Engineering
Simplicity

Security Director Insights Installation and Upgrade Guide

Published

2023-06-30

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

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 Insights Installation and Upgrade Guide

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 Security Director Insights Installation and Upgrade Guide
Security Director Insights Overview | 11
Benefits | 11
Security Director Insights Architecture | 11
Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files | 12
Add Security Director Insights as a Log Collector | 19
Security Director Insights High Availability Deployment Architecture | 23
Configure Security Director Insights High Availability | 25
Before You Begin | 25
Enable HA | 27
Manually Trigger Failover | 30
Disable HA | 33
Upgrade HA | 35
Configure High Availability for Security Director Insights as Log Collector | 37
Configure Policy Enforcer for Security Director Insights Mitigation | 39
Add Security Director Insights Nodes | 40
Configure Security Director Insights as Integrated Policy Enforcer | 40
Create Custom Feeds for Mitigation | 44
Configure Security Director Insights Mitigation Using Policy Enforcer | 44
Monitor Mitigation Through Policy Enforcer | 45

Upgrade Security Director Insights | 47

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 understand the architecture and deployment of Security Director Insights. It also includes procedures for configuring Policy Enforcer for mitigation, adding log collector nodes, and HA configuration.

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`
Italic text like this	- Introduces or emphasizes important new terms. - Identifies guide names. - Identifies RFC and Internet draft titles.	- A policy *term* is a named structure that defines match conditions and actions. - *Junos OS CLI User Guide* - RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	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** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

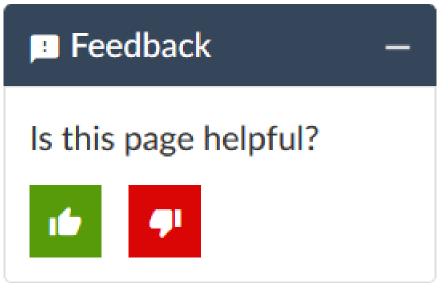
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• 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

Security Director Insights Installation and Upgrade Guide

Security Director Insights Overview | 11

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files | 12

Add Security Director Insights as a Log Collector | 19

Security Director Insights High Availability Deployment Architecture | 23

Configure Security Director Insights High Availability | 25

Configure High Availability for Security Director Insights as Log Collector | 37

Configure Policy Enforcer for Security Director Insights Mitigation | 39

Upgrade Security Director Insights | 47

Security Director Insights Overview

Security Director Insights is a single virtual appliance (Service VM) that runs on the VMware vSphere infrastructure. It facilitates automated security operations. It enables you to take effective actions on security events logged by Juniper Networks security products. The events that affect a host or events that are impacted by a particular threat source are presented by Security Director Insights from different security modules. These events provide instantaneous information about the extent and stage of an attack. Security Director Insights also detects the hosts and servers under attack by analyzing events that are not severe enough to block. The application contains an option to verify the incidents using your trusted threat intelligence providers. After you have verified the incidents, you can take preventive and remedial actions using the rich capabilities of our security products.

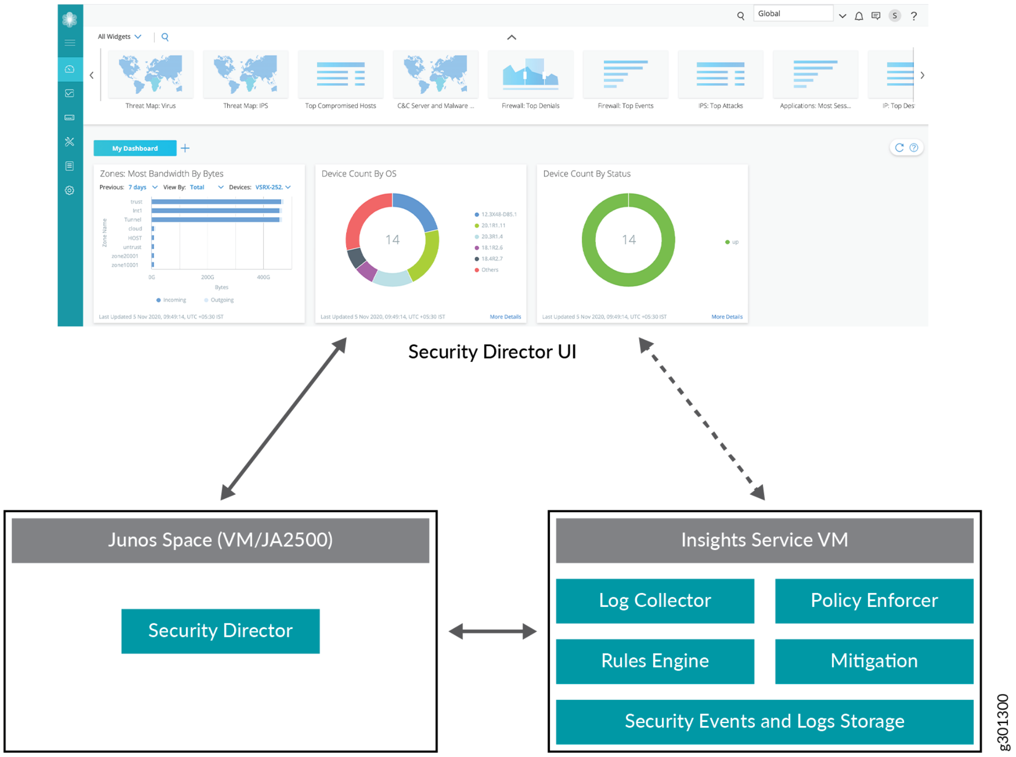
Benefits

- Reduce the number of alerts across disparate security solutions
- Quickly react to active threats with one-click mitigation
- Improve the security operations center (SOC) teams' ability to focus on the highest priority threats

Security Director Insights Architecture

The Service VM provides the following functionality, as shown in Figure 1 on page 12.

Figure 1: Security Director Insights Architecture



- The Service VM works with the Security Director ecosystem. The Security Director Insights GUI is integrated into the Security Director GUI.
- The Log Collector and Policy Enforcer are integrated within the Security Director Insights VM.

RELATED DOCUMENTATION

Add Insights Nodes

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.

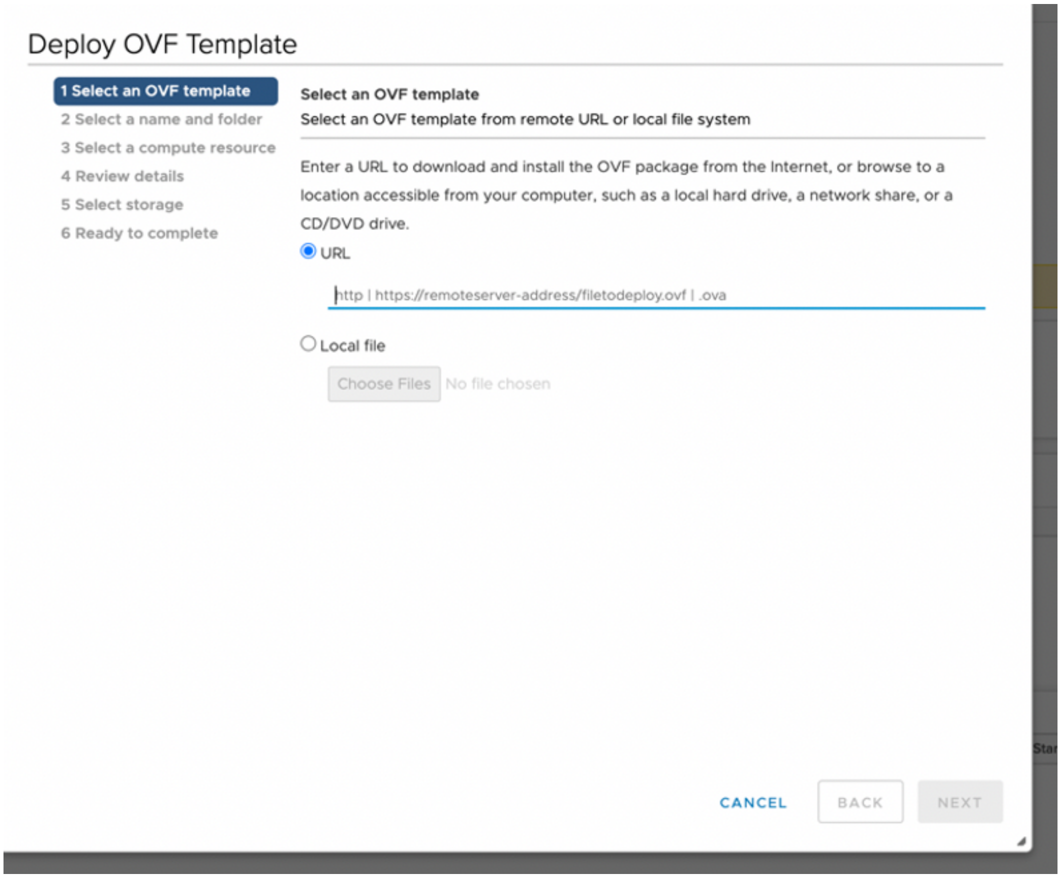
   > **NOTE:** Do not change the name of the Security Director Insights VM image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Security Director Insights VM may fail.

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 2 on page 14.

Figure 2: Select an OVF Template Page



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

http | https://remoteserver-address/filetodeploy.ovf | .ova

○ 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.

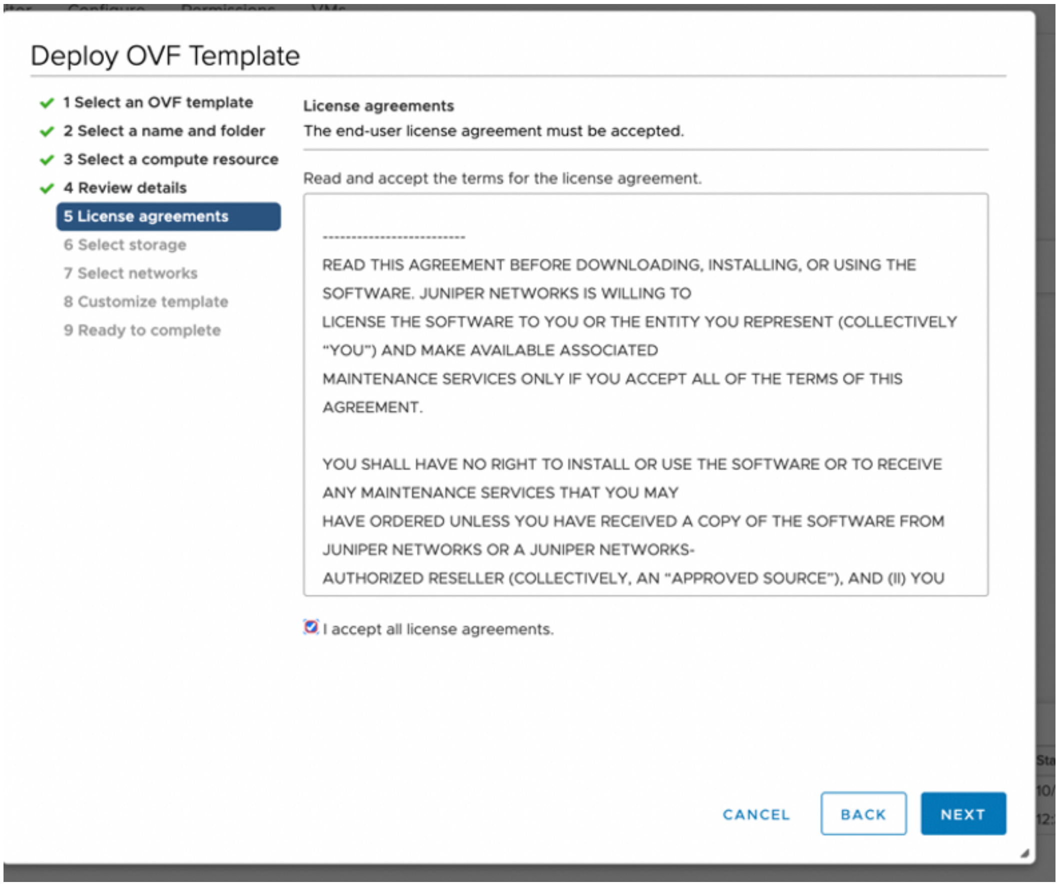
7. Select the destination compute resource for the VM, and click **Next**.

   The Review details page appears.

8. Verify the OVA details and click **Next**.

   The License agreements page appears, as shown in Figure 3 on page 15.

Figure 3: License Agreement Page



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.

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.

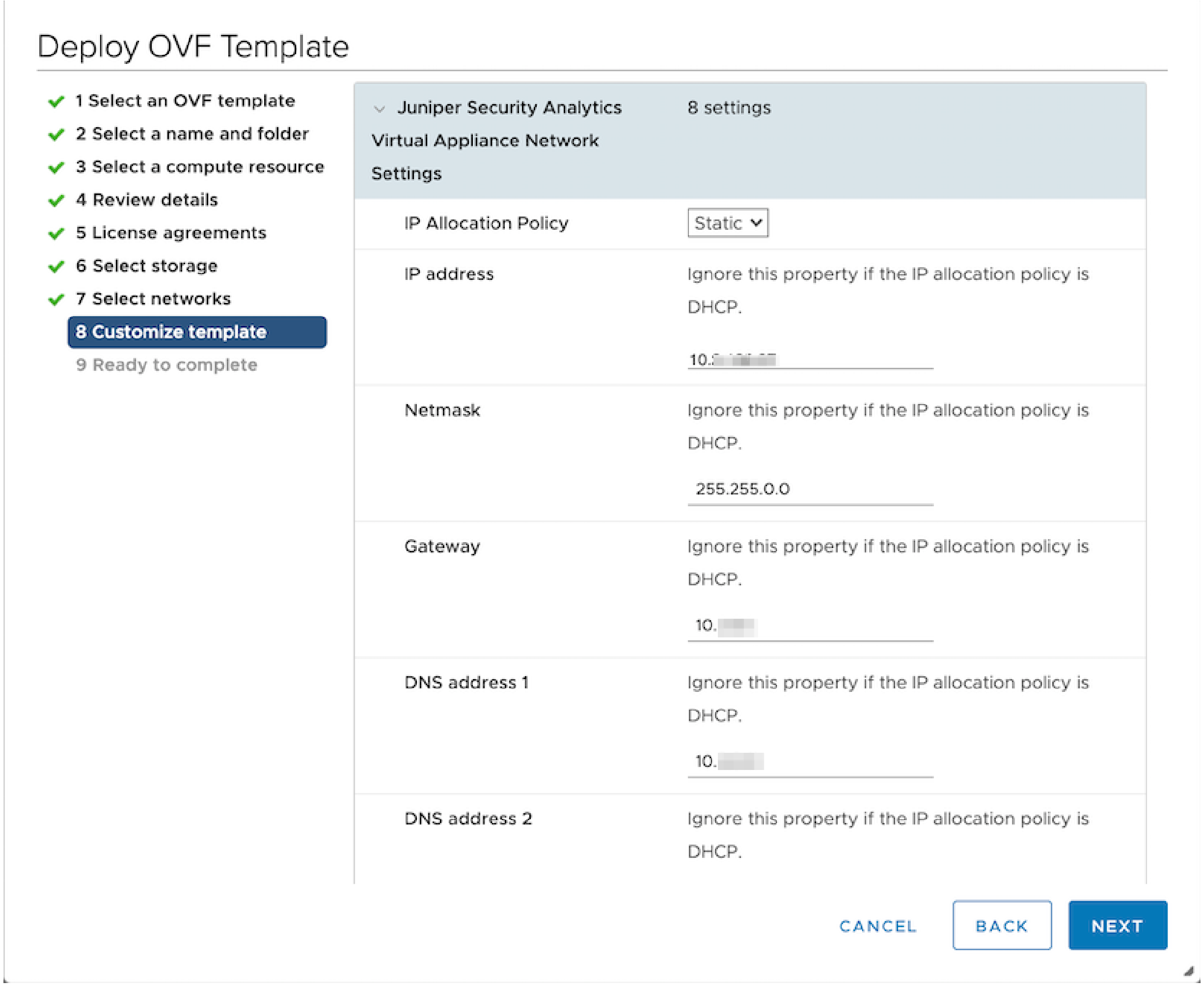
    Click **Next**. The Customize template page appears. For DHCP instructions, see Step 13.

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 4: 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 — 8 settings

IP Allocation Policy: Static

IP address: Ignore this property if the IP allocation policy is DHCP. 10.[redacted]

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.[redacted]

DNS address 1: Ignore this property if the IP allocation policy is DHCP. 10.[redacted]

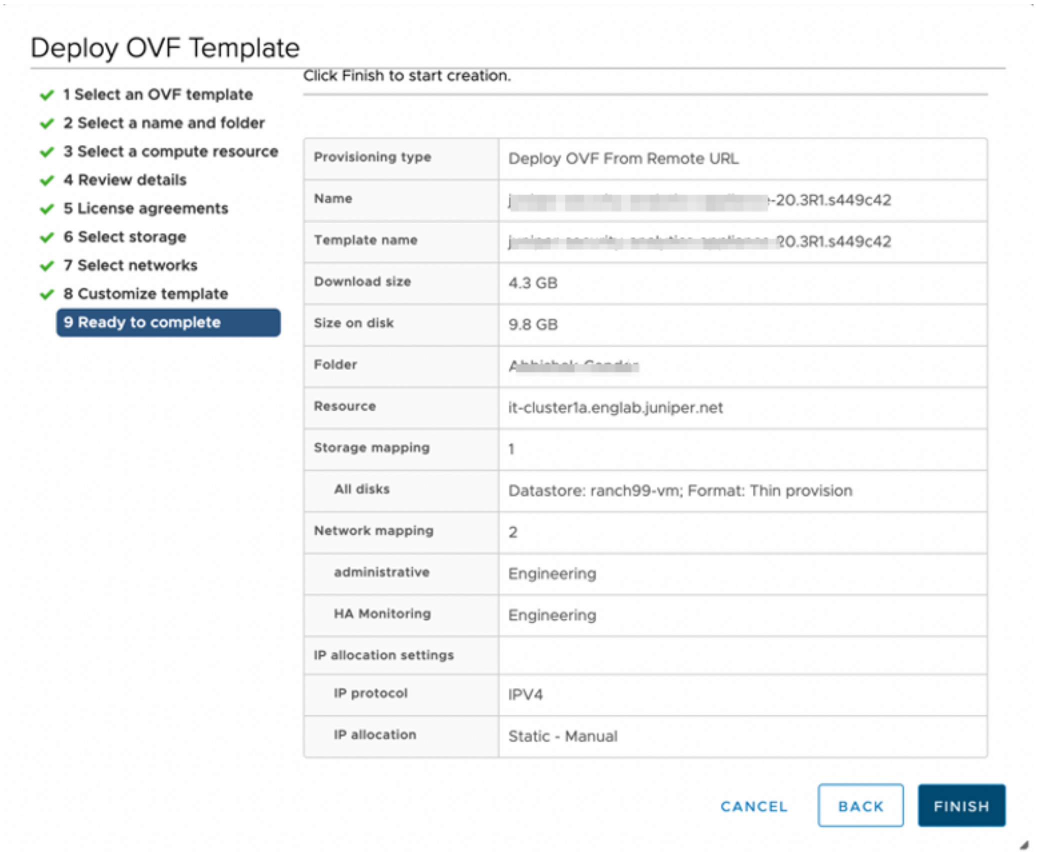
DNS address 2: Ignore this property if the IP allocation policy is DHCP.

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 5 on page 17.

Figure 5: Ready to Complete Page



Deploy OVF Template

Click Finish to start creation.

Provisioning type	Deploy OVF From Remote URL
Name	j[redacted]-20.3R1.s449c42
Template name	j[redacted]20.3R1.s449c42
Download size	4.3 GB
Size on disk	9.8 GB
Folder	[redacted]
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

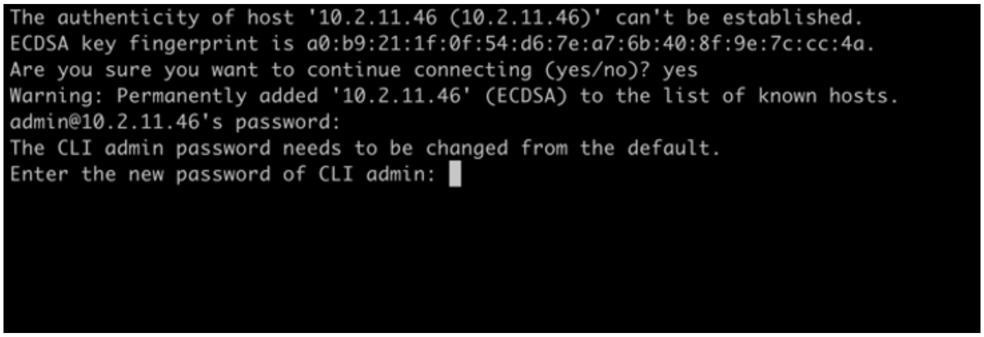
14. Verify all the details and click **Finish** to begin the OVA installation.

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 6 on page 18.

Figure 6: 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.

17. You must now add the Security Director Insights node to Junos Space by performing the following steps.

    - Log in to Security Director GUI and navigate to **Administration** > **Insights Management** > **Insights Nodes**.
    - Enter the Security Director Insights IP address and the admin password (from Step 16).
    - Click **Save** to complete integrating the Security Director Insights VM into Security Director.

    To know more about how to add Security Director Insights nodes, see *Add Insights Nodes*.

> **NOTE:** You can use the Security Director Insights VM as a log collector and as an integrated Policy Enforcer.

RELATED DOCUMENTATION

Add Security Director Insights as a Log Collector | 19

Configure Security Director Insights High Availability | 25

Security Director Insights High Availability Deployment Architecture | 23

Configure Policy Enforcer for Security Director Insights Mitigation | 39

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.

> **NOTE:** After you upgrade to Log Collector 21.3, you can access historical logs from the legacy log collector (Log Collector 20.1) by switching between both log collectors. 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 read-only log collector support to enable you to view existing data in the event viewer. For details, see Security Director Release Notes.

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
   ```

Table 3 on page 20 below lists the required specifications for deploying Security Director Insights as a log collector for various events per second (eps) rates.

Table 3: Specifications

Setup	CPU	Memory
5k	4	16
10k	8	16
15k	8	24
25k	16	32

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**.

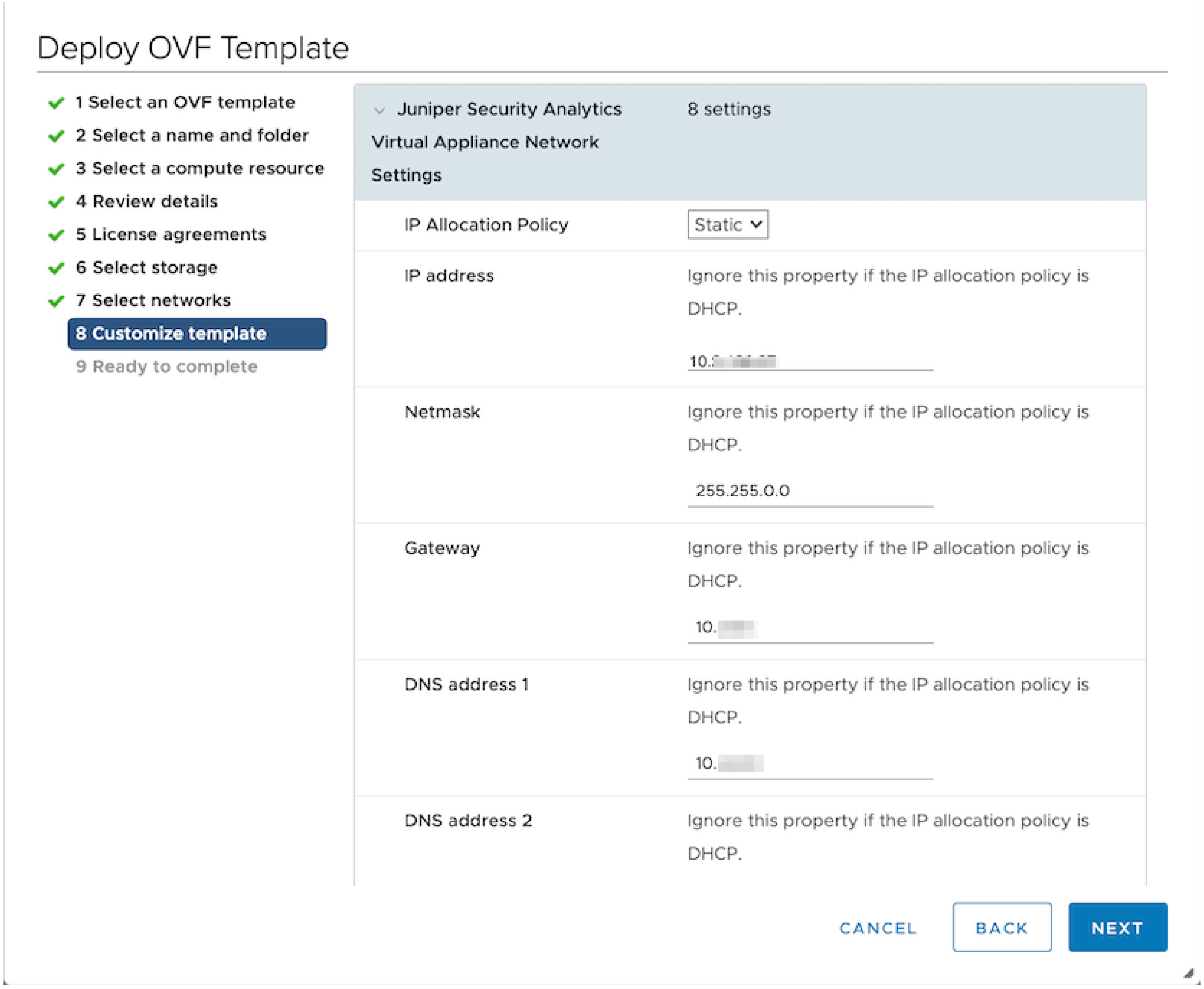
   The Add Collector Node page appears.

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 7 on page 21 and Figure 8 on page 22.

Figure 7: Deploy OVF Template Page



Juniper Security Analytics Virtual Appliance Network Settings — 8 settings

IP Allocation Policy: Static

IP address: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

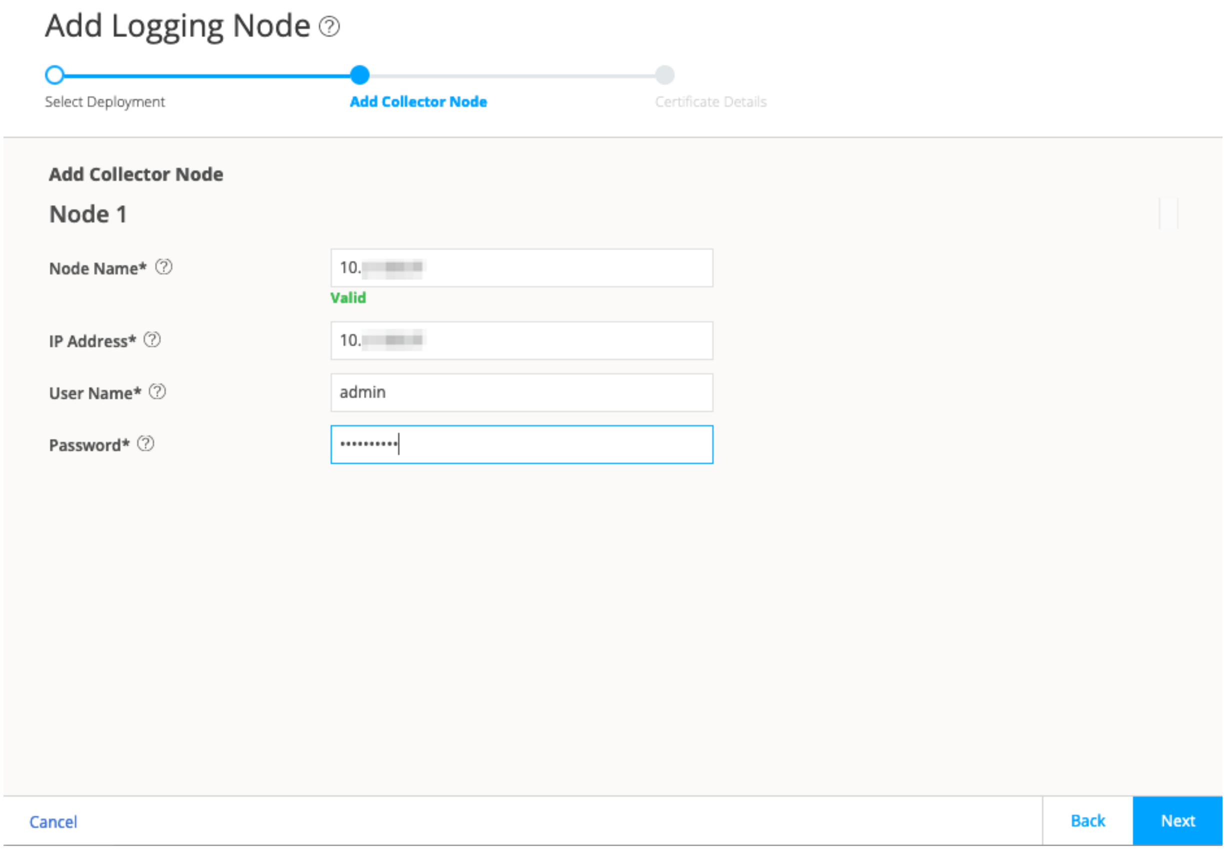
Netmask: Ignore this property if the IP allocation policy is DHCP.
255.255.0.0

Gateway: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

DNS address 1: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

DNS address 2: Ignore this property if the IP allocation policy is DHCP.

Figure 8: Add Logging Node Page



Add Collector Node

Node 1

Node Name*	10.[redacted] Valid
IP Address*	10.[redacted]
User Name*	admin
Password*	••••••••••

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.

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

NOTE:

- The log collector in Security Director Insights supports 25K events per second (eps).
- Disable the raw log: **user:Core#(applications)# set log-collector raw-log off**.
- Make sure that the SRX Series device configuration points to the corresponding SDI log collector.

RELATED DOCUMENTATION

Configure Security Director Insights High Availability | 25

Security Director Insights High Availability Deployment Architecture | 23

Configure Policy Enforcer for Security Director Insights Mitigation | 39

Security Director Insights High Availability Deployment Architecture

You can deploy Security Director Insights as a single node and as two nodes with high availability (HA).

Security Director Insights requires the following system and network configurations for the HA deployment:

- Two Security Director Insights systems for two nodes HA.
- Each system must have two network interfaces: one for management and another for HA monitoring.
- The IP addresses of the management interface of the two systems must be in the same subnet.
- The IP addresses of the HA monitoring interface of the two systems must be in the same subnet.

  The management and HA monitoring interfaces must be in different subnets.
- Virtual IP addresses for each subnet.

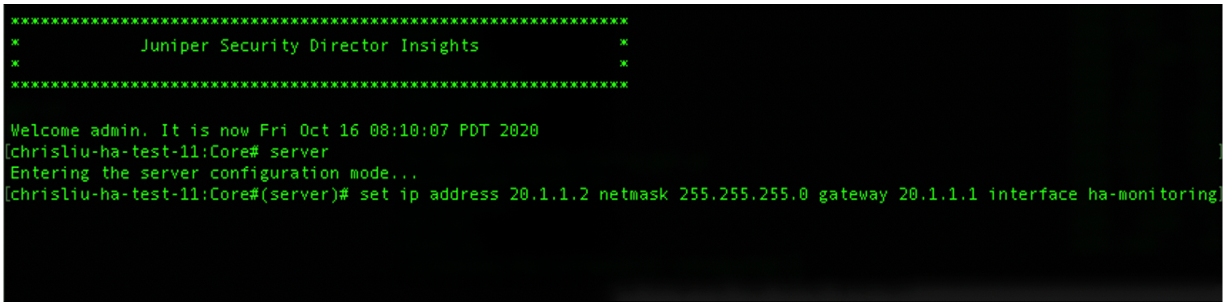
The following example shows the network configuration for the HA deployment:

- System 1:
  - Management IP: 10.1.1.2/24
  - HA monitoring IP: 20.1.1.2/24
- System 2:
  - Management IP: 10.1.1.3/24
  - HA monitoring IP: 20.1.1.3/24
- Virtual IP address for data traffic: 10.1.1.4/24
- Virtual IP address for HA monitoring: 20.1.1.4/24

The virtual IP addresses are used when you configure HA in the Security Director Insights GUI. The virtual IP addresses are automatically assigned to one of the systems, which becomes the active node. When failover occurs, the virtual IP addresses are automatically assigned to the other system, which is the standby node.

You can configure the HA monitoring IP address using a CLI command, as shown in Figure 9 on page 24.

Figure 9: HA Monitoring IP Address Configuration



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

Welcome admin. It is now Fri Oct 16 08:10:07 PDT 2020
[chrisliu-ha-test-11:Core# server                                                                                    ]
Entering the server configuration mode...
[chrisliu-ha-test-11:Core#(server)# set ip address 20.1.1.2 netmask 255.255.255.0 gateway 20.1.1.1 interface ha-monitoring]
```

RELATED DOCUMENTATION

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files | **12**

Configure Security Director Insights High Availability | **25**

Configure Policy Enforcer for Security Director Insights Mitigation | **39**

Add Security Director Insights as a Log Collector | **19**

Configure Security Director Insights High Availability

IN THIS SECTION

- Before You Begin | 25
- Enable HA | 27
- Manually Trigger Failover | 30
- Disable HA | 33
- Upgrade HA | 35

Security Director Insights supports two-node high availability (HA) with the following specifications:

- Once you enable HA, one Security Director Insights virtual machine (VM) becomes the active node and another Security Director Insights VM becomes the standby node.
- You must specify the virtual IP address assigned to the HA system to inject logs through the virtual IP address.
- If the active node is abnormal or down, the failover to the standby node occurs automatically. You need not change anything when you inject logs.

This topic explains how to setup Security Director Insights HA.

Before You Begin

Before you enable HA:

1. Read "Security Director Insights High Availability Deployment Architecture" on page 23.

   > **NOTE:** If you are using Policy Enforcer inside Security Director Insights and Policy Enforcer is not in HA, you must not deploy Security Director Insights in HA.

2. The two Security Director Insights VMs must have the same Security Director Insights software versions. In each Security Director Insights VM, configure the following network interfaces to enable HA:

   - Eth0—For normal Security Director Insights data and management

- Eth1—For HA monitoring

Without the HA feature, Security Director Insights VM requires only a single network interface, eth0, for data and management. The standard Security Director Insights OVA deployment configures only the eth0 interface.

3. Use the following procedure to configure IP addresses for the network interfaces:

   - Go to Security Director Insights CLI.

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

   - Enter the Settings menu.

     ```
     # server
     ```

   - View already configured IP addresses.

     ```
     # show ip
     ```

   - Configure the eth0 IP address.

     ```
     # set ip interface management address ${eth0_ip} gateway ${eth0_gateway} netmask ${eth0_netmask}
     ```

   - Configure the eth1 IP address.

     ```
     # set ip interface ha-monitoring address ${eth1_ip} gateway ${eth1_gateway} netmask
     ${eth1_netmask}
     ```

   - Verify the configured IP addresses.

     ```
     # show ip
     ```

     NOTE:

     You must ensure that:

     - On each node, the IP addresses of the eth0 and eth1 interfaces are in different subnets.
     - The IP address of the eth0 interface of the active and standby nodes are in the same subnet.
     - The IP address of the eth1 interface of the active and standby nodes are in the same subnet.

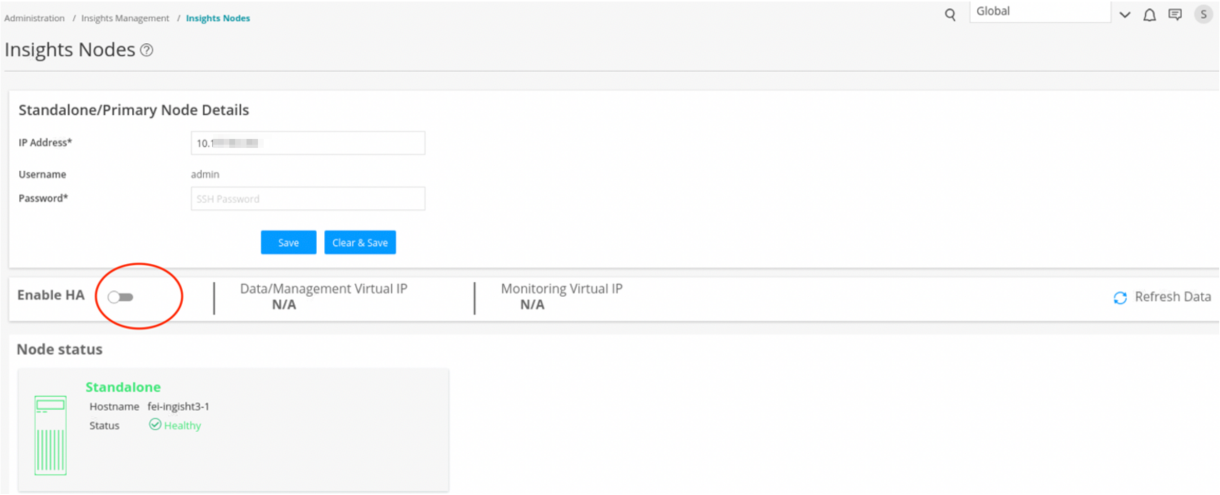
Enable HA

Before you enable HA, you must add the active node.

1. To add the active node:
   - Select **Security Director** > **Administration** > **Insights Management** > **Insights Nodes**.

     The Insights Nodes page appears.
   - Enter the IP address of the active node, admin password, and click **Save**.
2. Once the active node is added successfully, toggle the Enable HA option on, as shown in Figure 10 on page 27.

Figure 10: Enable HA



Standalone/Primary Node Details

IP Address* 10.1[redacted]

Username admin

Password* SSH Password

Enable HA

Data/Management Virtual IP N/A

Monitoring Virtual IP N/A

Node status

Standalone

Hostname fei-ingisht3-1

Status Healthy

   The HA Setup page appears.

3. Complete the configuration according to the guidelines provided in Table 4 on page 27, and click **Save & Enable**.

Table 4: Fields on the HA Setup Page

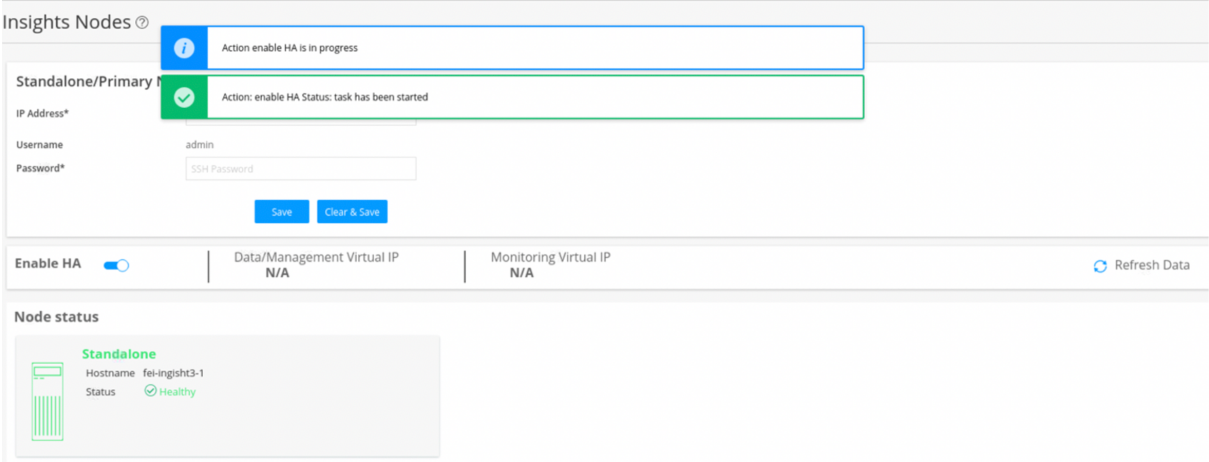
Setting	Guideline
Secondary Node Details	
Secondary system IP	Enter the IP address of the eth0 interface of the standby node.
Username	Username is “admin” and you cannot modify it.
Password	Enter the Security Director Insights VM password.

Table 4: Fields on the HA Setup Page *(continued)*

Setting	Guideline
HA Settings	
Data Virtual IP/Netmask	Enter the virtual IP address of the HA management interface.
HA monitor Virtual IP/Netmask	Enter the virtual IP address of the HA monitoring interface.
Ping IPs	(Optional) Enter one or more IP addresses that both nodes can reach to check the connectivity.

You are taken back to the Insights Nodes page. You will see the status messages, as shown in Figure 11 on page 28. Note that the HA enabling takes several minutes.

Figure 11: Enable HA in Progress



Insights Nodes

Action enable HA is in progress

Action: enable HA Status: task has been started

Standalone/Primary N

IP Address*

Username admin

Password* SSH Password

Enable HA

Data/Management Virtual IP N/A

Monitoring Virtual IP N/A

Node status

Standalone

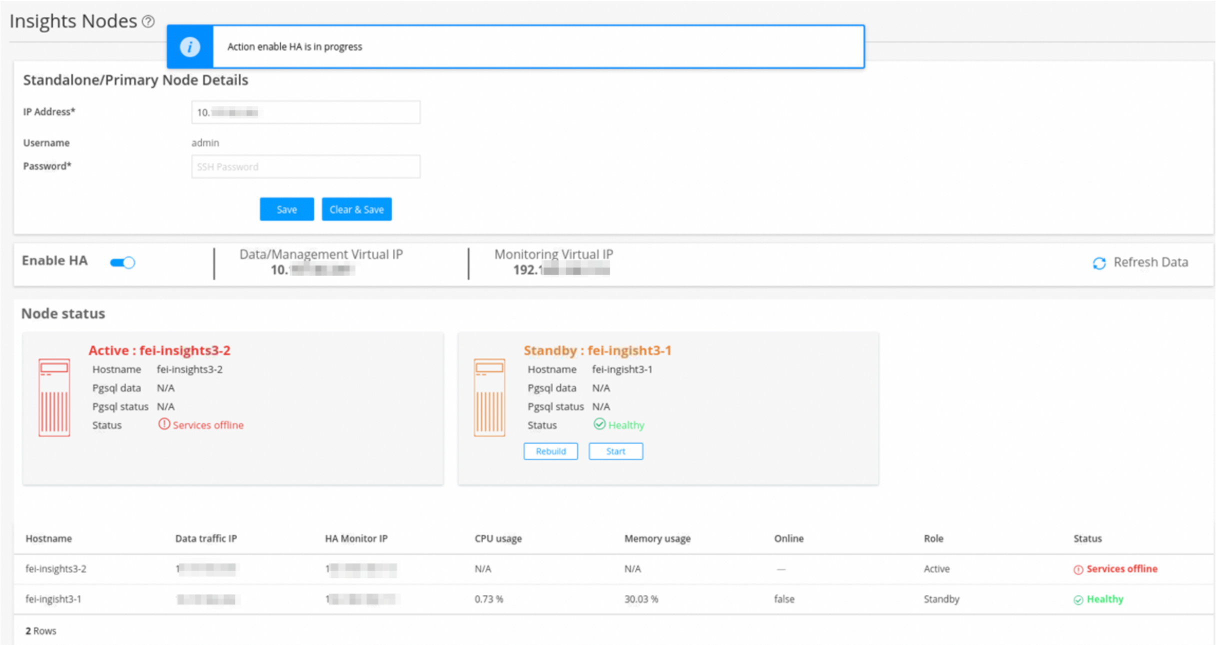
Hostname fei-ingisht3-1

Status Healthy

4. Click **Refresh Data**.

   You will see intermittent status messages, as shown in Figure 12 on page 29.

Figure 12: Enable HA Intermittent Status



Insights Nodes

Action enable HA is in progress

Standalone/Primary Node Details

IP Address* 10.[redacted]

Username admin

Password* SSH Password

Enable HA | Data/Management Virtual IP 10.[redacted] | Monitoring Virtual IP 192.1[redacted] | Refresh Data

Node status

Active : fei-insights3-2
Hostname fei-insights3-2
Pgsql data N/A
Pgsql status N/A
Status Services offline

Standby : fei-ingisht3-1
Hostname fei-ingisht3-1
Pgsql data N/A
Pgsql status N/A
Status Healthy

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-insights3-2	1[redacted]	1[redacted]	N/A	N/A	—	Active	Services offline
fei-ingisht3-1	[redacted]	1[redacted]	0.73 %	30.03 %	false	Standby	Healthy

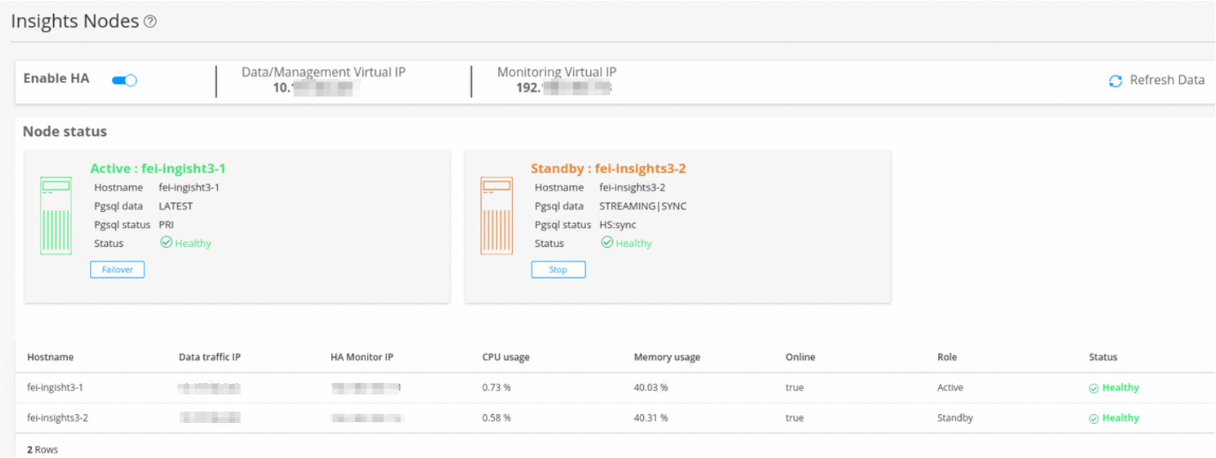
2 Rows

5. Keep clicking the **Refresh Data** option until you see that:

   - Both nodes are healthy.
   - Data and management virtual IP addresses are the same as the ones configured on the HA Setup page.

   Figure 13 on page 29 shows the status of the nodes once the HA is enabled successfully.

Figure 13: HA Enabled



Insights Nodes

Enable HA | Data/Management Virtual IP 10.[redacted] | Monitoring Virtual IP 192.[redacted] | Refresh Data

Node status

Active : fei-ingisht3-1
Hostname fei-ingisht3-1
Pgsql data LATEST
Pgsql status PRI
Status Healthy

Standby : fei-insights3-2
Hostname fei-insights3-2
Pgsql data STREAMING|SYNC
Pgsql status HS:sync
Status Healthy

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-ingisht3-1	[redacted]	[redacted]	0.73 %	40.03 %	true	Active	Healthy
fei-insights3-2	[redacted]	[redacted]	0.58 %	40.31 %	true	Standby	Healthy

2 Rows

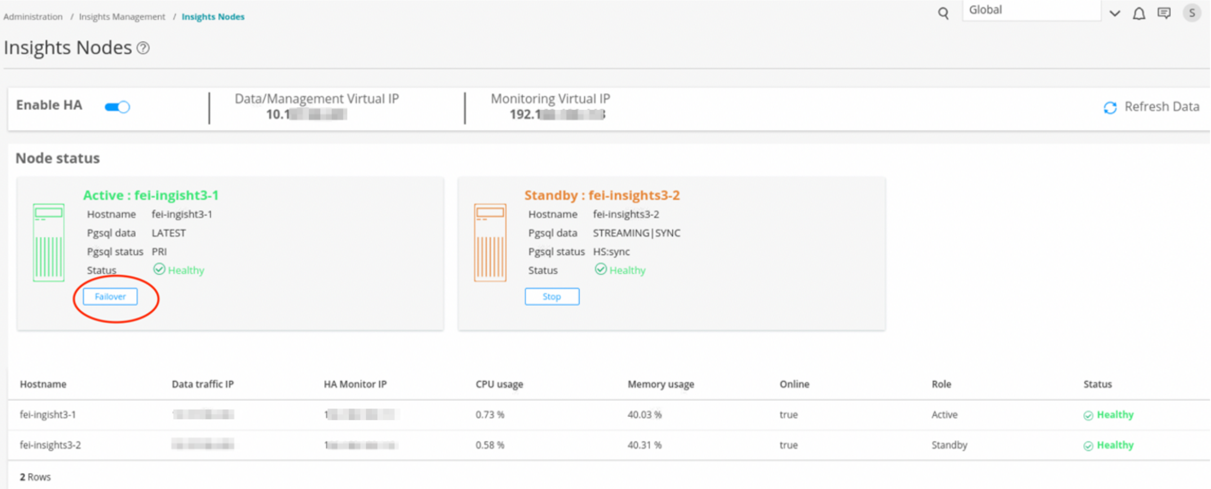
Manually Trigger Failover

You can initialize the HA failover if the active node encounters any issues.

To enable failover to the standby node:

1. In the Insights Node page, click **Failover** under the active node, as shown in Figure 14 on page 30.

Figure 14: Initiate Failover



Insights Nodes

Enable HA

Data/Management Virtual IP
10.1[redacted]

Monitoring Virtual IP
192.1[redacted]

Node status

Active : fei-ingisht3-1

Hostname	fei-ingisht3-1
Pgsql data	LATEST
Pgsql status	PRI
Status	✓ Healthy

Standby : fei-insights3-2

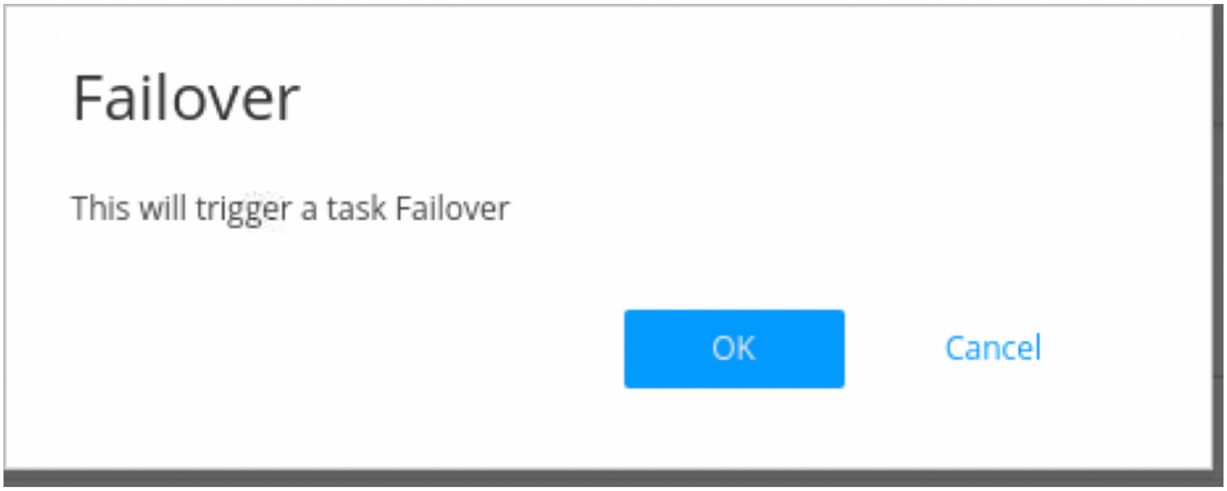
Hostname	fei-insights3-2
Pgsql data	STREAMING|SYNC
Pgsql status	HS:sync
Status	✓ Healthy

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-ingisht3-1	[redacted]	1[redacted]	0.73 %	40.03 %	true	Active	✓ Healthy
fei-insights3-2	[redacted]	1[redacted]	0.58 %	40.31 %	true	Standby	✓ Healthy

2 Rows

A confirmation message appears, as shown in Figure 15 on page 30.

Figure 15: Failover Confirmation Message



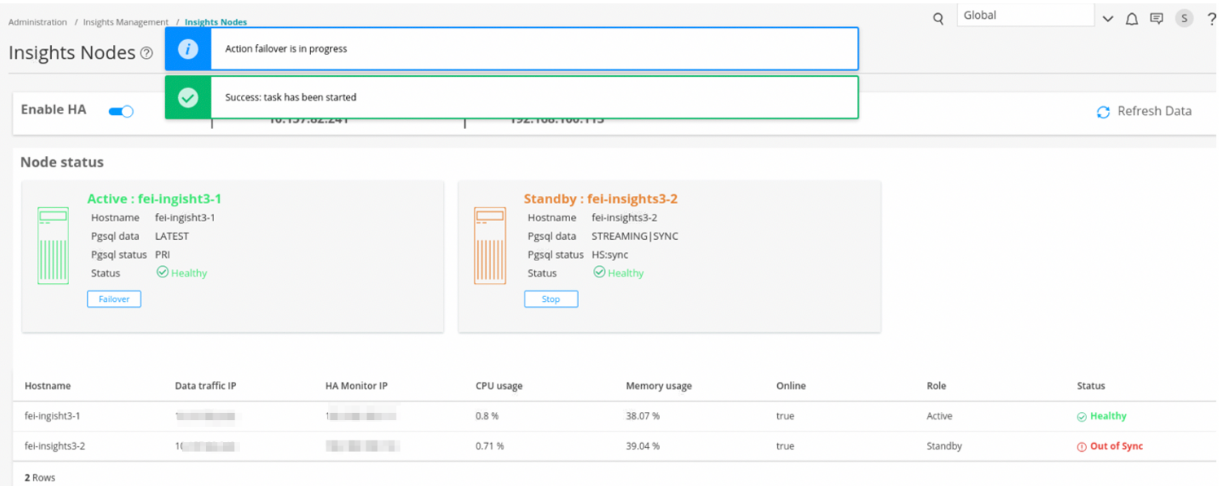
Failover

This will trigger a task Failover

2. Click **OK**.

The failover action takes several minutes to complete. During the process, you will see intermittent status messages, as shown in Figure 16 on page 31.

Figure 16: Failover Intermittent Status



Action failover is in progress

Success: task has been started

Enable HA

Node status

Active : fei-ingisht3-1
Hostname fei-ingisht3-1
Pgsql data LATEST
Pgsql status PRI
Status ✓ Healthy

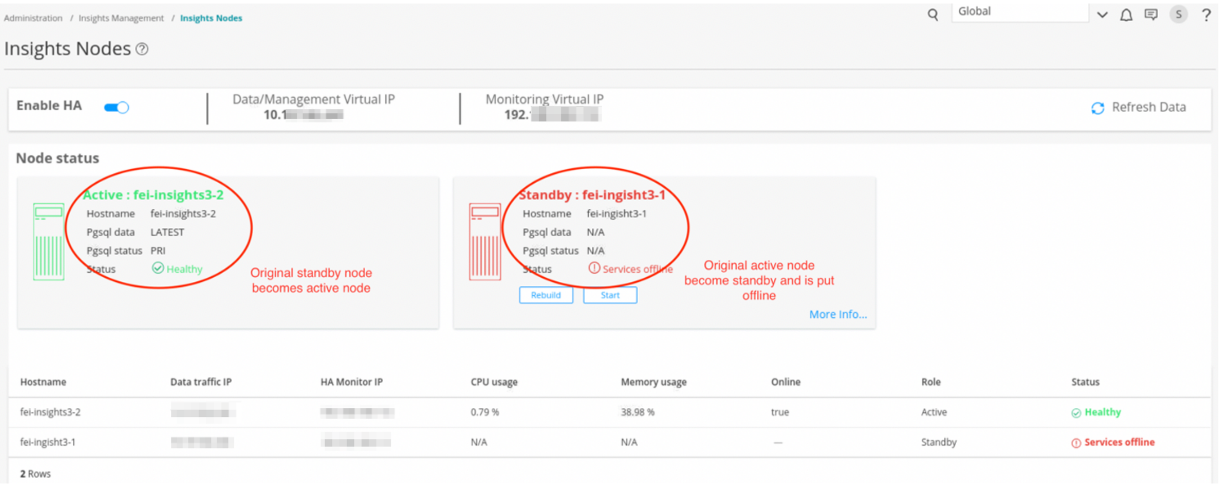
Standby : fei-insights3-2
Hostname fei-insights3-2
Pgsql data STREAMING|SYNC
Pgsql status HS:sync
Status ✓ Healthy

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-ingisht3-1	[redacted]	[redacted]	0.8 %	38.07 %	true	Active	✓ Healthy
fei-insights3-2	[redacted]	[redacted]	0.71 %	39.04 %	true	Standby	ⓘ Out of Sync

2 Rows

Once the failover is enabled, the original standby node becomes the new active node and the original active node is put in an offline mode, as shown in Figure 17 on page 31.

Figure 17: Standby Node Offline



Enable HA

Data/Management Virtual IP
10.1[redacted]

Monitoring Virtual IP
192.[redacted]

Node status

Active : fei-insights3-2
Hostname fei-insights3-2
Pgsql data LATEST
Pgsql status PRI
Status ✓ Healthy

Original standby node becomes active node

Standby : fei-ingisht3-1
Hostname fei-ingisht3-1
Pgsql data N/A
Pgsql status N/A
Status ⓘ Services offline

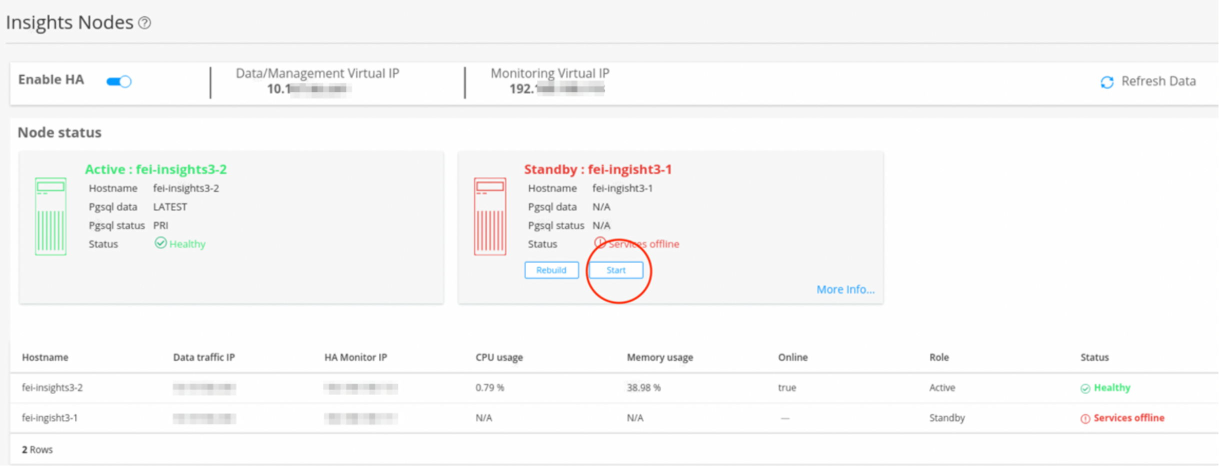
Original active node become standby and is put offline

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-insights3-2	[redacted]	[redacted]	0.79 %	38.98 %	true	Active	✓ Healthy
fei-ingisht3-1	[redacted]	[redacted]	N/A	N/A	—	Standby	ⓘ Services offline

2 Rows

3. To bring the new standby node back online, click **Start**, as shown in Figure 18 on page 32.

Figure 18: Start Standby Node



Insights Nodes

Enable HA

Data/Management Virtual IP 10.1[redacted]

Monitoring Virtual IP 192.[redacted]

Node status

Active : fei-insights3-2

Hostname fei-insights3-2

Pgsql data LATEST

Pgsql status PRI

Status ✓ Healthy

Standby : fei-ingisht3-1

Hostname fei-ingisht3-1

Pgsql data N/A

Pgsql status N/A

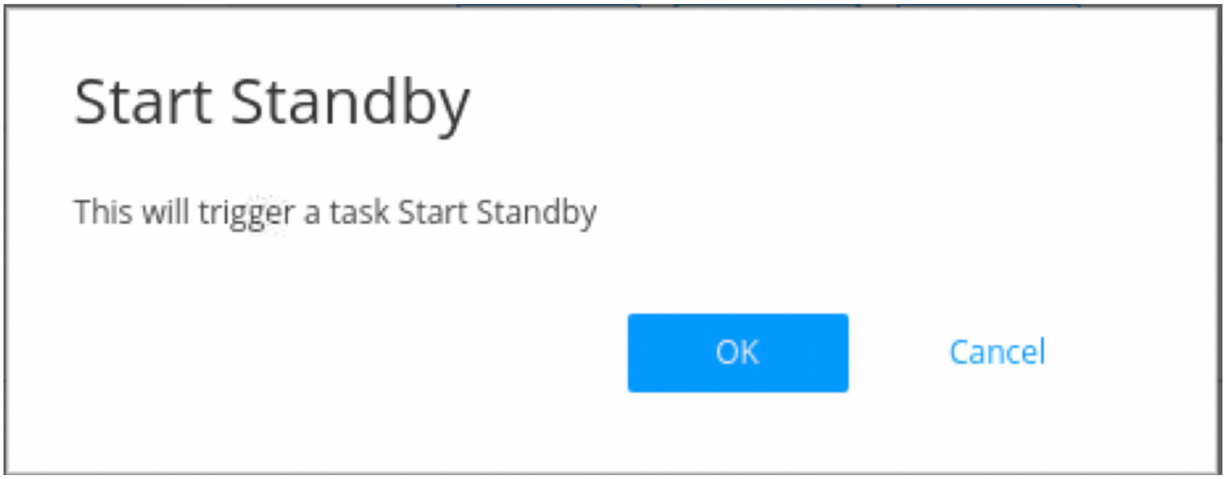
Status ⓘ Services offline

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-insights3-2	[redacted]	[redacted]	0.79 %	38.98 %	true	Active	✓ Healthy
fei-ingisht3-1	[redacted]	[redacted]	N/A	N/A	—	Standby	ⓘ Services offline

2 Rows

A confirmation message appears, as shown in Figure 19 on page 32.

Figure 19: Start Standby Confirmation



Start Standby

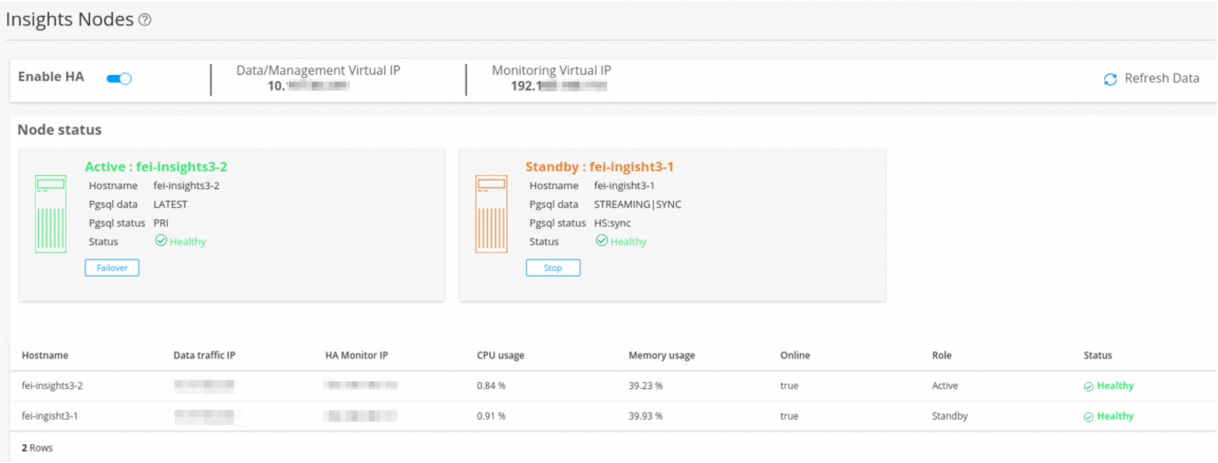
This will trigger a task Start Standby

4. Click **OK** to continue.

   The Start action takes several minutes to complete.

   Once the Start action is complete, the status of both the nodes shows online and healthy. The original active node is now online as a standby node, as shown in Figure 20 on page 33.

Figure 20: Standby Start Action



Insights Nodes

Enable HA

Data/Management Virtual IP
10.[redacted]

Monitoring Virtual IP
192.1[redacted]

Refresh Data

Node status

Active : fei-insights3-2

Hostname fei-insights3-2
Pgsql data LATEST
Pgsql status PRI
Status Healthy

Failover

Standby : fei-ingisht3-1

Hostname fei-ingisht3-1
Pgsql data STREAMING|SYNC
Pgsql status HS:sync
Status Healthy

Stop

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-insights3-2	[redacted]	[redacted]	0.84 %	39.23 %	true	Active	Healthy
fei-ingisht3-1	[redacted]	[redacted]	0.91 %	39.93 %	true	Standby	Healthy

2 Rows

5. If the standby node encounters any synchronization issues with the active node, click **Stop** under the Standby node.

6. Click **Rebuild** to synchronize data between the two nodes.

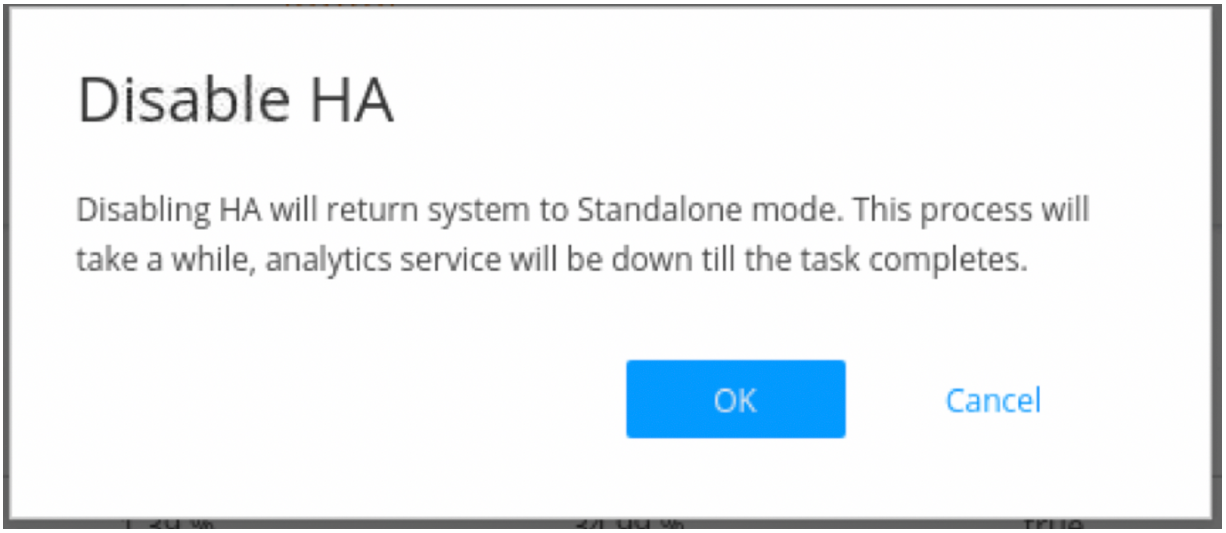
Disable HA

To disable HA:

1. In the Insights Nodes page, toggle the Enable HA option off.

   A confirmation message appears before HA is disabled, as shown in Figure 21 on page 34.

Figure 21: Disable HA Confirmation



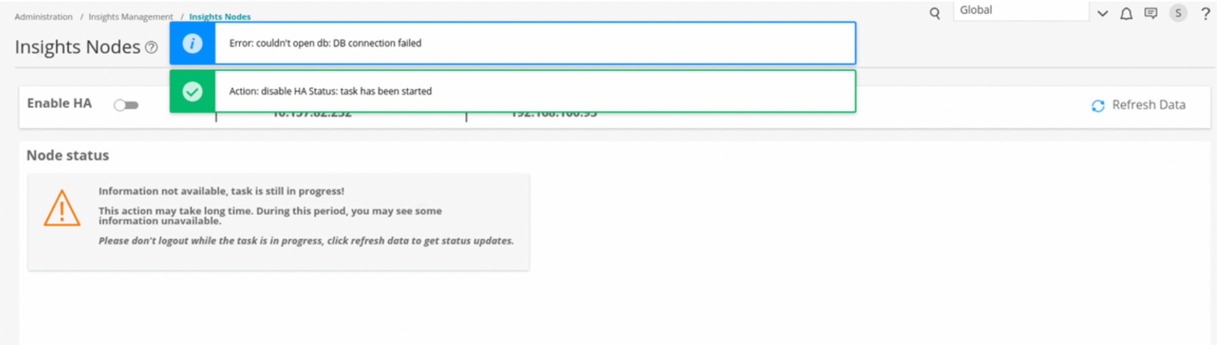
Disable HA

Disabling HA will return system to Standalone mode. This process will take a while, analytics service will be down till the task completes.

2. Click **OK** to confirm the HA disabling.

Disabling HA takes several minutes. During the process, intermittent status messages are displayed, as shown in Figure 22 on page 34. Keep clicking **Refresh Data** until HA is disabled successfully.

Figure 22: HA Disabling Status



Error: couldn't open db: DB connection failed

Action: disable HA Status: task has been started

Node status

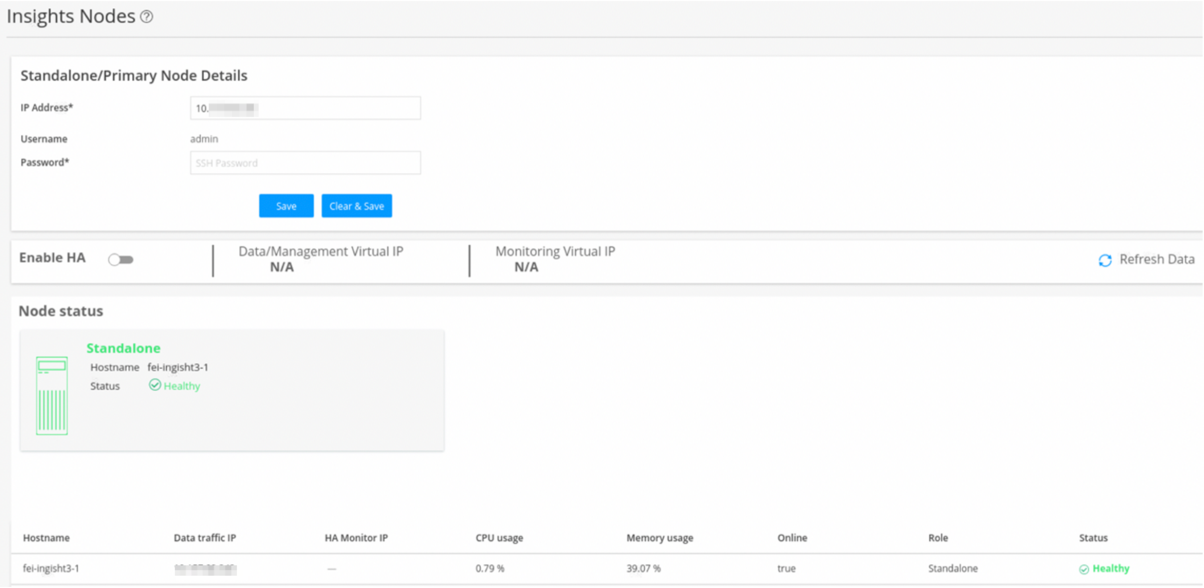
Information not available, task is still in progress!

This action may take long time. During this period, you may see some information unavailable.

Please don't logout while the task is in progress, click refresh data to get status updates.

Once HA is disabled successfully, you can see only the active node VM in the Insights Nodes page, as shown in Figure 23 on page 35.

Figure 23: HA Disabled



Insights Nodes

Standalone/Primary Node Details

IP Address*: 10.[redacted]

Username: admin

Password*: SSH Password

Enable HA

Data/Management Virtual IP: N/A

Monitoring Virtual IP: N/A

Node status

Standalone

Hostname: fei-ingisht3-1

Status: Healthy

Hostname	Data traffic IP	HA Monitor IP	CPU usage	Memory usage	Online	Role	Status
fei-ingisht3-1	[redacted]	—	0.79 %	39.07 %	true	Standalone	Healthy

Upgrade HA

When a new Security Director Insights software version is available, perform the following procedure to upgrade the HA nodes. You must upgrade HA only from the active node for both the nodes to be upgraded.

1. Go to Security Director Insights CLI.

   ssh admin@${active_node_ip}

2. Enter the Settings menu.

   #server

3. Obtain the software upgrade package.

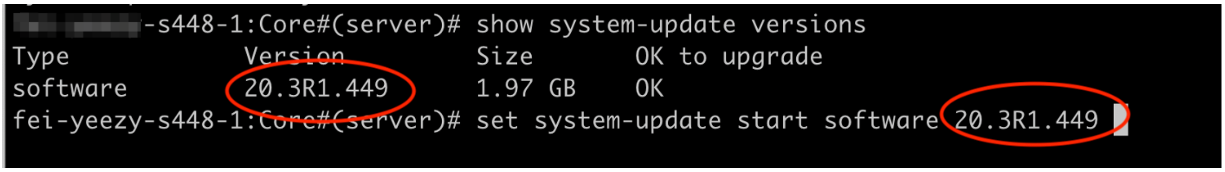
   #set system-update copy user@${pkg_location_ip}:/${package_file_path/name}

4. View the software upgrade package version.

   # show system-update versions

5. Initiate the upgrade.

# set system-update start software ${new_version}



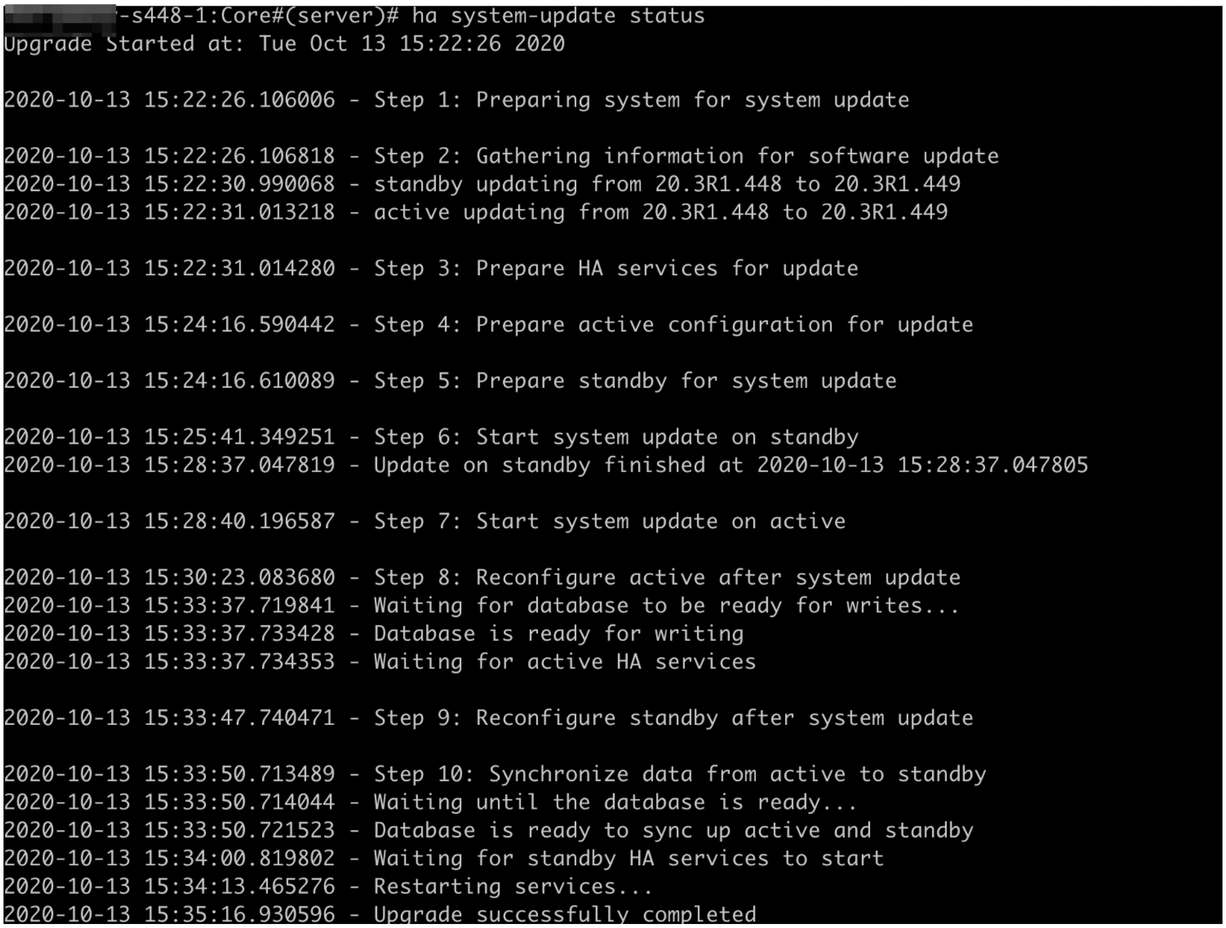
```
[redacted]-s448-1:Core#(server)# show system-update versions
Type              Version           Size        OK to upgrade
software          20.3R1.449        1.97 GB     OK
fei-yeezy-s448-1:Core#(server)# set system-update start software 20.3R1.449
```

6. Verify the HA upgrade status.

   # ha system-update status

   Wait until the upgrade is finished successfully in both active and standby nodes, as shown in Figure 24 on page 36.

Figure 24: HA Upgrade



```
[redacted]-s448-1:Core#(server)# ha system-update status
Upgrade Started at: Tue Oct 13 15:22:26 2020

2020-10-13 15:22:26.106006 - Step 1: Preparing system for system update

2020-10-13 15:22:26.106818 - Step 2: Gathering information for software update
2020-10-13 15:22:30.990068 - standby updating from 20.3R1.448 to 20.3R1.449
2020-10-13 15:22:31.013218 - active updating from 20.3R1.448 to 20.3R1.449

2020-10-13 15:22:31.014280 - Step 3: Prepare HA services for update

2020-10-13 15:24:16.590442 - Step 4: Prepare active configuration for update

2020-10-13 15:24:16.610089 - Step 5: Prepare standby for system update

2020-10-13 15:25:41.349251 - Step 6: Start system update on standby
2020-10-13 15:28:37.047819 - Update on standby finished at 2020-10-13 15:28:37.047805

2020-10-13 15:28:40.196587 - Step 7: Start system update on active

2020-10-13 15:30:23.083680 - Step 8: Reconfigure active after system update
2020-10-13 15:33:37.719841 - Waiting for database to be ready for writes...
2020-10-13 15:33:37.733428 - Database is ready for writing
2020-10-13 15:33:37.734353 - Waiting for active HA services

2020-10-13 15:33:47.740471 - Step 9: Reconfigure standby after system update

2020-10-13 15:33:50.713489 - Step 10: Synchronize data from active to standby
2020-10-13 15:33:50.714044 - Waiting until the database is ready...
2020-10-13 15:33:50.721523 - Database is ready to sync up active and standby
2020-10-13 15:34:00.819802 - Waiting for standby HA services to start
2020-10-13 15:34:13.465276 - Restarting services...
2020-10-13 15:35:16.930596 - Upgrade successfully completed
```

RELATED DOCUMENTATION

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files | 12
Configure Policy Enforcer for Security Director Insights Mitigation | 39
Add Security Director Insights as a Log Collector | 19
Security Director Insights High Availability Deployment Architecture | 23

Configure High Availability for Security Director Insights as Log Collector

Starting in Security Director Insights Release 21.3, you can configure high availability (HA) for Security Director Insights as log collector.

To configure HA for the log collector:

1. Enable the log collector function in two nodes of Security Director Insights through Security Director Insights CLI terminal.

   a. Go to Security Director Insights CLI.

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

   b. Enter the application CLI menu.

      # applications

   c. Enable the log collector.

      # set log-collector enable on

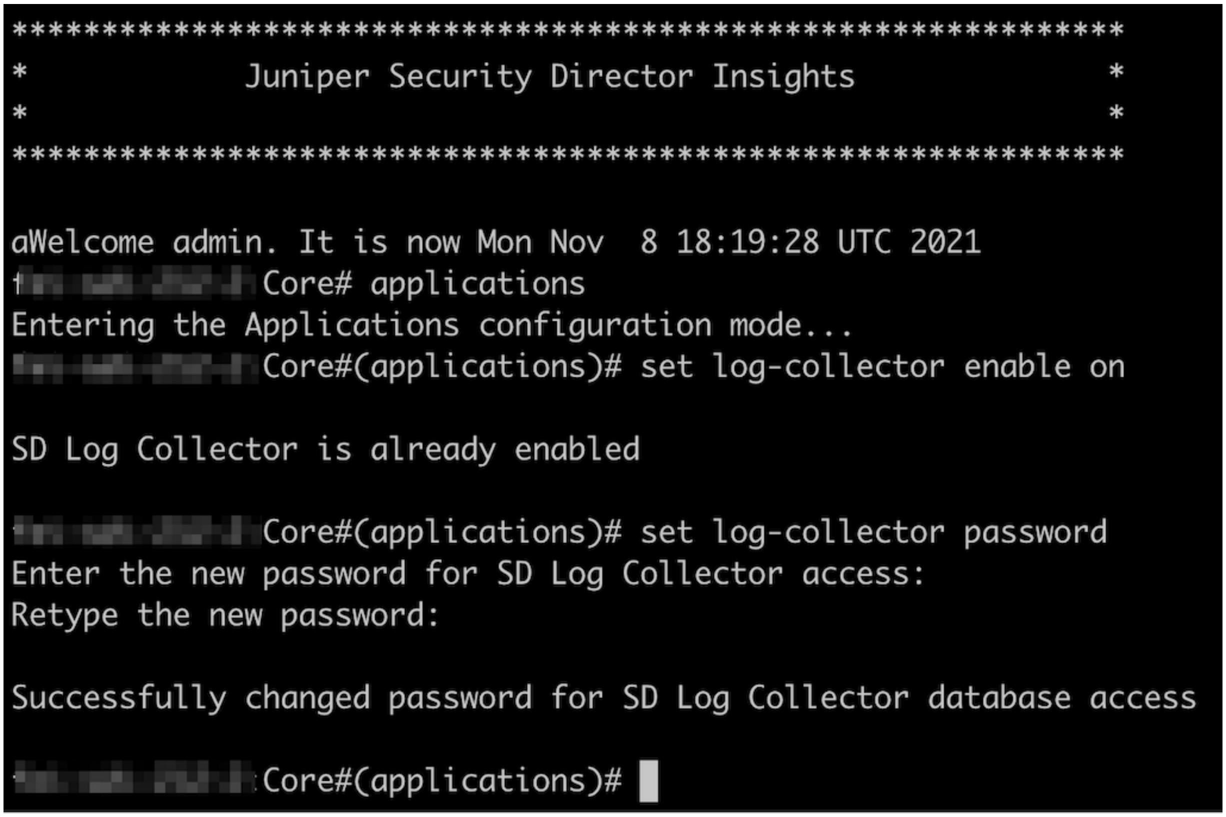
   d. Set the log collector password.

      # set log-collector password

   e. Retype the new password.

      You will receive the password change success message as shown in Figure 25 on page 38.

Figure 25: Enable Log Collector



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

aWelcome admin. It is now Mon Nov  8 18:19:28 UTC 2021
[redacted]Core# applications
Entering the Applications configuration mode...
[redacted]Core#(applications)# set log-collector enable on

SD Log Collector is already enabled

[redacted]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

[redacted]Core#(applications)# █
```

2. Enable the Security Director Insights HA through Security Director Insights CLI terminal.

   a. Go to Security Director Insights CLI.

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

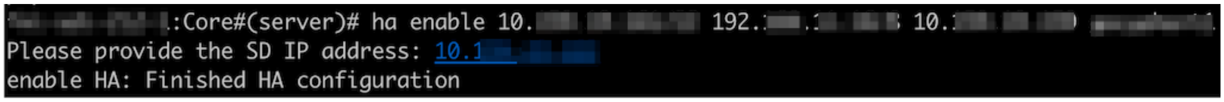
   b. Enable HA.

      ha enable ${VIP_data_interface}/${VIP_data_subnet} ${VIP_monitoring_interface}/{VIP_monitoring_subet} ${secondary_node_data_interface_ip} ${secondary_node_admin_password}

   c. Provide the Security Director IP address.

      HA is enabled and a confirmation message is shown, as shown in Figure 26 on page 38.

Figure 26: Enable HA



```
[redacted]:Core#(server)# ha enable 10.[redacted] 192.[redacted] 10.[redacted] [redacted]
Please provide the SD IP address: 10.1[redacted]
enable HA: Finished HA configuration
```

3. Add the HA virtual IP address as a log collector in Security Director UI.

a. Select **Security Director** > **Administration** > **Logging Management** > **Logging Node**.

b. Click the + icon to add logging nodes.

   The Add Logging Node page appears.

c. Choose the Log Collector type as Security Director Log Collector, and click **Next**.

d. In the IP Address field, enter the HA virtual IP address.

e. In the Username field, enter ’admin’.

f. In the Password field, enter the log collector password that you have configured in Step 1d.

g. Click **Next**.

   The certificate details are displayed.

h. Click **Finish**.

i. Review the summary of configuration changes from the summary page.

j. Click OK to add the node.

RELATED DOCUMENTATION

Configure Security Director Insights High Availability | **25**

Add Security Director Insights as a Log Collector | **19**

Configure Policy Enforcer for Security Director Insights Mitigation

IN THIS SECTION

- Add Security Director Insights Nodes | **40**
- Configure Security Director Insights as Integrated Policy Enforcer | **40**
- Create Custom Feeds for Mitigation | **44**
- Configure Security Director Insights Mitigation Using Policy Enforcer | **44**
- Monitor Mitigation Through Policy Enforcer | **45**

Security Director Insights performs mitigation using Juniper® Advanced Threat Prevention Cloud (Juniper ATP Cloud) or Policy Enforcer. This topic explains how to configure Policy Enforcer for mitigation. Policy Enforcer is integrated within the Security Director Insights virtual machine (VM). You can mitigate the IP addresses with either the Security Director Insights integrated Policy Enforcer or the legacy standalone Policy Enforcer. If you are using the integrated Policy Enforcer for mitigation, use the IP address of the Security Director Insights VM wherever Policy Enforcer details need to be entered.

Add Security Director Insights Nodes

To add the Security Director Insights node:

1. Log in to the Security Director GUI and navigate to **Administration** > **Insights Management** > **Insights Nodes**.

2. Enter the Security Director Insights IP address and the admin password.

3. Click **Save**.

   The Security Director Insights VM is added to Security Director. To know more about adding Security Director Insights nodes, see *Add Insights Nodes*.

Configure Security Director Insights as Integrated Policy Enforcer

To configure the integrated Policy Enforcer:

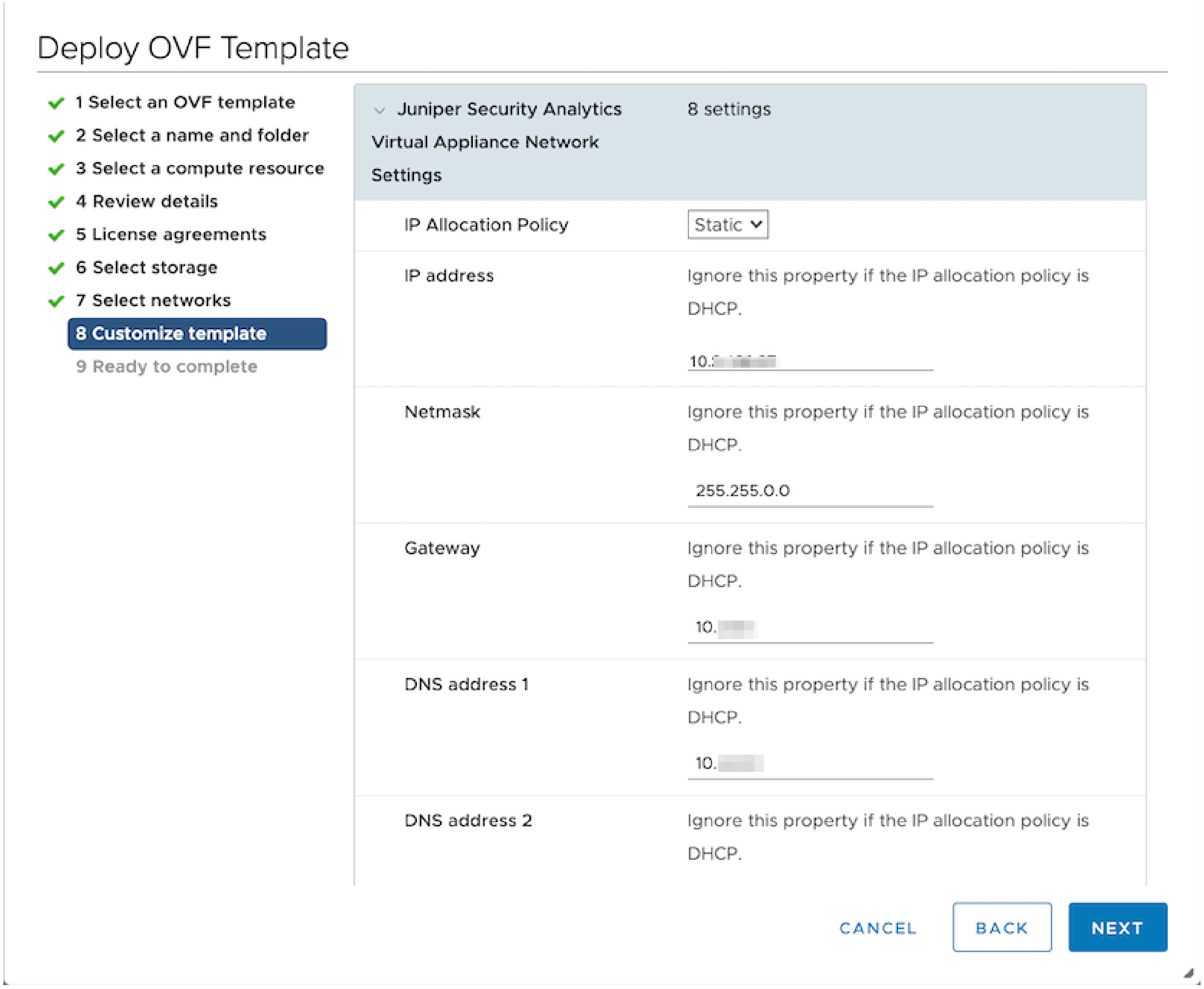
1. Select **Security Director** > **Administration** > **Policy enforcer** > **Settings**.

   The Settings page appears.

2. 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 Settings page, as shown in Figure 27 on page 41 and Figure 28 on page 42.

Figure 27: 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 Virtual Appliance Network Settings — 8 settings

IP Allocation Policy: Static

IP address: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

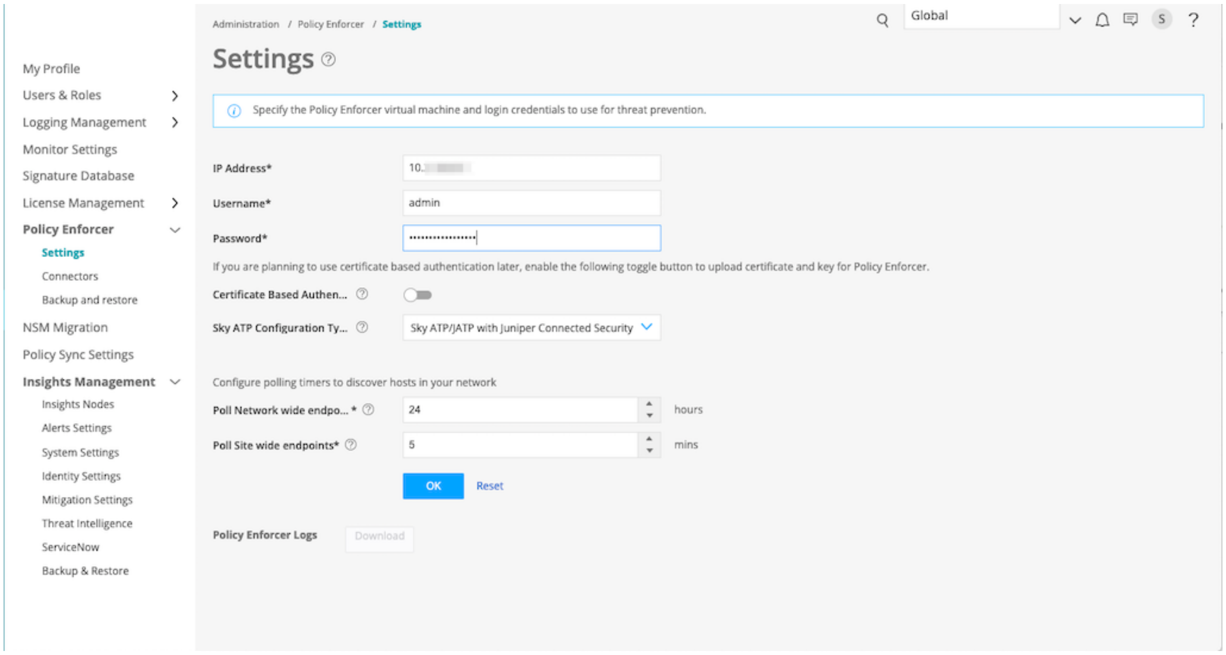
Netmask: Ignore this property if the IP allocation policy is DHCP.
255.255.0.0

Gateway: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

DNS address 1: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

DNS address 2: Ignore this property if the IP allocation policy is DHCP.

Figure 28: Policy Enforcer Settings Page



Settings

Specify the Policy Enforcer virtual machine and login credentials to use for threat prevention.

IP Address* 10.[redacted]

Username* admin

Password* ••••••••••••••••

If you are planning to use certificate based authentication later, enable the following toggle button to upload certificate and key for Policy Enforcer.

Certificate Based Authen...

Sky ATP Configuration Ty... Sky ATP/JATP with Juniper Connected Security

Configure polling timers to discover hosts in your network

Poll Network wide endpo...* 24 hours

Poll Site wide endpoints* 5 mins

Policy Enforcer Logs

3. In the Username field, enter “admin” as the username for the integrated Policy Enforcer.

4. In the Password field, enter the admin password that you used to bring up the Security Director Insights VM.

5. In the SkyATP Configuration Type field, select **Sky ATP/JATP with Juniper Connected Security** from the list and click **OK**.

   A confirmation page appears displaying the Policy Enforcer configuration success message and to confirm setting up the threat prevention policy.

6. Click **OK**.

   The Threat Prevention Policy Guided Setup page appears.

7. Click **Start Setup**.

8. In the Tenants page, do not create any tenants. Skip this step and click **Next**.

   The Security Fabric page appears.

9. In the Security Fabric page, perform the following configuration:

   - Select an existing site or click **+** to create a new site.

- In the Enforcement Point column, click **Add Enforcement Point** to add the SRX Series device as an enforcement point. This enables the SRX Series device to receive feeds from Security Director Insights.
- Click **Next**.

  The Policy Enforcement Group page appears.

10. In the Policy Enforcement Group page, perform the following configuration:
    - Click **+** to create a new policy enforcement group or use an existing group.
    - Click **Next**.

      The SkyATP Realm page appears.

11. In the SkyATP Realm page, perform the following configuration:
    - Click **+** and enter the existing ATP Cloud realm credentials. If you do not have the credentials, you will get an option to create the ATP Cloud realm credentials.
    - Click **OK**.

      If the ATP Cloud realm is added successfully, assign a site in the Sites Assigned column.

    - Click **Next**.

      The Policies page appears.

12. In the Policies page, perform the following configuration:
    - Click **+** to create a threat prevention policy.
    - In the Name field, enter a name for the policy and description in the Description field.
    - In the Profiles section, select the following profiles: Include C&C profile in policy, Include infected host profile in policy, and Include malware profile in policy.
    - Click **OK**.

      You are taken back to the Policies page.

    - Click **Next**.

      The Geo IP page appears.

13. In the Geo IP page, skip the configuration and click **Finish**.

    The Summary page appears.

14. Review the configuration summary and click **OK**.

    A new threat prevention policy is created.

Create Custom Feeds for Mitigation

To mitigate incidents through Policy Enforcer, you must create custom feeds for blocklist and infected host.

To create the Policy Enforcer custom feeds:

1. Select **Security Director** > **Configure** > **Threat Prevention** > **Feed Sources** > **Custom Feeds**.

2. Click **Create** and select **Feeds with local files** from the drop-down list.

   The Create local custom feed page appears.

3. In the Name field, enter a name for the custom feed and description in the Description field.

4. From the Feed Type drop-down list, select **Blacklist**.

5. From the Zones/Realms drop-down list, select the Juniper ATP Cloud realm you created using the Guided Setup.

6. From the User Input Type drop-down list, select **IP, Subnet and Range**.

7. Click **OK**.

   A new custom feed for blocklist is created and you are taken back to the Custom Feeds page.

8. Repeat Steps 1 to 7 to create another custom feed for the infected host. In the Feed Type field, select **Infected-Hosts** from the list.

You will see two new custom feeds listed on the Custom Feeds page: one for blocklist and one for infected host.

Configure Security Director Insights Mitigation Using Policy Enforcer

To configure mitigation settings using Policy Enforcer:

1. Select **Security Director** > **Administration** > **Insights Management** > **Mitigation Settings**.

   The Mitigation Settings page appears.

2. Select the **Policy Enforcer** tab.

3. Complete the configuration by using the guidelines in Table 5 on page 45.

4. Click **Save**.

   If all the parameters are correct, mitigation is enabled.

Table 5: Policy Enforcer Mitigation Guidelines

Setting	Guideline
Policy Enforcer Hostname	The Policy Enforcer virtual machine IP address automatically appears. This is the IP address that you configure in the Policy Enforcer > Settings page.
Policy Enforcer SSH User Name	The SSH username automatically appears. This is the same username that you configure in the Policy Enforcer > Settings page.
Policy Enforcer SSH Password	Enter the Policy Enforcer SSH password. This is the same password that you enter in the Policy Enforcer > Settings page.
API User Name	If you have the credentials for the Policy Enforcer Controller APIs, enter the existing API username. Else, enter a name and Security Director Insights will create a new username.
API Password	If you have the credentials for the Policy Enforcer Controller APIs, enter the existing API password. Else, enter a password and Security Director Insights will create a new password.
Blocklist Feed Name	Enter the blocklist custom feed name that you created in the Configure > Threat Prevention > Feed Sources > Custom Feeds page.
Infected-Host Feed Name	Enter the infected host custom feed name that you created in the Configure > Threat Prevention > Feed Sources > Custom Feeds page.

NOTE: Security Director Insights supports mitigation using Juniper ATP Cloud and Policy Enforcer. Only one plugin can be active at a given time. Before you enable Policy Enforcer mitigation settings, ensure to disable the Juniper ATP Cloud plugin if it is enabled.

Monitor Mitigation Through Policy Enforcer

The following example shows how to mitigate incidents through Policy Enforcer.

To monitor the mitigation:

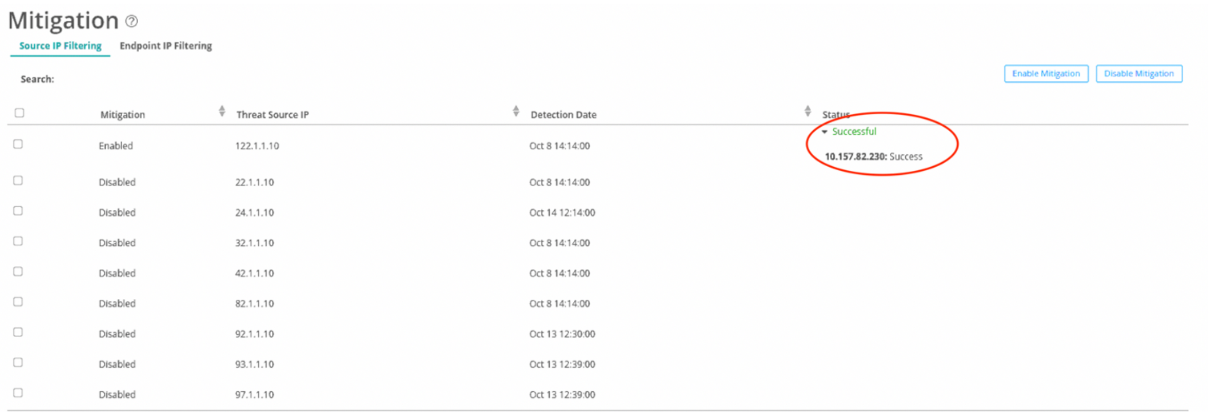
1. Select **Security Director** > **Monitor** > **Insights** > **Mitigation**.

   The Mitigation page appears.

2. Select one or more IP addresses and click **Enable Mitigation**.

   If the mitigation is Successful, the status column displays Successful, as shown in Figure 29 on page 46.

Figure 29: Mitigation Successful



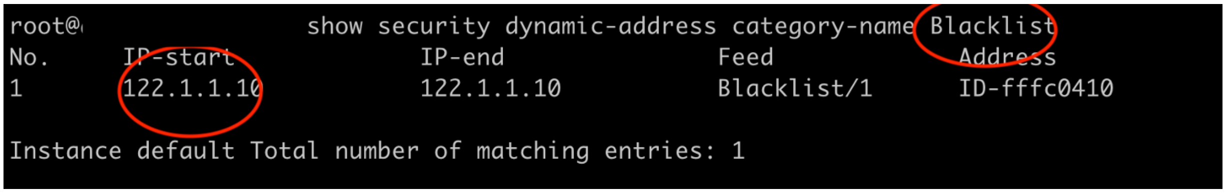
□	Mitigation	Threat Source IP	Detection Date	Status
□	Enabled	122.1.1.10	Oct 8 14:14:00	Successful **10.157.82.230:** Success
□	Disabled	22.1.1.10	Oct 8 14:14:00	
□	Disabled	24.1.1.10	Oct 14 12:14:00	
□	Disabled	32.1.1.10	Oct 8 14:14:00	
□	Disabled	42.1.1.10	Oct 8 14:14:00	
□	Disabled	82.1.1.10	Oct 8 14:14:00	
□	Disabled	92.1.1.10	Oct 13 12:30:00	
□	Disabled	93.1.1.10	Oct 13 12:39:00	
□	Disabled	97.1.1.10	Oct 13 12:39:00	

   The mitigated IP addresses listed under the Source IP Filtering tab are added to the custom blocklist feed.

   The mitigated IP addresses listed under the Endpoint IP Filtering tab are added to the infected host custom feed.

3. Verify the blocklisted IP addresses in the SRX Series device that was added as an endpoint in Policy Enforcer. The device receives one blocklist feed with the IP address that you mitigated in Step 2, as shown in Figure 30 on page 46.

Figure 30: Blocklisted IP Address



```
root@                show security dynamic-address category-name Blacklist
No.     IP-start            IP-end                Feed            Address
1       122.1.1.10          122.1.1.10            Blacklist/1     ID-fffc0410

Instance default Total number of matching entries: 1
```

RELATED DOCUMENTATION

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files | 12
Add Security Director Insights as a Log Collector | 19
Security Director Insights High Availability Deployment Architecture | 23
Configure Security Director Insights High Availability | 25

Upgrade Security Director Insights

Table 6 on page 47 shows the upgrade path for Security Director Insights.

Table 6: Upgrade Path

Upgrading to Release	Upgrade Path	Description
Security Director Insights 21.3R1	21.2R1 > 21.3R1	You can upgrade from the following release: • Security Director Insights Release 21.2R1
Security Director Insights 21.2R1	21.1R1 > 21.2R1	You can upgrade from the following release: • Security Director Insights Release 21.1R1
Security Director Insights 21.1R1	20.3R1 > 21.1R1	You can upgrade from the following release: • Security Director Insights Release 20.3R1

To upgrade from a previous version of Security Director Insights:

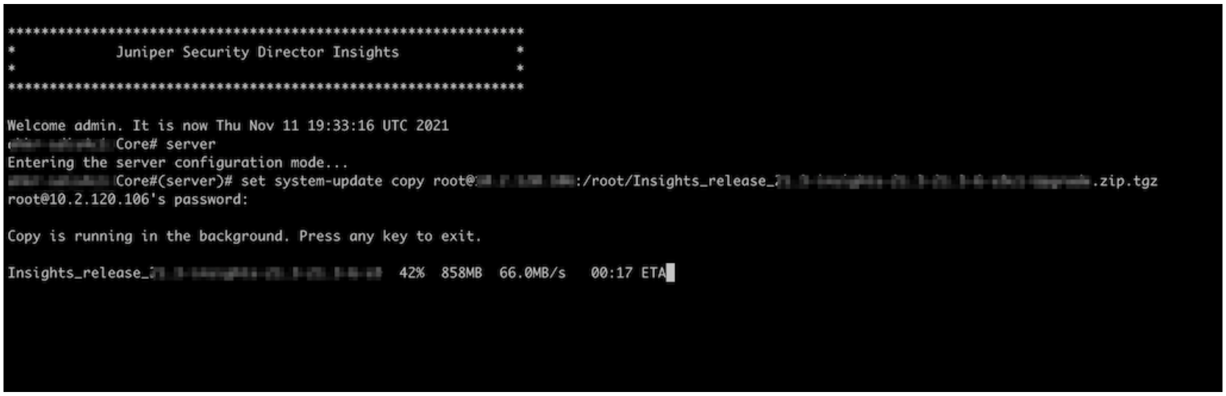
1. Download the release image from the download site to a location (virtual machine) that is accessible from Security Director Insights.

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 31: Copy the Upgrade Package



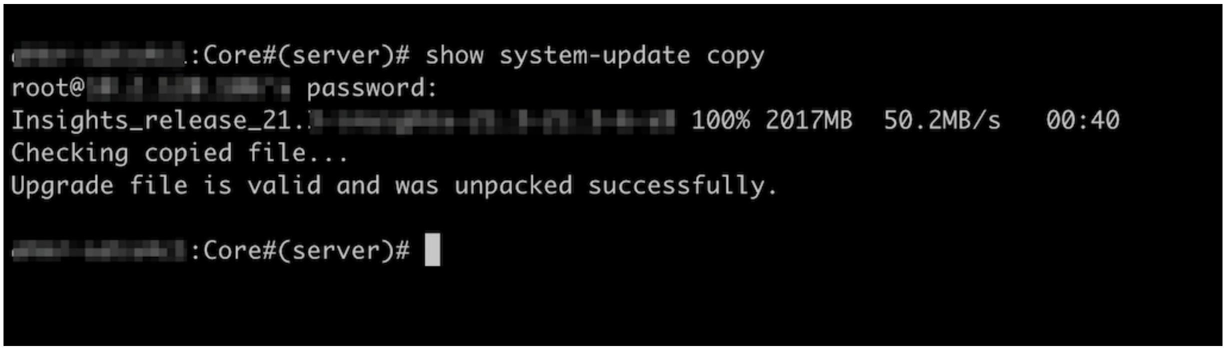
```
******************************************************************
*            Juniper Security Director Insights                  *
*                                                                *
******************************************************************

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

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

Insights_release_[redacted]  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 32: Check Copy Progress

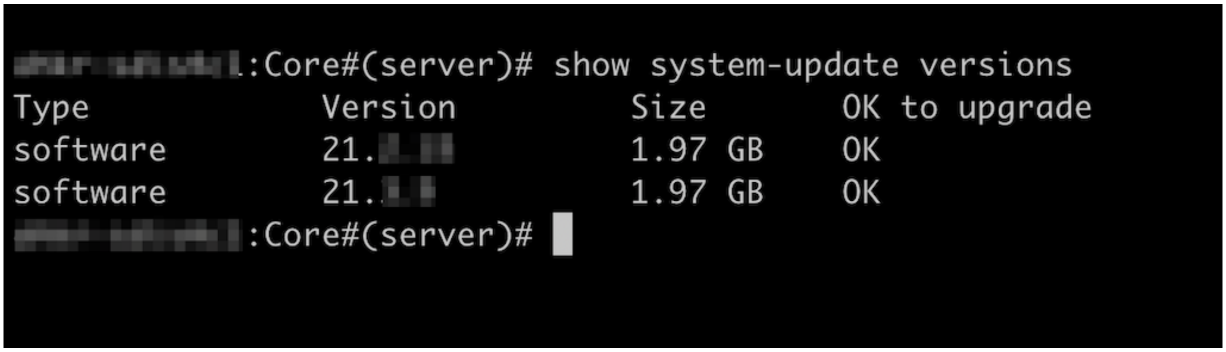


```
[redacted]:Core#(server)# show system-update copy
root@[redacted] password:
Insights_release_21.[redacted] 100% 2017MB  50.2MB/s   00:40
Checking copied file...
Upgrade file is valid and was unpacked successfully.

[redacted]:Core#(server)#
```

5. Check the available upgrade versions:

   show system-update versions.

Figure 33: Available Upgrade Versions



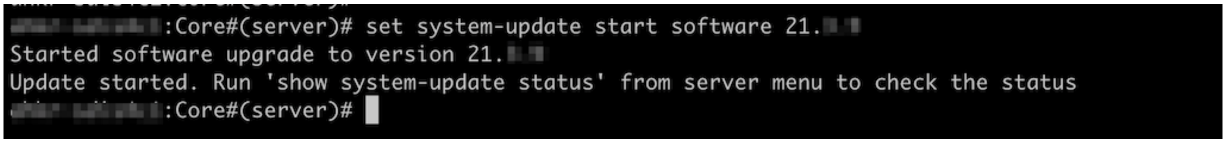
```
[redacted]:Core#(server)# show system-update versions
Type            Version         Size       OK to upgrade
software        21.[redacted]         1.97 GB    OK
software        21.[redacted]          1.97 GB    OK
[redacted]:Core#(server)# █
```

6. Start the upgrade process:

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

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

Figure 34: Start Upgrade Process

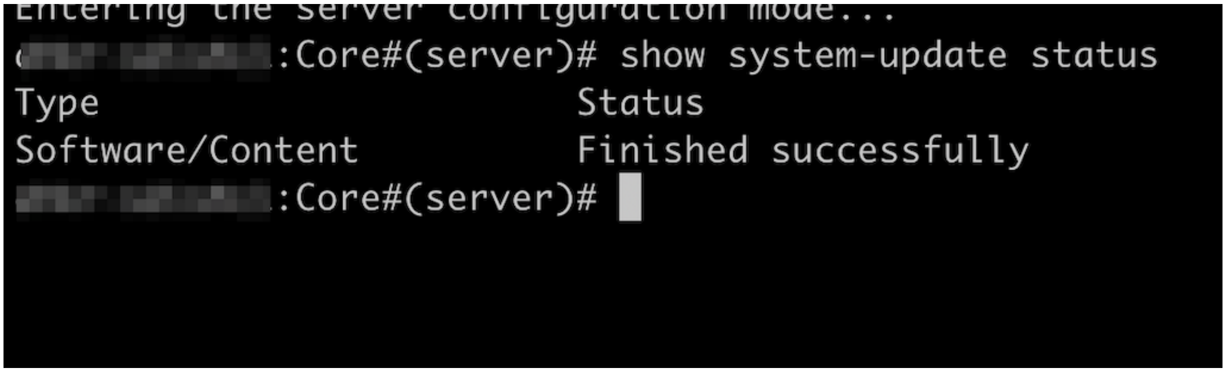


```
[redacted]:Core#(server)# set system-update start software 21.[redacted]
Started software upgrade to version 21.[redacted]
Update started. Run 'show system-update status' from server menu to check the status
[redacted]:Core#(server)# █
```

7. Monitor the status of upgrade:

   show system-update status.

Figure 35: Monitor Upgrade Status



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