Security Director” on page 15](#) are still applicable. You can choose to install using the existing method or through the Junos Space store.

RELATED DOCUMENTATION

| [Install and Upgrade Security Director from the Junos Space Store](#) | 20

Install and Upgrade 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](#).
- Ensure the HDD size (>500GB) of Junos Space Platform before configuring integrated Log Collector. OpenNMS should be in the disabled state.

For configuring Log Collector component in Junos Space store:

- For integrated deployment of Log Collector, install the Integrated Log Collector on a Junos Space virtual appliance.
- Deploy and configure JSA for using JSA as Log Collector. See, [“JSA Log Collector Overview” on page 41](#).

For configuring Policy Enforcer component in Junos Space Store:

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

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

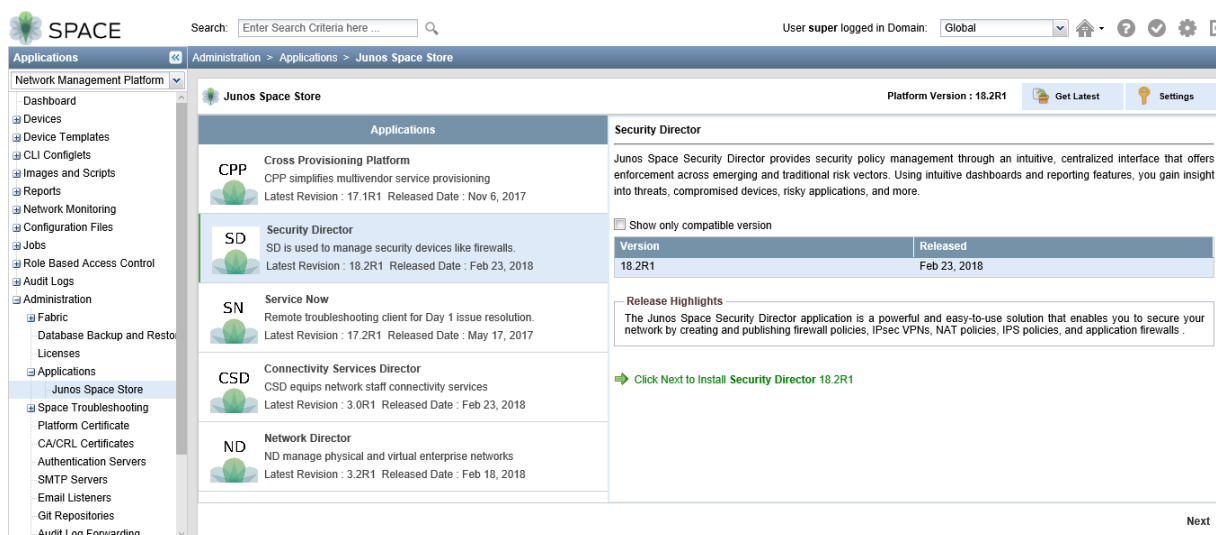
1. Log in to Junos Space Network Management Platform.
2. Select **Administration > Applications > Junos Space Store**.

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 2 on page 21](#).

Figure 2: 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.

- 5. Select the components, which you want to configure and complete the configuration according to the guidelines given in [Table 4 on page 23](#).

NOTE: Junos Space store allows the component configuration while installing Security Director. Upgrade of components is not handled by Junos Space Store.

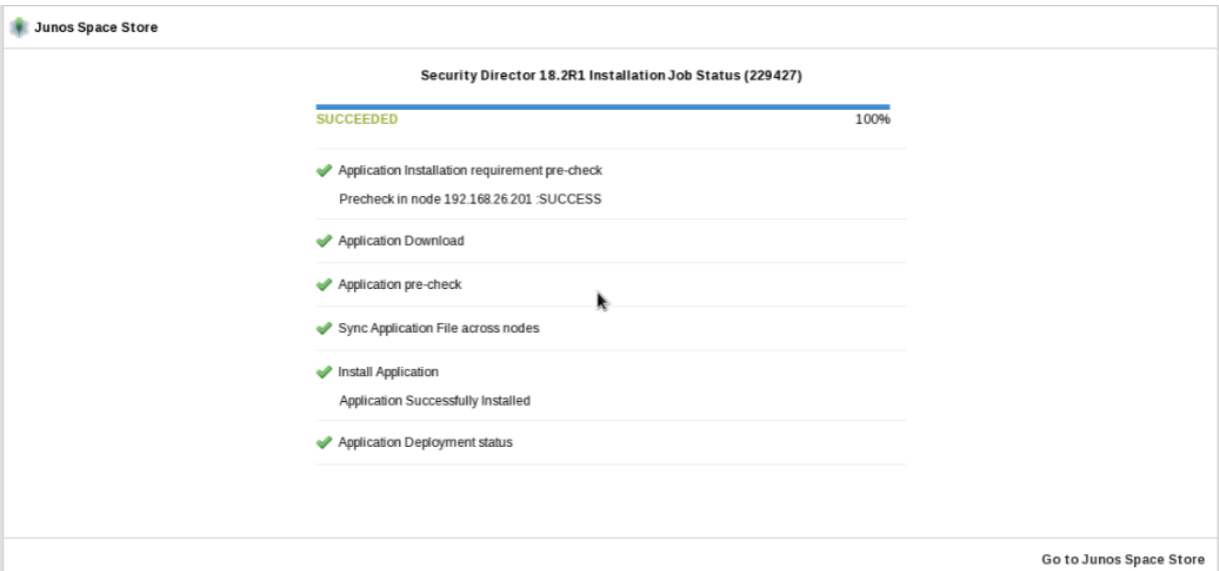
- 6. Click **Next**.

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

- 7. Click **Accept and Install**.

The job status is displayed as shown in [Figure 3 on page 22](#).

Figure 3: 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 4 on page 23](#).

Figure 4: Verifying the Installed or Upgraded Version

Administration > Applications > Junos Space Store

Junos Space Store Platform Version : 18.2R1 [Get Latest](#) [Settings](#)

Applications		Security Director [Installed Version : 18.2R1]				
CSD Connectivity Services Director CSD equips network staff connectivity services Latest Revision : 3.0R1 Released Date : Feb 23, 2018	Junos Space Security Director provides security policy management through an intuitive, centralized interface that offers enforcement across emerging and traditional risk vectors. Using intuitive dashboards and reporting features, you gain insight into threats, compromised devices, risky applications, and more.					
ND Network Director ND manage physical and virtual enterprise networks Latest Revision : 3.2R1 Released Date : Feb 18, 2018	<input type="checkbox"/> Show only compatible version <table border="1"> <thead> <tr> <th>Version</th> <th>Released</th> </tr> </thead> <tbody> <tr> <td>18.2R1</td> <td>Feb 23, 2018</td> </tr> </tbody> </table>		Version	Released	18.2R1	Feb 23, 2018
Version	Released					
18.2R1	Feb 23, 2018					
SN Service Now Remote troubleshooting client for Day 1 issue resolution. Latest Revision : 17.2R1 Released Date : May 17, 2017	Release Highlights The Junos Space Security Director application is a powerful and easy-to-use solution that enables you to secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls.					
CPP Cross Provisioning Platform CPP simplifies multivendor service provisioning Latest Revision : 17.1R1 Released Date : Nov 6, 2017	Warning: Security Director is already installed					
SD Security Director SD is used to manage security devices like firewalls. Latest Revision : 18.2R1 Released Date : Feb 23, 2018						

Table 4: Security Director Components Description

Fields	Description
Log Collector	
Deployment Mode	<ul style="list-style-type: none"> Integrated—The integrated Log Collector is installed on Junos Space node (virtual appliance). <p>Integrated Log Collector on a Junos Space virtual appliance supports only 500 eps.</p> <p>NOTE: For Integrated Log Collector, OpenNMS must be disabled. On the Junos Space Network Management Platform, the disk space must be greater than 500GB.</p>
Node Type	Select one of the following: <ul style="list-style-type: none"> Security Director Log Collector Juniper Secure Analytics
Node Name	Enter the Node name.
IP Address	Enter the IPv4 or IPv6 address.
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 configureNode.sh command.</p> <p>For JSA, provide the admin credentials that is used to login to the JSA console.</p>

Table 4: Security Director Components Description (*continued*)

Fields	Description
Policy Enforcer	
Deployment Mode	<p>Select Standalone.</p> <p>NOTE: For Policy Enforcer, only Standalone option is available.</p>
IP Address	Specify the IP address of the Policy Enforcer virtual machine.
Password	Enter the password to login to the virtual machine with the root credentials.
ATP Cloud Configuration Type	<p>Select one of the following configuration types:</p> <ul style="list-style-type: none"> • ATP Cloud—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. • ATP Cloud with Juniper Connected Security —A full version of the product. All Policy Enforcer features and threat prevention types are available. • None—There are no feeds available from ATP Cloud, 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	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.
PollSite End Point	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.

RELATED DOCUMENTATION

[Junos Space Store Overview](#) | 19

2

CHAPTER

Setting Up and Upgrading Log Collector

Log Collector 22.3 Overview | **26**

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files | **27**

Add Security Director Insights as a Log Collector | **33**

Upgrade Security Director Insights | **38**

JSA Log Collector Overview | **41**

Add JSA Log Collector Node to Security Director | **42**

Log Collector 22.3 Overview

You can use the Security Director Insights OVA file to install Security Director Insights and use the Security Director Insights VM as a log collector (Log Collector 22.3) and as an integrated Policy Enforcer.

In this chapter, you'll learn how to configure Security Director Insights as a log collector.

[Table 5 on page 26](#) below lists the required specifications for deploying Security Director Insights as a log collector for various events per second (eps) rates.

Table 5: Specifications

EPS	CPU	Memory	CPU/Memory Reservation
5k	4	16	8.8 GHz /16Gb
10k	8	16	17.6 GHz/16Gb
25k	24	80	50 GHz/80Gb

The log retention policies are:

- 365 days
- 80% storage size (This has higher priority)

Benefits

- A single Security Director Insights VM provides up to 25K eps making it easier for you to scale up with less virtual resources.
- Security Director Insights and Policy Enforcer capability are readily available for users of Log Collector 22.3, which is bundled with the Log Collector.
- It is the best long-term solution against vulnerabilities.

Log Collector 22.3 — Architecture



RELATED DOCUMENTATION

[Deploy and Configure Security Director Insights with Open Virtualization Appliance \(OVA\) Files](#) | 27

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files

Security Director Insights requires VMware ESXi server version 6.5 or later to support a virtual machine (VM) with the following configuration:

- 8 CPUs
- 24-GB RAM
- 1.2-TB disk space

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

To deploy and configure the Security Director Insights with OVA files, perform the following tasks:

1. Download the Security Director Insights VM OVA image from the Juniper Networks software [download page](#).

NOTE: Do not change the name of the Security Director Insights VM image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Security Director Insights VM may fail.

2. Launch the vSphere Client that is connected to the ESXi server, where the Security Director Insights VM is to be deployed.
3. Select **File > Deploy OVF Template**.

The Deploy OVF Template page appears, as shown in [Figure 5 on page 29](#).

Figure 5: Select an OVF Template Page

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template
Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☒ URL

☐ Local file

No file chosen

4. In the Select an OVF template page, select the **URL** option if you want to download the OVA image from the internet or select **Local file** to browse the local drive and upload the OVA image.
5. Click **Next**.
The Select a name and folder page appears.
6. Specify the OVA name, installation location for the VM, and click **Next**.
The Select a compute resource page appears.
7. Select the destination compute resource for the VM, and click **Next**.
The Review details page appears.
8. Verify the OVA details and click **Next**.
The License agreements page appears, as shown in [Figure 6 on page 30](#).

Figure 6: License Agreements Page

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 License agreements**
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

License agreements
The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

READ THIS AGREEMENT BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. JUNIPER NETWORKS IS WILLING TO LICENSE THE SOFTWARE TO YOU OR THE ENTITY YOU REPRESENT (COLLECTIVELY "YOU") AND MAKE AVAILABLE ASSOCIATED MAINTENANCE SERVICES ONLY IF YOU ACCEPT ALL OF THE TERMS OF THIS AGREEMENT.

YOU SHALL HAVE NO RIGHT TO INSTALL OR USE THE SOFTWARE OR TO RECEIVE ANY MAINTENANCE SERVICES THAT YOU MAY HAVE ORDERED UNLESS YOU HAVE RECEIVED A COPY OF THE SOFTWARE FROM JUNIPER NETWORKS OR A JUNIPER NETWORKS-AUTHORIZED RESELLER (COLLECTIVELY, AN "APPROVED SOURCE"), AND (II) YOU

☒ I accept all license agreements.

[CANCEL](#)
[BACK](#)
[NEXT](#)

9. Accept the EULA and click **Next**.

The Select storage page appears.

10. Select the destination file storage for the VM configuration files and the disk format. (Thin Provision is for smaller disks and Thick Provision is for larger disks.)

Click **Next**. The Select networks page appears.

11. Select the network interfaces that will be used by the VM.

IP allocation can be configured for DHCP or Static addressing. We recommend using Static IP Allocation Policy.

Click **Next**. The Customize template page appears. For DHCP instructions, see to Step 13.

12. For IP allocation as Static, configure the following parameters for the virtual machine:

- IP address—Enter the Security Director Insights VM IP address.
- Netmask—Enter the netmask.

- Gateway—Enter the gateway address.
- DNS Address 1—Enter the primary DNS address.
- DNS Address 2—Enter the secondary DNS address.

Figure 7: Customize Template Page

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Juniper Security Analytics	
Virtual Appliance Network Settings	
IP Allocation Policy	Static
IP address	Ignore this property if the IP allocation policy is DHCP. 10.0.0.1
Netmask	Ignore this property if the IP allocation policy is DHCP. 255.255.0.0
Gateway	Ignore this property if the IP allocation policy is DHCP. 10.0.0.1
DNS address 1	Ignore this property if the IP allocation policy is DHCP. 10.0.0.1
DNS address 2	Ignore this property if the IP allocation policy is DHCP.

CANCEL BACK NEXT

13. For IP allocation as DHCP, enter the search domain, hostname, device name, and device description for the virtual machine.

This option is recommended only for the Proof of Concept type of short-term deployments. Do not use this option.

Click **Next**. The Ready to complete page appears, as shown in [Figure 8 on page 32](#).

Figure 8: Ready to Complete Page

Deploy OVF Template

Click Finish to start creation.

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- ✓ 8 Customize template
- 9 Ready to complete**

Provisioning type	Deploy OVF From Remote URL
Name	juniper-20.3R1.s449c42
Template name	juniper-20.3R1.s449c42
Download size	4.3 GB
Size on disk	9.8 GB
Folder	Abhishek_Gandhi
Resource	it-cluster1a.englab.juniper.net
Storage mapping	1
All disks	Datastore: ranch99-vm; Format: Thin provision
Network mapping	2
administrative	Engineering
HA Monitoring	Engineering
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

[CANCEL](#)
[BACK](#)
[FINISH](#)

14. Verify all the details and click **Finish** to begin the OVA installation.

15. After the OVA is installed successfully, power on the VM and wait for the boot-up to complete.

16. Once the VM powers on, in the CLI terminal, log in as administrator with the default username as "admin" and password as "abc123".

After you log in, you will be prompted to change the default admin password. Enter a new password to change the default password, as shown in [Figure 9 on page 33](#).

Figure 9: Default Admin Password Reset

```
The authenticity of host '10.2.11.46 (10.2.11.46)' can't be established.
ECDSA key fingerprint is a0:b9:21:1f:0f:54:d6:7e:a7:6b:40:8f:9e:7c:cc:4a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.2.11.46' (ECDSA) to the list of known hosts.
admin@10.2.11.46's password:
The CLI admin password needs to be changed from the default.
Enter the new password of CLI admin: █
```

The Security Director Insights deployment is now complete.

RELATED DOCUMENTATION

[Add Security Director Insights as a Log Collector](#) | 33

Add Security Director Insights as a Log Collector

To use the log collector functionality that comes along with the Security Director Insights installation, add the IP address of the Security Director Insights virtual machine (VM) as a log collector.

Before you add the log collector node in the GUI, you must set the administrator password. By default, the Security Director log collector is disabled. You must first enable it and then set the administrator password.

To enable the log collector and configure the administrator password:

1. Go to the Security Director Insights CLI.

```
# ssh admin@${security-director-insights_ip}
```

2. Enter the application configuration mode.

```
user:Core# applications
```

3. Enable Security Director log collector.

```
user:Core#(applications)# set log-collector enable on
```

4. Configure the administrator password.

user:Core#(applications)# set log-collector password

Enter the new password for SD Log Collector access:

Retype the new password:

Successfully changed password for SD Log Collector database access

To add the Security Director Insights VM IP address as a log collector node:

1. From the Security Director user interface, select **Administration > Logging Management > Logging Nodes**, and click the plus sign (+).

The Add Logging Node page appears.

2. Choose the Log Collector type as **Security Director Log Collector**.

3. Click **Next**.

The Add Collector Node page appears.

4. In the Node Name field, enter a unique name for the log collector.

5. In the IP Address field, enter the IP address of the Security Director Insights VM.

The IP address used in the Deploy OVF Template page must be used in the Add Collector Node page, as shown in [Figure 10 on page 35](#) and [Figure 11 on page 36](#).

Figure 10: Deploy OVF Template Page

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- 8 Customize template**
- 9 Ready to complete

▼ Juniper Security Analytics 8 settings

Virtual Appliance Network Settings

IP Allocation Policy	Static ▼
IP address	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="10.0.0.0"/>
Netmask	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="255.255.0.0"/>
Gateway	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="10.0.0.1"/>
DNS address 1	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="10.0.0.1"/>
DNS address 2	Ignore this property if the IP allocation policy is DHCP. <input type="text" value=""/>

[CANCEL](#) [BACK](#) [NEXT](#)

Figure 11: Add Logging Node Page

Add Logging Node ?

Progress bar: Select Deployment (unselected), **Add Collector Node** (selected), Certificate Details (unselected)

Add Collector Node

Node 1

Node Name* ? 10. [redacted]
Valid

IP Address* ? 10. [redacted]

User Name* ? admin

Password* ? [redacted]

Cancel Back Next

6. In the User Name field, enter the username of the Security Director Insights VM.
7. In the Password field, enter the password of the Security Director Insights VM.
8. Click **Next**.
The certificate details are displayed.
9. Click **Finish** and then click **OK** to add the newly created Logging Node.

NOTE: Starting in Security Director Release 21.3R1 Hot Patch V1, you can add both the legacy log collector node and the Security Director Insights VM on the Logging Nodes page in Security Director. We've added the legacy log collector support for read-only purpose to view existing data in the event viewer. You cannot add same type of log collector nodes on the Logging Nodes page.

10. After you add Security Director Insights as a log collector, enable the following options in Junos Space:

- a. Log in to Junos Space.
- b. Select **Administration > Applications**.
- c. Right-click **Log Director** and select **Modify Application Settings**.
- d. Enable the following options:
 - Enable SDI Log Collector Query Format
 - Integrated Log Collector on Space Server

Performance Matrix

Table 6 on page 37 shows the performance matrix for various events per second (eps) rates.

Table 6: Performance Matrix for EPS

CPU	Memory	EPS	CPU/Memory Reservation
4	16	5K	8.8 GHz / 16Gb
8	16	10K	17.6 GHz / 16Gb
24	80	25K	50 GHz / 80Gb

NOTE: CPU and Memory values must be reserved according to the performance matrix, to achieve the correlating EPS.

RELATED DOCUMENTATION

Configure Security Director Insights High Availability

Security Director Insights High Availability Deployment Architecture

Configure Policy Enforcer for Security Director Insights Mitigation

Upgrade Security Director Insights

Table 7 on page 38 shows Security Director Insights upgrade path.

Table 7: Upgrade Path

Upgrading to Release	Upgrade Path
Security Director Insights 22.3R1	22.2R1 > 22.3R1
Security Director Insights 22.2R1	22.1R1 > 22.2R1
Security Director Insights 22.1R1	21.3R1 > 22.1R1
Security Director Insights 21.3R1	21.2R1 > 21.3R1

To upgrade from a previous version of Security Director Insights:

1. Download the release image from the [download site](#) to a location (virtual machine) that is accessible from Security Director Insights.
2. Type **server** to switch to the server mode of CLI.
3. Copy the upgrade package to Security Director Insights:
set system-update copy user@ip_addr:/location.

Figure 12: Copy the Upgrade Package

```

*****
*      Juniper Security Director Insights      *
*                                              *
*****

Welcome admin. It is now Thu Nov 11 19:33:16 UTC 2021
Core# server
Entering the server configuration mode...
Core#(server)# set system-update copy root@10.2.120.106:/root/Insights_release_21.1-2021-11-11-19-33-16.zip.tgz
root@10.2.120.106's password:

Copy is running in the background. Press any key to exit.

Insights_release_21.1-2021-11-11-19-33-16.zip.tgz 42% 858MB 66.0MB/s 00:17 ETA

```

NOTE: You can host the upgrade file to any location that is accessible by secure copy protocol (scp).

4. Check the copy progress:

show system-update copy.

Figure 13: Check Copy Progress

```

Core#(server)# show system-update copy
root@10.2.120.106 password:
Insights_release_21.1-2021-11-11-19-33-16.zip.tgz 100% 2017MB 50.2MB/s 00:40
Checking copied file...
Upgrade file is valid and was unpacked successfully.

Core#(server)#

```

5. Check the available upgrade versions:

show system-update versions.

Figure 14: Available Upgrade Versions

```

[redacted]:Core#(server)# show system-update versions
Type          Version      Size      OK to upgrade
software      21.1.1.1      1.97 GB   OK
software      21.1.1.1      1.97 GB   OK
[redacted]:Core#(server)#

```

6. Start the upgrade process:

set system-update start software <version-number>.

Use the <tab> key to select the software version number.

Figure 15: Start Upgrade Process

```

[redacted]:Core#(server)# set system-update start software 21.1.1.1
Started software upgrade to version 21.1.1.1
Update started. Run 'show system-update status' from server menu to check the status
[redacted]:Core#(server)#

```

7. Monitor the status of upgrade:

show system-update status.

Figure 16: Monitor Upgrade Status

```

Entering the server configuration mode...
[redacted]:Core#(server)# show system-update status
Type          Status
Software/Content Finished successfully
[redacted]:Core#(server)#

```


JSA Log Collector Overview

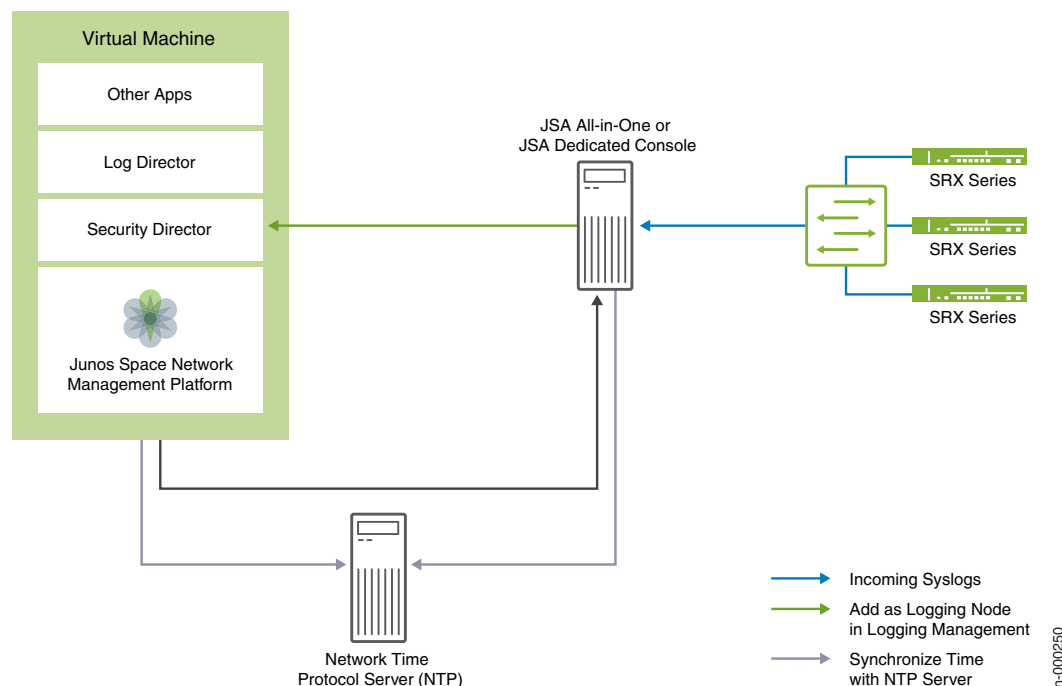
You can use Juniper Secure Analytics (JSA) as a Log Collector to view log data in Security Director. From the JSA console, Security Director queries logs from SRX Series devices. Security Director can use either JSA3800, JSA5800, JSA7500, or virtual JSA for log collection. You must add JSA as a logging node in Security Director to view log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

NOTE: The JSA version supported by Security Director to be added as log collector node is JSA Release 2014.8.R4 or later.

After JSA is deployed, you can configure network devices to send system logs to JSA. It collects the logs in a standalone or clustered setup. For more details on deploying and configuring JSA, see [Juniper Secure Analytics](#) documentation.

Figure 17 on page 41 shows the deployment example using the JSA All-in-One or JSA Dedicated Console.

Figure 17: Using JSA All-in-One or JSA Dedicated Console



To add JSA as a logging node in Security Director, see [“Add JSA Log Collector Node to Security Director”](#) on page 42.

Add JSA Log Collector Node to Security Director

You must deploy Juniper Secure Analytics (JSA) as a log collector and then add it to Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

Before You Begin

- Deploy JSA as a Log Collector.
- Configure system log and security logging for the devices managed by Junos Space Security Director from **Devices > Security Devices > Modify Configuration**.
- While adding SRX firewall as a log source in JSA or QRadar, set the log source type to Juniper Junos Platform and not Juniper SRX Series Services Gateway.
- You must have the recent version of Juniper Junos Device Support Module (DSM) installed on JSA or QRadar.
- After upgrading Log Collector, database password will reset to default credentials, that is, admin/abc123. You must re-configure the database password after Log Collector upgrade before adding the Log Collector node to Security Director.

To add Log Collector to Security Director:

1. From the Security Director user interface, select **Administration > Logging Management > Logging Nodes**, and click the plus sign (+).

The Add Logging Node page appears.

2. Choose the Log Collector type as **Juniper Secure Analytics**.

3. Click **Next**.

4. Complete the configuration for JSA Node.



CAUTION: For JSA, provide the admin credentials that is used to log in to the JSA console.

5. Click **Next**.

The certificate details are displayed.

6. Click **Finish**.
7. Review the summary of configuration changes from the summary page and click **Edit** to modify the details, if required.
8. Click **OK** to add the node.

A new logging node with your configuration is added. To verify that the node is configured correctly, click **Logging Management** to check the status of the node.

To remove an existing Security Director Log Collector and add JSA as a Log Collector:

1. Select **Administration > Logging Management > Logging Nodes**.
2. Select the existing Security Director Log Collector and click the delete icon to delete Security Director Log Collector node.
3. Click the + icon to add JSA as a Log Collector.
4. Configure the SRX Series devices to stop sending logs to Security Director Log Collector, and ensure that logs are sent to the JSA node.

RELATED DOCUMENTATION

| [JSA Log Collector Overview](#) | 41