JUNIPER NETWORKS | Engineering Simplicity

Security Director Insights User Guide

Published
2023-06-29

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

Security Director Insights User 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

3

Configure

About the Documentation

IN THIS SECTION

Use this guide to configure Juniper Security Director Insights, a component of Security Director. It enables you to take effective automated actions on security events from Juniper Networks security products.

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 viii 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 viii 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		

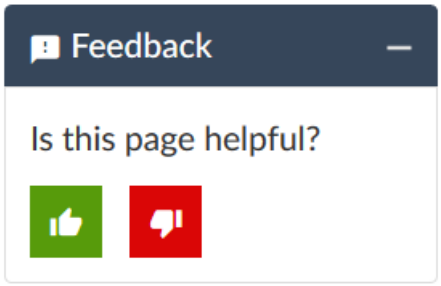
Table 2: Text and Syntax Conventions *(continued)*

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/.

CHAPTER 1

Overview

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.

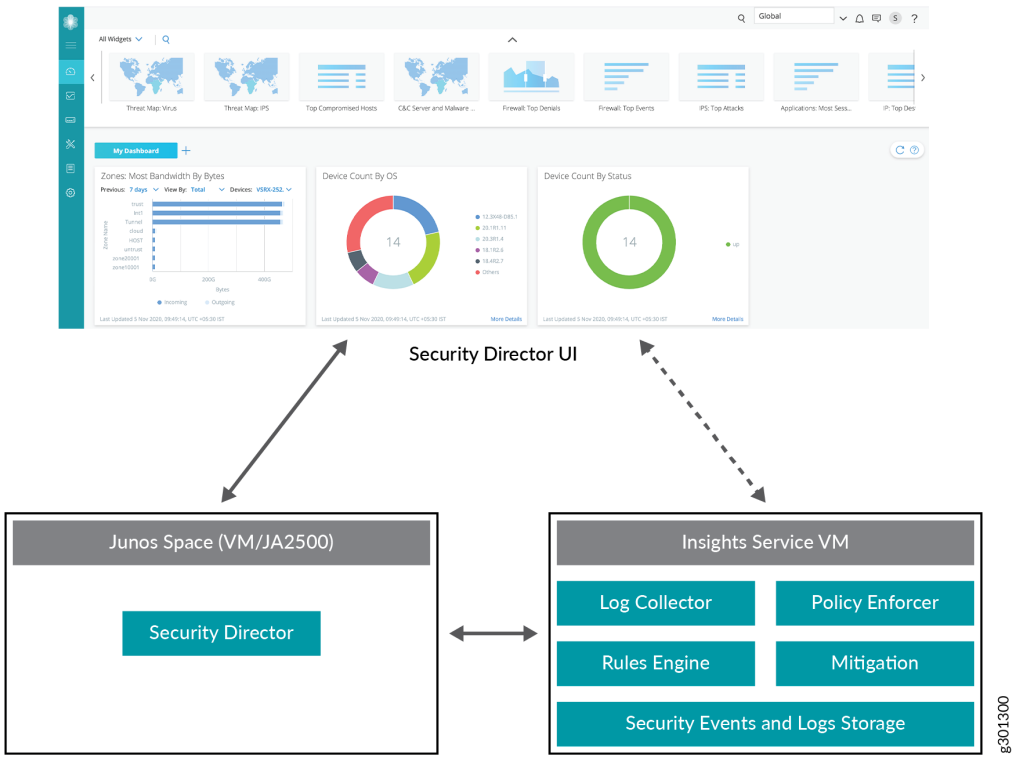
Benefits

- 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 14.

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 | 17

2
CHAPTER

Administration

Add Insights Nodes

Use Security Director Insights to automate security operations and take effective actions on security events logged by Juniper Networks Security products. It connects disparate security tools for seamless security operations and incident response. It ingests logs from SRX Series devices and other security vendors to correlate and provide automated enrichment to identify the threats.

Security Director Insights is a single virtual appliance (Service VM) that runs on the VMware vSphere infrastructure. You must configure Security Director Insights as nodes for Security Director to discover the Security Director Insights virtual machine (VM).

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

To configure a standalone or primary (active) node:

1. Select **Security Director** > **Administration** >**Insights Management** > **Insights Nodes**.

   The Insights Nodes page appears.

2. Complete the configuration according to the guidelines provided in Table 3 on page 17.

3. Click **Save**.

   If the details provided are valid, the Security Director Insights node is added successfully. Click **Reset** to remove the node.

Table 3: Add Insights Nodes

Setting	Guidelines
IP Address	Enter the IP address of the Security Director Insights VM. (This is the IP address you configured during the Security Director Insights VM installation).
Username	The username to access the VM is always *admin*. You cannot modify this field.
Password	Enter the password to access the Security Director Insights VM. (This is the same password you use to log in to the VM CLI with your admin credentials).

To configure the secondary (standby) node details:

1. Select the **Enable HA** option.

   The HA Setup page appears.

2. Complete the configuration according to the guidelines provided in Table 4 on page 18.

3. Click **Save & Enable**.

   The Insights Nodes page appears. It shows the status of the secondary node activation.

4. Click **Refresh Data** to check the status of the secondary node configuration.

   After the configuration is successful, you see the respective IP addresses appearing in the Data/Management Virtual IP and Monitoring Virtual IP columns.

> **NOTE:** Keep clicking the Refresh Data option until you see that the secondary node is configured successfully and all the other errors disappear, if any.

Table 4: Configure HA Setup

Setting	Guidelines
Secondary Node Details	
Secondary system IP	Enter the IP address of the secondary (standby) node.
Username	The username to access the virtual machine is always 'admin'. You cannot modify this field.
Password	Enter your SSH password to access the secondary node. (This is the same password you use to log in to the VM CLI with your admin credentials.)
HA Settings	
Data Virtual IP/Netmask	Enter the virtual IP address for data traffic between primary (active) and secondary (standby) nodes.
HA monitor Virtual IP/Netmask	Enter the virtual IP address for HA monitoring traffic between active and standby nodes.
Ping IPs	(Optional) Enter a list of IP addresses for ping tests.

NOTE: To enable HA, the IP addresses on Security Director Insights must be static.

In the Node Status section, you can see the complete configuration details of the primary (active) and secondary (standby) nodes.

You can take the following actions:

- Stop standby—In the Standby section, click **Stop** to temporarily stop HA service on a standby node to perform maintenance tasks.
- Start standby—In the Standby section, click **Start** to restart the HA service, if it is stopped.
- Rebuild standby—To rebuild out-of-sync data on the standby node, click **Rebuild**.
- Failover—To manually shut down the HA service on the active node, so that the standby node becomes the active node, click **Failover** in the Active section. The virtual IP address will be reassigned to the new active node. You can use the Failover option to perform any maintenance tasks on the active node. You must click **Start** to restart the HA services.

Table 5 on page 19 shows more details of each Security Director Insights node in the Insights Node page.

Table 5: Insights Node Details

Field Name	Description
Hostname	Specifies the hostname of the node.
Data Traffic IP	Specifies the data traffic IP address of the node.
HA Monitor IP	Specifies the HA monitoring IP address of the node.
CPU Usage	Specifies the CPU usage of the node.
Memory Usage	Specifies the memory usage of the node.
Online	Specifies whether the node is online or offline.
Role	Specifies whether the node is primary (active) or secondary (standby).
Status	Specifies the health of the node.

RELATED DOCUMENTATION

About the Alerts Settings Page

To access this page, select **Security Director** > **Administration** > **Insights Management** > **Alert Settings**.

The configurations we do from the Alert Settings page are for system-audit and system-health checks. On this page, you can configure alert settings, so that when the system state reaches a certain threshold, an alert is generated and you are notified.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create new alert settings. See "Create a New Alert Setting" on page 21.
- Display, delete, or edit an existing alert configuration.

Field Descriptions

Table 6 on page 20 describes the fields on the Alert Settings page.

Table 6: Fields on the Alert Settings Page

Field	Description
Description	Provides details about the alert settings, such as alert type, event type, report format, and date range.
Delivery	Specifies whether an alert is generated based on a trigger or by schedule.
Actions	For each generated alert, you can take different actions such as, display the alert, edit the alert setting, or delete the alert.

Display, Delete, or Edit an Existing Alert

To display, delete, or edit an existing alert configuration:

- Select **Display** to view the details of an alert in HTML or PDF format. You can configure the format.

- Select **Edit** and then **Save** to modify the alert configuration. You can, for example, change details of the system audit and system health alert settings.
- Select **Delete** and then **Save** to delete the current settings of an alert.

RELATED DOCUMENTATION

Create a New Alert Setting | 21

Create a New Alert Setting

You can configure alert settings to generate alerts based on system health or data in the system audit records. You can configure event types to include in the alert notification, date range, whether to notify all users or only the current user, alerts related to the overall health of the system, when there was a data retention, and so on. You can generate an alert immediately or schedule the alert generation for a later day and time. The generated report is sent to the recipient's e-mail ID in HTML or PDF format.

To create an alert setting:

1. Select **Administration** > **Insights Management** > **Alert Settings**.

   The Alerts Settings page appears.

2. Click **Create**.

   The Create New Alert Setting page appears.

3. Complete the configuration according to the guidelines provided in Table 7 on page 21.

4. Click **Save**.

   A new alert setting is created and displayed on the Alerts Settings page.

Table 7: Create New Alert Setting

Setting	Guideline
Type	Select the type of alert notification to be configured: System Audit or System Health.
System Audit Alert Settings	

Table 7: Create New Alert Setting *(continued)*

Setting	Guideline
Event Type	Select the event types to include in the alert notification: • Login/Logout—Generate an alert when a user logs in to or logs out of the system. • Add/Update Users—Generate an alert when a new user is added or an existing user's details are updated. • System Settings—Generate alerts when there are changes to the system settings. • Restarts—Generate an alert when the system is restarted. • Remote Support—Generate an alert when a user has sought remote support to address any issues.
Users	Select whether to send the alert notification to all users or only to the current user.
Date Range	To filter the report notification by time period, select one of the following options: Last Day, Last Week, Last Month, Last Year
Max Num Results	Enter the number of rows of results to include in the alert notification (default is 25).
Format	Select **HTML** or **PDF** as the notification output format.
Generate On	Select **Trigger** to generate an alert immediately. Select **By Schedule** to schedule the alert generation on a specified day and time. For time, use the format 00:00 am or pm.
Recipient's Email	Enter a valid e-mail address of the recipient. You can enter more than one e-mail ID. Separate e-mail IDs with commas.
System Health Alert Settings	
Health	For system health alerts, select either **Overall Health** metrics, **Data Retention**, or **HA Alerts**. For data retention, you will receive alerts when the device reaches 80% capacity. You must delete old data to store the incoming data.
Format	Select **HTML** or **PDF** as the notification output format.
Generate On	Select **Trigger** to generate an alert immediately. Select **By Schedule** to schedule the alert generation on a specified day and time. For time, use the format 00:00 am or pm. **NOTE:** For HA alerts, you can only trigger an alert. You cannot schedule the alert generation.

Table 7: Create New Alert Setting *(continued)*

Setting	Guideline
Recipient's Email	Enter a valid e-mail address of the recipient. You can enter more than one e-mail ID. Separate e-mail IDs with commas.

RELATED DOCUMENTATION

About the Alerts Settings Page | 20

Add Insights Nodes | 17

Configure System Settings

Use the System Settings page to configure or revise outgoing e-mail notification settings. You can also test the current outgoing mail configuration. E-mail notifications are generated for alert settings configured on the Alert Settings page. Ensure that the Security Director Insights node connectivity is working fine. E-mail messages are sent from the Security Director Insights VM.

To configure outgoing e-mail settings:

1. Select **Administration**> **Insights Management**> **System Settings**.

   The System Settings page appears.

2. In the Outgoing Email Settings section, complete the configuration according to the guidelines provided in Table 8 on page 23.

Table 8: Configure Outgoing E-mail Settings

Setting	Guideline
SMTP Host	Enter the IP address of the enterprise mail host.
SMTP Port	Enter the SMTP port number (default is 587). You can add Gmail. Most of the other e-mail providers use port 465 for SSL.

Table 8: Configure Outgoing E-mail Settings *(continued)*

Setting	Guideline
Use SSL	This option is enabled by default. You can use Secure Sockets Layer (SSL) for further protection. Deselect the option to disable the use of SSL.
SMTP Login	Enter the username that you want to use for authentication.
SMTP Password	Enter an SMTP password for the login account.
From Address	Enter the e-mail address of the sender; the default is noreply@juniper.net.

On the Administration > Insights Management > System Settings page, in the Test Outgoing Email Settings section, you can test the current outgoing mail configuration.

To test an outgoing e-mail setting:

1. Enter an e-mail address (or series of e-mail addresses, separated by commas) to which the test e-mail will be sent by Security Director Insights.

2. Click **Test** to test your e-mail notification configuration. An e-mail will be sent by Security Director Insights to the e-mail address(es) entered, based on the configuration settings.

   The format of the test e-mail is **This e-mail is a confirmation that your Insights Central Manager (VM name) is correctly configured. This email was sent on Fri, 09 Oct 2020 at 22:02:02 +0000 to abc@xxx.com. For further information, please visit https://support.juniper.net.**

   NOTE: This test verifies the ability to send an e-mail. It does not test the validity of the e-mail address.

RELATED DOCUMENTATION

Add Insights Nodes | 17

About the Identity Settings Page

To access this page, select **Administration** > **Insights Management** > **Identity Settings**.

Security Director Insights interfaces with Juniper Identity Management Service (JIMS) to map endpoint IP addresses in events and logs to usernames and hostnames. You can configure JIMS to provide access information to Security Director Insights.

Tasks You Can Perform

You can perform the following tasks from the Identity Settings page:

- Add a JIMS configuration. See "Add JIMS Configuration" on page 26.
- Delete or edit an existing JIMS configuration. See "Edit and Delete an Identity Setting" on page 27.
- Select **Test** to test the JIMS configuration. You can verify the configuration and check whether the Security Director Insights VM can communicate with JIMS successfully.

Field Descriptions

Table 9 on page 25 provides guidelines to use the fields on the Identity Settings page.

Table 9: Fields on the Identity Settings Page

Field	Description
Details	Specifies details about the JIMS configuration.
Actions	For each JIMS configuration, you can take different actions such as editing or deleting the JIMS configuration.

RELATED DOCUMENTATION

Add JIMS Configuration | 26

Edit and Delete an Identity Setting | 27

Add JIMS Configuration

Use the Add JIMS Configuration page to configure a JIMS profile to obtain user identities. Ensure that you have added the IP address of Security Director Insights in the JIMS server.

To add a JIMS configuration:

1. Select **Administration**> **Insights Management**> **Identity Settings**.

   The Identity Settings page appears.

2. Click **Create**.

   The Add JIMS Configuration page appears.

3. Complete the configuration according to the guidelines provided in Table 10 on page 26.

4. Click **Save**.

   A new JIMS configuration is added to Security Director Insights and listed on the Identity Settings page.

Table 10: Add JIMS Configuration

Setting	Guideline
JIMS Endpoint Hostname/IP	Enter a valid IPv4 or IPv6 address or the hostname of the JIMS server.
JIMS Port Number	Select the connection port of the JIMS server from the list. The range is 1 to 65,535.
SSL	Select an SSL setting: **Enabled** or **Disabled**.
Identity Sources	Select an identity source to collect data from: Active Directory, Syslog, or both.
Use Reverse DNS	Reverse DNS lookup converts an IP address to hostname to identify the domain name of the source. Choose to enable or disable the Use Reverse DNS setting. This option is enabled by default.
Exclude hostnames	You can disallow identity mapping for certain hosts. Enter the hostnames separated by commas. Identity mappings for these hosts are ignored and not included in event handling and displays.

Table 10: Add JIMS Configuration ***(continued)***

Setting	Guideline
OAuth Client ID	Enter the Open Authorization (OAuth) client ID that the Security Director Insights provides to the JIMS server as part of its authentication. Security Director Insights must authenticate itself with the JIMS server to obtain an access token that allows it to query the JIMS server for user identity information. The client ID must be consistent with the API client configured on JIMS.
OAuth Client Secret	Enter the client secret that Security Director Insights provides to the JIMS server as part of its authentication. The client secret must be consistent with the API client configured on JIMS.

RELATED DOCUMENTATION

About the Identity Settings Page | 25
Edit and Delete an Identity Setting | 27

Edit and Delete an Identity Setting

IN THIS SECTION

You can edit and delete a JIMS configuration from the Identity Settings page.

Edit a JIMS Configuration

To edit a JIMS configuration:

1. Select **Administration**>**Insights Management**>**Identity Settings**.

   The Identity Settings page appears.

2. Select the JIMS configuration that you want to modify, and click the **Edit** icon.

   The Edit JIMS Configuration page appears, displaying the same fields that were presented when you added the JIMS configuration.

3. Modify the JIMS configuration fields.

4. Click **Save** to save your changes.

   You are taken to the Identity Settings page. A confirmation message appears, indicating the status of the edit operation.

Delete a JIMS Configuration

To delete a JIMS configuration:

1. Select **Administration**>**Insights Management**>**Identity Settings**.

   The Identity Settings page appears.

2. Select the JIMS configuration that you want to delete, and click the **Delete** icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected JIMS configuration.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

About the Identity Settings Page | 25
Add JIMS Configuration | 26

Configure Mitigation Settings

In response to an incident, you can either isolate or quarantine an infected endpoint based on its IP address and block the threat source IP address. This prevents you from downloading files that are known to be harmful or suspicious. Mitigation is performed by either Security Director Policy Enforcer or Juniper Advanced Threat Prevention Cloud (ATP Cloud).

To configure mitigation settings:

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

   The Mitigation Settings page appears.

2. Complete the configuration according to the guidelines provided in Table 11 on page 29.

3. Click **Save**.

   The mitigation settings are saved and enabled.

Table 11: Configure Mitigation Settings

Setting	Guideline
ATP Cloud	
Application Token	Add an application token to allow Security Director Insights or OpenAPI users to securely access ATP Cloud APIs over HTTPS.
Open API (Infected hosts) URL	Enter an endpoint URL for the infected host (OpenAPI) and blocklisted API (Gophro).
Open API (Threat Intelligence) URL	Enter the Threat Intelligence OpenAPI URL to program the ATP Cloud command-and-control (C&C) server feeds.
Blocklist Feed Name	Enter the blocklist feed name. Security Director Insights sends the source IP addresses to the blocklist feed with the specified feed name. You cannot modify the feed name after it is configured.
Policy Enforcer	
Hostname	Enter the hostname of the Policy Enforcer VM. (This is the hostname you configured during the installation of the Policy Enforcer VM.) To configure Policy Enforcer running on Security Director Insights, enter the hostname or IP address of the Security Director Insights VM.

Table 11: Configure Mitigation Settings ***(continued)***

Setting	Guideline
SSH Username	Enter **root** as the username of the Policy Enforcer VM (for the standalone Policy Enforcer). For the integrated Policy Enforcer running on Security Director Insights, the 'admin' username is already prepopulated.
SSH Password	Enter the root password of the Policy Enforcer VM (for the standalone Policy Enforcer). For the integrated Policy Enforcer running on Security Director Insights, enter the password of the Security Director Insights CLI administrator.
API Username	Enter the username of the Policy Enforcer controller API.
API Password	Enter the password of the Policy Enforcer controller API.
Blocklist Feed Name	Ensure that you have configured the blocklist custom feed under Configure > Threat Prevention > Feed Sources > Create Custom Feed.
Infected Host Feed Name	Ensure that you have configured the infected host custom feed under Configure > Threat Prevention > Feed Sources > Create Custom Feed.

Click **Test** to verify the configuration. Also, you have an option to disable the already enabled mitigation setting.

RELATED DOCUMENTATION

How to Monitor Mitigation | 69

About the Threat Intelligence Page

To access this page, select **Administration** > **Insights Management** > **Threat Intelligence**.

Look up your trusted threat intelligence providers for indicators of compromise to confirm the maliciousness of the reported event. Indicators of compromise include IP addresses, URLs, and file hash observed in the log data. What is considered malicious is based on available knowledge about the threat intelligence provider's output.

Security Director Insights supports the following threat intelligence sources:

Source	Data
IBM X-Force	IP lookup and file hash
VirusTotal	File hash and URL lookup
Opswat	File hash, URL lookup, and IP lookup

Tasks You Can Perform

You can perform the following tasks from the Threat Intelligence page:

- Configure a threat intelligence source. See "Configure Threat Intelligence Source" on page 32.
- Edit and delete an existing threat intelligence source. See "Edit and Delete Threat Intelligence Source" on page 33.
- Click **Test** to test the validity of the API key and check whether the Security Director VM can reach a threat intelligence source.

Field Descriptions

Table 12 on page 31 provides guidelines on using the fields on the Threat Intelligence page.

Table 12: Fields on the Threat Intelligence Page

Field	Description
Source	Specifies the threat intelligence source.
Description	Specifies the corresponding API details configured for the threat intelligence source.

RELATED DOCUMENTATION

Configure Threat Intelligence Source | 32
Edit and Delete Threat Intelligence Source | 33

Configure Threat Intelligence Source

Configure the threat intelligence providers for IP address, URL, file hash to confirm the maliciousness of the reported event.

To configure the threat intelligence source:

1. Select **Administration** > **Insights Management** > **Threat Intelligence**.

   The Threat Intelligence page appears.

2. Click the plus icon (+).

   The Create Configuration page appears.

3. Complete the configuration according to the guidelines provided in Table 13 on page 32.

4. Click **OK**.

   A new threat intelligence source is configured and listed on the Threat Intelligence page.

Table 13: Configure Threat Intelligence Source

Setting	Guideline
Source Name	Select the threat intelligence providers from the list. The supported threat intelligence providers are IBM X-Force, VirusTotal, and OPSWAT Metadefender.
API Key	Enter a valid API key to look up the threat intelligence provider's APIs. • VirusTotal API Key • OPSWAT API Key • IBM X-Force API Key
API Password	Enter a password, if you using IBM X-Force, to look up the threat intelligence provider's APIs.

RELATED DOCUMENTATION

About the Threat Intelligence Page | 30
Edit and Delete Threat Intelligence Source | 33

Edit and Delete Threat Intelligence Source

IN THIS SECTION

You can edit and delete the threat intelligence providers from the Threat Intelligence page.

Edit a Threat Intelligence Source

To edit a threat intelligence source configuration:

1. Select **Administration** > **Insights Management** > **Threat Intelligence**.

   The Threat Intelligence page appears.

2. Select the threat intelligence source that you want to modify, and click the **Edit** icon (pencil).

   The Modify Configuration page appears, displaying the same fields that were presented when you configured the threat intelligence sources.

3. Modify the configuration fields as needed.

4. Click **Save** to save your changes.

   You are taken to the Threat Intelligence page. A confirmation message appears, indicating the status of the edit operation.

Delete a Threat Intelligence Source

To delete a threat intelligence source:

1. Select **Administration**>**Insights Management**>**Threat Intelligence**.

   The Threat Intelligence page appears.

2. Select the threat intelligence source that you want to delete and click the **Delete** icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected threat intelligence source.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

About the Threat Intelligence Page | 30
Configure Threat Intelligence Source | 32

About the ServiceNow Configuration Page

To access this page, select **Administration** > **Insights Management** > **ServiceNow Configuration**.

You can configure your ServiceNow account to create tickets for incidents.

Tasks You Can Perform

You can perform the following tasks from the ServiceNow Configuration page:

- Configure your ServiceNow account.
- Reset the already configured ServiceNow account details.

Field Descriptions

Table 14 on page 35 provides guidelines on using the fields on the ServiceNow Configuration page.

Table 14: Fields on the ServiceNow Configuration Page

Field	Description
ServiceNow Instance URL	Specify the URL of your ServiceNow account. Ensure that you have provided the correct URL. For example, https://example.service-now.com/.
Username	Specify the username to access the ServiceNow instance URL.
Password	Specify the password to access the ServiceNow instance URL.

After you configure the ServiceNow account successfully, you can start creating ServiceNow tickets for any incident on the Monitor > Insights > Incidents page. Expand an incident and click **Create Ticket**.

RELATED DOCUMENTATION

How to Monitor Incidents | 64

Add Insights Nodes | 17

About the Backup & Restore Page

To access this page, select **Administration** > **Insights Management** > **Backup & Restore**.

You can back up different configurations of Security Director Insights (not the data collected by Insights) and restore the configuration from the existing backup configuration files.

The configuration backup includes the configurations for Security Director Insights and Log Collector, but not for Policy Enforcer. You can restore the backup configuration settings to any Security Director Insights and Log Collector systems running the same version. There is no dependency on the data contained within Security Director.

Tasks You Can Perform

You can perform the following tasks from the Backup and Restore page:

- Create a new backup. See “Create a Backup File and Restore the Configuration” on page 37.
- Restore the configuration from a backed up configuration of Insights.
- Download and delete the backup configuration. See “Download and Delete a Backup File” on page 38.
- View the last restoration status. It is shown in the right-hand side of the page.

Field Descriptions

Table 15 on page 36 provides guidelines on using the fields on the Backup & Restore page.

Table 15: Fields on the Backup and Restore Page

Field	Description
File Name	Specifies the filename of the backup configuration file.
Size	Specifies the size of the backup file.
Date	Specifies the date and time when the backup was last taken.
Software Version	Specifies the backup software version of Security Director Insights.

RELATED DOCUMENTATION

Create a Backup File and Restore the Configuration | 37
Download and Delete a Backup File | 38

Create a Backup File and Restore the Configuration

IN THIS SECTION

You can create a new backup of the current configuration (not the data collected by Insights) from the Backup and Restore page. You can restore the configuration from an existing backup or select a configuration file from your local storage.

Create a New Backup File

To create a new backup file:

1. Select **Administration** > **Insights Management** > **Backup & Restore**.

   The Backup & Restore page appears.

2. Click the plus icon (+).

   The BACKUP page appears.

3. Click **OK**.

   Backup is initiated and you are taken to the Backup & Restore page. After the backup is complete, the backup filename and additional details are listed.

> **NOTE:** You can backup only the configuration. The configuration backup includes the configurations for Security Director Insights and Log Collector, but not for Policy Enforcer.

Restore a Configuration

To restore a configuration:

1. Select **Administration** > **Insights Management** > **Backup & Restore**.

   The Backup & Restore page appears. You can restore the configuration from an existing backup or select a file from your local storage.

2. To restore the configuration from an existing backup, select the backup file listed on the Backup & Restore page and click the **Restore** icon (clock).

   OR

   To restore the configuration from a file in your local storage, click the clock icon.

   The RESTORE page appears. Click **Browse** and select the configuration file from your local storage.

3. Click **OK**.

> **NOTE:** During restoration, all services are temporarily stopped. You can restore the backup configuration settings to any Security Director Insights and Log Collector systems running the same version. There is no dependency on the data contained within Security Director.

RELATED DOCUMENTATION

About the Backup & Restore Page | 35
Download and Delete a Backup File | 38

Download and Delete a Backup File

IN THIS SECTION

You can download a backup file to your local system. You can also delete a backup file.

Download a Backup File

To download a backup to your local system:

1. Select **Administration** > **Insights Management** > **Backup & Restore**.

   The Backup & Restore page appears.

2. Select the backup file that you want to download and click the download icon.

   The backup file is downloaded to your local system as a ZIP file.

Delete a Backup File

To delete a backup file:

1. Select **Administration** > **Insights Management** > **Backup & Restore**.

   The Backup & Restore page appears.

2. Select the backup file that you want to delete and click the delete icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected backup file.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

About the Backup & Restore Page | 35

Create a Backup File and Restore the Configuration | 37

3
CHAPTER

Configure

About the Log Parsers Page

To access this page, click **Configure** > **Insights** > **Log Parsers**.

Use the flexible log parser to define how the system log data must be parsed. The flexible parser enables you to provide a sample of your logs to create a new parser, parse the logs, normalize the fields, filter logs based on your configured criteria, and assign severity and semantics to various fields. You can create multiple parsers for different log sources. You can also import the parsers from a file or export the parsers to a standard file that can be saved and shared.

Security Director Insights includes prepackaged parsers for SRX Series device logs. You can export a prepackaged parser to a file and save a copy of that parser. This is a sample parser. You can add any logs to it, change the filter criteria, or modify the conditions for severity settings according to your environment and Security Operation Center (SOC) process. Before modifying a prepackaged log parser, it's good to export it to a file and save a copy of the default parser. You can always import it back to the SRX Series device if you need it later.

Tasks You Can Perform

You can perform the following tasks from the Log Parsers page:

- Create a new log parser. See "Create a New Log Parser" on page 43.
- Import and export log parsers. See "Import and Export Log Parsers" on page 48.
- Edit and delete a log parser. See "Edit and Delete a Log Parser" on page 47.

Field Descriptions

Table 16 on page 42 provides guidelines to configure the Log Parsers.

Table 16: Fields on the Log Parsers Page

Field	Description
Name	Specifies the name of the log parser that you have created.
Description	Specifies the corresponding description provided for the log parser.

RELATED DOCUMENTATION

Create a New Log Parser

Use the New Log Parser page to create your own log parser by using sample logs. You can build your own parser by mapping fields in your sample logs to Security Director Insights event fields, indicating which types of events will generate an incident.

To create a new log parser:

1. Select **Configure** > **Insights** > **Log Parsers**.

   The Log Parsers page appears.

2. Select the plus icon (+).

   The New Log Parser page appears.

3. Complete the configuration according to the guidelines provided in Table 17 on page 43.

4. Click **Finish**, and you are presented with the results of your flexible log parser as they are applied to the sample logs provided.

   Review the results carefully to determine whether your mapping, filtering, and assignment conditions are as expected.

Table 17: Add New Log Parser

Setting	Guideline
Create/Edit Parser	
Name	Enter a unique and descriptive name for the log parser.
Description	Enter a description for the log parser.
Parse Log File	

Table 17: Add New Log Parser *(continued)*

Setting	Guideline
Raw Log	Upload the raw log file by browsing to it, or paste the log data in a separate field provided below the Browse button. Ensure the log file contains an RFC-compliant syslog header.
Log File Format	Specify the format of the sample log file. The available options are: • XML • JSON • CSV • Others
CSV Headers (if the log file format is CSV)	If your log file is in CSV format, you may provide a comma-delimited list of field names in this field. If the CSV headers are not provided, the fields will be named as csv*N*, where *N* is the field position.
Grok Pattern (if the log file format is others)	If you select the Others option for the log file format, you must supply a grok pattern for the log file. A grok pattern may consist of one or more lines. The grok pattern line beginning with LOGPATTERN is the pattern that will be applied to the logs. A grok pattern must include a pattern named LOGPATTERN, otherwise the parser will not have any pattern to use.
Field Mapping	
Mapped Fields and Unmapped Fields	In the Unmapped Field section, select a field in the Parsed Fields column and then select a value in the Insights Fields column to map. After selecting both the fields, click **Map**. The mapped fields now appear in the Mapped Fields section, which lists all fields that have been mapped to each other. You can perform the following actions from the Field Mapping page: • Click a circular arrow icon in the Mapped Fields section to undo a mapping. • Click the filter icon in the Unmapped Fields section to enter text for searching. • In the Unmapped Fields section, you can select multiple fields from the Parsed Fields column and map them to one field from the Insights Fields column. When you do this, a sort icon appears in the Mapped Fields section. Use the Sort capability to select the order in which multiple fields are applied based on whether those fields contain a valid value or not. Higher in the order takes priority. • Select the **Counter** check box to count the number of times a field appears. **NOTE:** Fields marked with * are mandatory.
Date Format	

Table 17: Add New Log Parser *(continued)*

Setting	Guideline
Field Mapping: Format Date and Time	This is an optional configuration. You can leave this field blank, if your log file is using a standard time as dictated by RFC 3164 or RFC 5424. Those headers are automatically parsed. If the timestamp cannot be parsed, use the Ruby strftime to provide a format string so that Security Director Insights can interpret the date and time in your log file as the event start time. For more information about the Ruby strftime format, see https://ruby-doc.org/core-2.3.0/Time.html#method-i-strftime.
Log Filtering	
Log Filtering	You can create filters to notify Security Director Insights about malicious and unmalicious events as you decide what logs are to be kept and which ones can be ignored. Log filtering removes logs that are "noisy" and not of particular interest and retains logs that are related to malicious events. With these filters, you can select **exact match** or **contains** filter for the string you enter. Click **Add** and configure filtering conditions as follows: • Select a log file field from the list. • Select a suitable filter condition from the list such as Matches, Contains, Does not Contain, and so on. If you select Matches, your provided string must match the selected field exactly. If you select Contains, your provided string must appear as a substring within the selected field. • In the edit field, enter a string to filter log files, and then click **Add**. Click **OK** and your condition is added to the filter. You can add multiple filters. An "or" condition is applied to the list of filters; therefore, the order of filters is not relevant. **NOTE:** Select the check box for a filter and click **Delete** to remove that filter.
Conditions Assignment	

Table 17: Add New Log Parser *(continued)*

Setting	Guideline
Assign Conditions	You can assign different conditions to an event, based on the filtering parameters you configure. • Event Severity—Assign conditions to define the severity of an event. Click **Add** and set conditions as follows: ◦ Select a severity level. The options are Benign, Low, Medium, High, and Critical. ◦ Select a field from the list to set the severity level for that field. ◦ Select a condition. For example, If you select Matches, your string must match the selected field exactly. If you select Contains, your string must appear as a substring within the selected field. ◦ In the edit field, enter a string to filter log files and click **Add**. • Progression—Assign conditions to define the progression of an event. Click **Add** and set conditions as follows: ◦ Select a progression level. The options are Phishing, Exploit, Download, Infection, and Execution. ◦ Select a field from the list to set the progression level for that field. ◦ Select a condition. For example, If you select Matches, your string must match the selected field exactly. If you select Contains, your string must appear as a substring within the selected field. ◦ In the edit field, enter a string to filter log files and click **Add**. • Blocked—Assign conditions to define the event is blocked or not. Click **Add** and set conditions as follows: ◦ Select a blocked level. The options are True and False. ◦ Select a field from the list to set the block level for that field. ◦ Select a condition. For example, If you select Matches, your string must match the selected field exactly. If you select Contains, your string must appear as a substring within the selected field. ◦ In the edit field, enter a string to filter log files and click **Add**.

RELATED DOCUMENTATION

About the Log Parsers Page | 42

Edit and Delete a Log Parser | 47

Import and Export Log Parsers | 48

Edit and Delete a Log Parser

IN THIS SECTION

You can edit and delete a log parser from the Log Parsers page.

Edit a Log Parser

To edit a log parser:

1. Select **Configure** > **Insights** > **Log Parsers**.

   The Log Parsers page appears.

2. Select the log parser that you want to edit, and click the pencil icon.

   The Edit Log Parser page appears, displaying the same fields that were presented when you added new log parsers.

3. Modify the log parser fields.

4. Click **Finish** to save your changes.

   You are taken to the Log Parsers page. A confirmation message appears, indicating the status of the edit operation.

Delete a Log Parser

To delete a log parser:

1. Select **Configure** > **Insights** > **Log Parsers**.

   The Log Parsers page appears.

2. Select a log parser that you want to delete and click the delete icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the log parser.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

- About the Log Parsers Page | 42
- Create a New Log Parser | 43
- Import and Export Log Parsers | 48

Import and Export Log Parsers

IN THIS SECTION

You can import and export log parsers into a standardized file that be stored and shared.

Import a Log Parser

To import a log parser

1. Select **Configure**>**Insights**>**Log Parsers**.

   The Log Parsers page appears.

2. Click **Import**.

   Browse your local system and select the log parser file to import. The log parser is imported and listed in the Log Parsers page.

Export a Log Parser

To import a log parser

1. Select **Configure**>**Insights**>**Log Parsers**.

   The Log Parsers page appears.

2. Select a log parser to export and click **Export**.

   The selected log parser is exported in a ZIP file and downloaded to the local system.

RELATED DOCUMENTATION

- About the Log Parsers Page | **42**
- Create a New Log Parser | **43**
- Edit and Delete a Log Parser | **47**

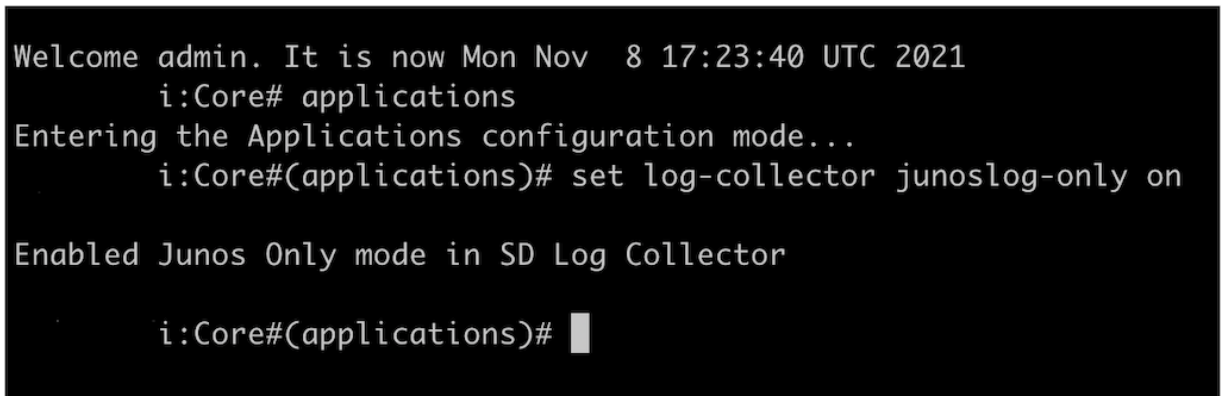
About the Log Sources Page

To access this page, select **Configure** > **Insights** > **Log Sources**.

Security products such as Juniper Secure Analytics (JSA) can act as a log source. You can create multiple log parsers for different log sources. The log source name is the hostname portion of the syslog message that Security Director Insights uses to identify the log source, and how Security Director Insights will parse its logged events.

Starting in Security Director Insights Release 21.3, you can enable Security Director log collector to receive logs from Junos only. Use the **set log-collector junoslog-only on** CLI command in the application mode, as shown in Figure 2 on page 50.

Figure 2: Enable Junoslog-Only Mode



Tasks You Can Perform

You can perform the following tasks from the Log Sources page:

- Add log sources. See “Add a Log Source” on page 51.
- Edit and delete log sources. See “Edit and Delete a Log Source” on page 52.
- View log statistics. See “View Log Statistics” on page 53.
- Enable or disable the third-party log sources by toggling the **Enable Third-Party Log Sources** option.

  If you enable this option, support for Junos Release 21.X logs is disabled. If you disable this option, support for Junos Release 21.X logs is enabled.

Field Descriptions

Table 18 on page 50 provides guidelines on using the fields on the Log Sources page.

Table 18: Fields on the Log Sources Page

Field	Description
Log Source Identifier	Specifies the unique string that needs to be looked for.
Parser	Specifies the name of the log parser assigned to that particular log source.
Severity	Specifies the severity of the log parser.

Table 18: Fields on the Log Sources Page *(continued)*

Field	Description
Actions	Specifies different actions that you can take for a log source.

RELATED DOCUMENTATION

- Add a Log Source | 51
- Edit and Delete a Log Source | 52
- View Log Statistics | 53

Add a Log Source

Use the Add Log Source page to create a log source and assign the log parser with a severity level.

To add a log source:

1. Select **Configure** > **Insights** > **Log Sources**.

   The Log Sources page appears.

2. Click **Create**.

   The Add Log Source page appears.

3. Complete the configuration according to the guidelines provided in Table 19 on page 51.

4. Click **Save**.

   A new log source is created and listed on the Log Sources page.

Table 19: Fields on the Add Log Source Page

Setting	Guideline
Log Source Identifier	Enter a unique name for the log source.
Parser	Select a required log parser from the list.
SSL	You can enable or disable SSL.

Table 19: Fields on the Add Log Source Page *(continued)*

Setting	Guideline
Default Severity	Assign a default severity level from the list.

RELATED DOCUMENTATION

- About the Log Sources Page | 49
- Edit and Delete a Log Source | 52
- View Log Statistics | 53

Edit and Delete a Log Source

IN THIS SECTION

You can edit and delete log sources from the Log Sources page.

Edit a Log Source

To edit a log source:

1. Select **Configure**>**Insights**>**Log Sources**.

   The Log Sources page appears.

2. Select the log source that you want to edit, click the pencil icon.

   The Update Log Sources page appears, displaying the same fields that were presented when you added new log sources.

3. Modify the log source fields.

4. Click **Save** to save your changes.

   You are taken to the Log Sources page. A confirmation message appears, indicating the status of the edit operation.

Delete a Log Source

To delete a log source:

1. Select **Configure**>**Insights**>**Log Sources**.

   The Log Sources page appears.

2. Select the log source that you want to delete, click the delete icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the log source.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

- About the Log Sources Page | **49**
- Add a Log Source | **51**
- View Log Statistics | **53**

View Log Statistics

The counter for each log source shows the number of logs collected over five minutes, one hour, one day, one week intervals, and a total count, broken down by the fields you chose when creating the custom log parser.

To view logs statistics:

1. Select **Configure**>**Insights**>**Log Sources**.

The Log Sources page appears.

2. Click **Counters**.

   The All Logs page appears.

   The logs statistics may include the following information:

   - All Incoming Logs: Aggregate (lifetime), Last five minutes, Last one hour, Last twenty four hours, and Last seven days
   - All Created Events: Aggregate(lifetime), Last five minutes, Last one hour, Last twenty four hours, and Last seven days

3. Click **Reset** to reset the counter or **Close** to close the page.

RELATED DOCUMENTATION

About the Log Sources Page | 49

Add a Log Source | 51

Edit and Delete a Log Source | 52

About the Event Scoring Rules Page

To access this page, select **Configure** > **Insights** > **Event Scoring Rules**.

You can use the event scoring rules to customize the log event to match your security operation center (SOC) processes. Rules comprise the following elements:

- Condition—The rules engine supports several match operations for different field types. For example, the matching operations include conditions such as Matches, Contains, Greater Than, and Less Than. You can combine multiple matching criteria in an ANY (OR) configuration or an ALL (AND) configuration. To apply a condition, select a normalized field from the event and match the criteria that trigger the rule.
- Action—An action is a response to an event. You can configure, increase, or lower the severity or look up a threat intelligence source.

Tasks You Can Perform

You can perform the following tasks from the Event Scoring Rules page:

- Create an event scoring rule. See "Create an Event Scoring Rule" on page 56.
- Edit and delete an event scoring rule. See "Edit and Delete Event Scoring Rules" on page 57.
- Enable or disable an event scoring rule.

Field Descriptions

Table 20 on page 55 provides guidelines on using the fields on the Event Scoring Rules page.

Table 20: Fields on the Event Scoring Rules Page

Field	Description
Rule Name	Specifies the name of the rule.
Rule Description	Specifies the condition applied for the rule.
Match Any/All Rules	Specifies the matching criteria set for the rule.
Actions	Specifies the action to be taken when the condition of a rule is met.
Status	Specifies the status of the rule, whether enabled or disabled.

Click **Enable** or **Disable** to either enable the event scoring rule or disable it.

RELATED DOCUMENTATION

Create an Event Scoring Rule | 56
Edit and Delete Event Scoring Rules | 57

Create an Event Scoring Rule

You can create rules for the log events by defining the matching condition and corresponding actions to take when a condition is met.

To create a rule for scoring log events:

1. Select **Configure** > **Insights** > **Event Scoring Rules**.

   The Event Scoring Rules page appears.

2. Click the plus icon (+).

   A page appears, on which you can define the rule's condition and actions.

3. In the text box that appears at the top of the page, enter a unique name for the rule.

4. In the Condition section:
   - Select a matching condition from the list: **Match Any** or **Match All**.
   - Select the type of event from the list. You can select from options such as:
     - Detection Method
     - Endpoint IP
     - Endpoint User Name
     - Event Name
     - Event Severity
     - File Hash
     - File Name
     - File Path
     - HTTP Content-Type
     - HTTP Referer
     - HTTP Status
     - Log Severity
     - Progression
     - Signature ID
     - Threat Source Host Name
     - Threat Source IP

- Threat Source User Name
- URL
- URL Hostname
- URL Path
- URL Query
- URL Scheme
- Vendor Response

- For the selected event, select a condition from the list.
- For the selected condition, provide necessary additional data.
- If you are defining more than one condition, click **Add**.

5. In the Action(s) section:
   a. Select a required action from the list, such as Raise or Lower Severity (by 0.25, 0.50, 0.75, or 1.0), Set Severity (value), Check feed, and Skip remaining rules.
   b. For the selected action, assign the additional actions from the list.
   c. If you are defining more than one action, click **Add**.
6. Click **Confirm**.

   A new rule is created and listed on the Event Scoring Rules page.

RELATED DOCUMENTATION

About the Event Scoring Rules Page | 54
Edit and Delete Event Scoring Rules | 57

Edit and Delete Event Scoring Rules

IN THIS SECTION

You can edit and delete event rules from the Event Scoring Rules page.

Edit an Event Scoring Rule

To edit an event scoring rule:

1. Select **Configure** > **Insights** > **Event Scoring Rules**.

   The Event Scoring Rules page appears.

2. Select the rule that you want to edit, and click the pencil icon.

   An edit page appears, displaying the same fields that were presented when you created a new rule.

3. Modify the rule.

4. Click **Confirm** to save your changes.

   You are taken to the Event Scoring Rules page. A confirmation message appears, indicating the status of the edit operation.

Delete an Event Scoring Rule

To delete an event scoring rule:

1. Select **Configure** > **Insights** > **Event Scoring**.

   The Event Scoring Rules page appears.

2. Select the rule that you want to delete, and click the delete icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the rule.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

About the Event Scoring Rules Page | 54

About the Incident Scoring Rules Page

To access this page, select **Configure** > **Insights** > **Incident Scoring Rules**.

Use incident scoring rules to score the risk of an incident by verifying that the indicators of compromise are already blocked from execution or mitigated by other events that contributed toward this incident. Rules comprise the following elements:

- Condition—The only matching condition available for any field type is *mitigated by another event*.
- Action—An action is a response to an incident. You can raise or lower the severity, set the severity value, or skip the remaining rules.

Tasks You Can Perform

You can perform the following tasks from the Incident Scoring Rules page:

- Create an incident scoring rule. See "Create an Incident Scoring Rule" on page 60.
- Edit and delete an incident scoring rule. See "Edit and Delete Incident Scoring Rules" on page 61.
- Enable or disable an incident scoring rule.

Field Descriptions

Table 21 on page 59 provides guidelines on using the fields on the Incident Scoring Rules page.

Table 21: Fields on the Incident Scoring Rules Page

Field	Description
Rule Name	Specifies the name of the rule.
Rule Description	Specifies the condition applied for the rule.
Match Any/All Rules	Specifies the match criteria set for the rule.

Table 21: Fields on the Incident Scoring Rules Page *(continued)*

Field	Description
Actions	Specifies the action to be taken when the condition of a rule is met.
Status	Specifies the status of the rule, whether enabled or disabled.

RELATED DOCUMENTATION

Create an Incident Scoring Rule | 60

Edit and Delete Incident Scoring Rules | 61

Create an Incident Scoring Rule

You can create rules for incidents by defining the matching condition and corresponding actions to take when a condition is met.

To create a rule for scoring incidents:

1. Select **Configure** > **Insights** > **Incident Scoring Rules**.

   The Incident Scoring Rules page appears.

2. Click the plus icon (+).

   A page appears, on which you can define the rule's condition and actions.

3. In the Rule Description field, enter a unique name for the rule.

4. In the Condition section:

   a. Select a matching condition from the list: **Match Any** or **Match All**.

   b. Select the type of incident from the list: **File Hash**, **Threat Source IP**, or **URL**.

   c. For the selected incident, select **mitigated by another event** as the condition.

   NOTE: To add multiple conditions, click **Add**.

5. In the Action(s) section:
   a. Select a required action from the list, such as Raise or Lower Severity (%), Set Severity (value), or Skip remaining rules.
   b. Based on the action you have selected, provide additional data.

   NOTE: To add multiple actions, click **Add**.

6. Click **Confirm**.

   A new rule is created and listed in the Incident Scoring Rules page.

Click **Enable** or **Disable** to either enable the incident scoring rule or disable it.

RELATED DOCUMENTATION

About the Incident Scoring Rules Page | 59
Edit and Delete Incident Scoring Rules | 61

Edit and Delete Incident Scoring Rules

IN THIS SECTION

You can edit and delete an incident scoring rule from the Incident Scoring Rules page.

Edit an Incident Scoring Rule

To edit an incident scoring rule:

1. Select **Configure** > **Insights** > **Incident Scoring Rules**.

   The Incident Scoring Rules page appears.

2. Select the rule that you want to edit, and click the pencil icon.

   An edit page appears, displaying the same fields that were presented when you created a new rule.

3. Modify the rule.

4. Click **Confirm** to save your changes.

   You are taken to the Incident Scoring Rules page. A confirmation message appears, indicating the status of the edit operation.

Delete an Incident Scoring Rule

To delete an incident scoring rule:

1. Select **Configure** > **Insights** > **Incident Scoring Rules**.

   The Incident Scoring Rules page appears.

2. Select the rule that you want to delete, and click the delete icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the rule.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

About the Incident Scoring Rules Page | 59

Create an Incident Scoring Rule | 60

4

CHAPTER

Monitor

How to Monitor Incidents

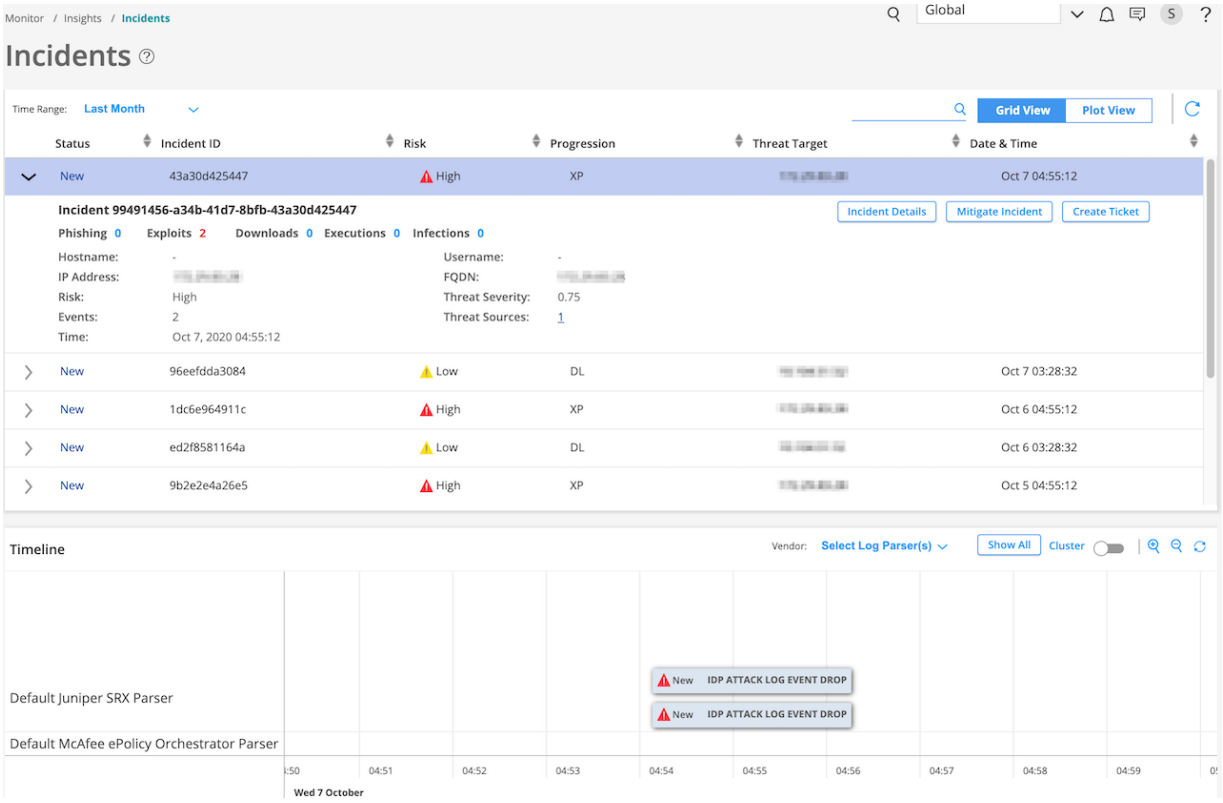
Use the Incidents page to view all incidents related to an endpoint in a user timeline view. To access the Incidents page, select **Monitor** > **Insights** > **Incidents**.

There are two ways to view your data. You can select either the Grid view or the Plot view. By default, the data is displayed in Grid view. In the Timeline section, you can select a log parser from the list to view log data in the timeline graph. You can zoom in, zoom out, show all data, and refresh the data.

Grid View

Click **Grid View** for a comprehensive details about incidents. You can view the incident ID, state of the incident, progression, and so on. You can expand an incident to view more details and create ServiceNow tickets if required, as shown in Figure 3 on page 64.

Figure 3: Grid View for Incidents



After you create a ticket, the status of the incident changes to Acknowledged, as shown in Figure 4 on page 65

Figure 4: Incidents Status Changed

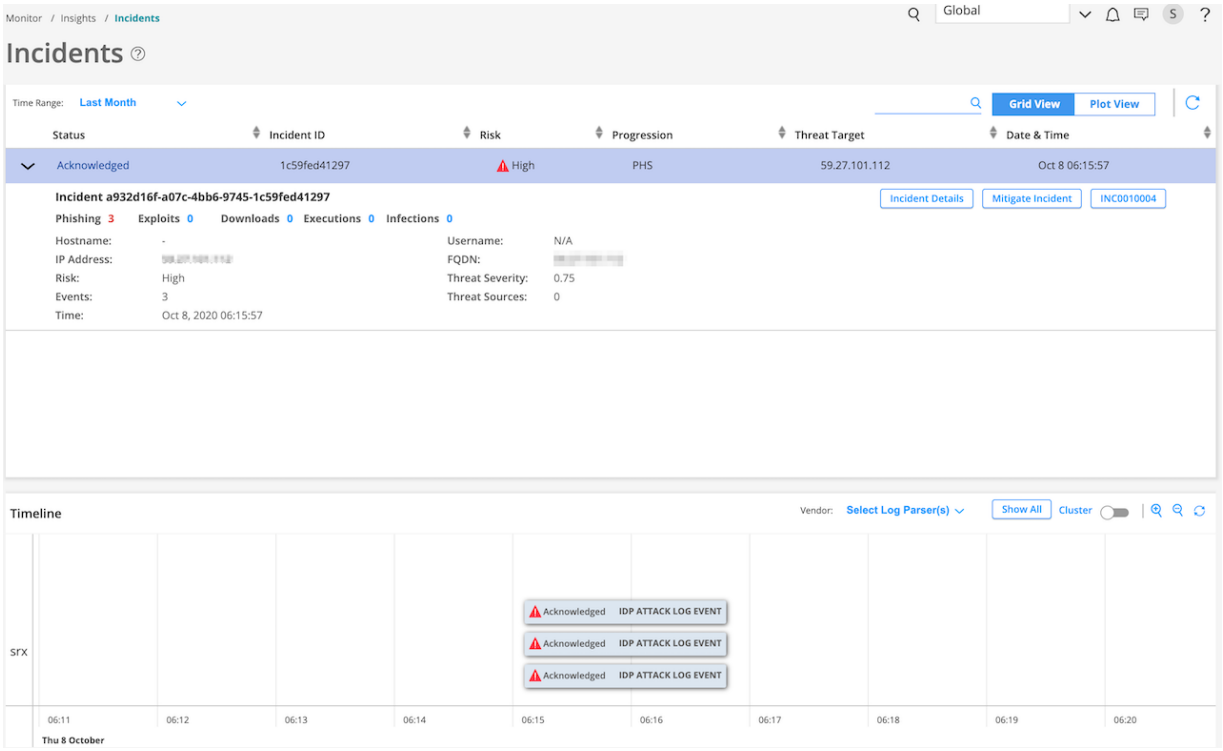


Table 22 on page 65 describes different fields available in this view. You can view data for a custom time range, last 24 hours, last week, last month, and last year.

Table 22: Fields on the Grid View Page

Field Name	Description
Status	Specifies the status of the ServiceNow ticket. After you create a ServiceNow ticket, the status shows Acknowledged, as shown in Figure 4 on page 65.
Incident ID	Specifies the incident ID.
Risk	Specifies the threat metric and severity rating.
Progression	Specifies the progression of an incident
Threat Target	Specifies the IP address of the targeted host.
Date & Time	Specifies the timestamp of the incident.

In the Status column, click **>** to see additional details (apart from details provided in Table 22 on page 65) about an incident, such as:

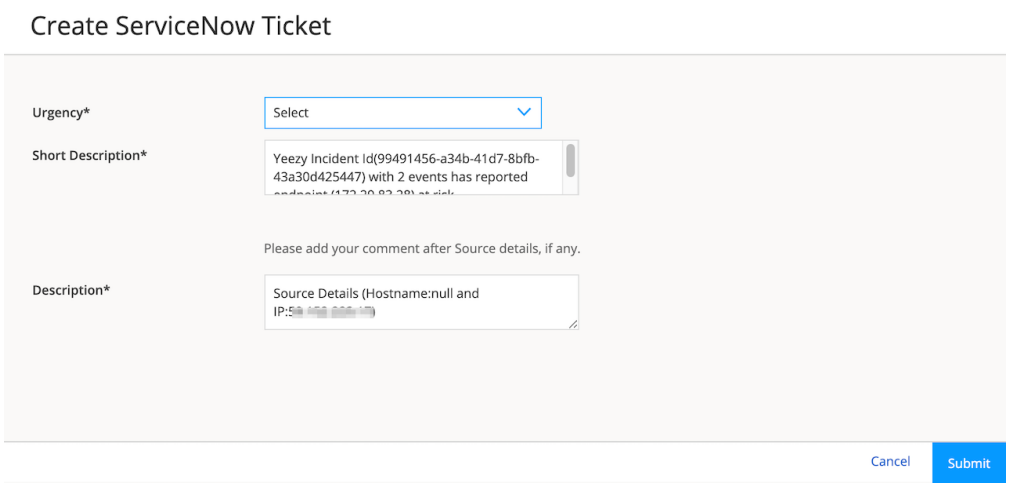
- Hostname—If Juniper Identity Management Service (JIMS) is configured, the hostname is shown.
- Username—If JIMS is configured, the username is shown.
- IP address
- Number of events that contributed to an incident
- Fully qualified domain name (FQDN)
- Threat severity value
- Number of threat sources associated with the Incident

Table 23 on page 66 explains the other options available for each incident.

Table 23: Options for Each Incident

Option	Description
Incident Details	Select **Incident Details** to see the following information about an incident: • Name of the incident • Source IP address of the incident • Date and time of the event • Vendor response for the event • Name of the log parser • Progression details • Detection method • Endpoint IP address • Raw log of the event • Starting and ending severity levels
Mitigate Incident	Select **Mitigate Incident** to enable the mitigation if it's disabled and vice versa. To mitigate incidents, you must have already configured ATP Cloud or Policy Enforcer. For more information about mitigation settings, see "Configure Mitigation Settings" on page 29

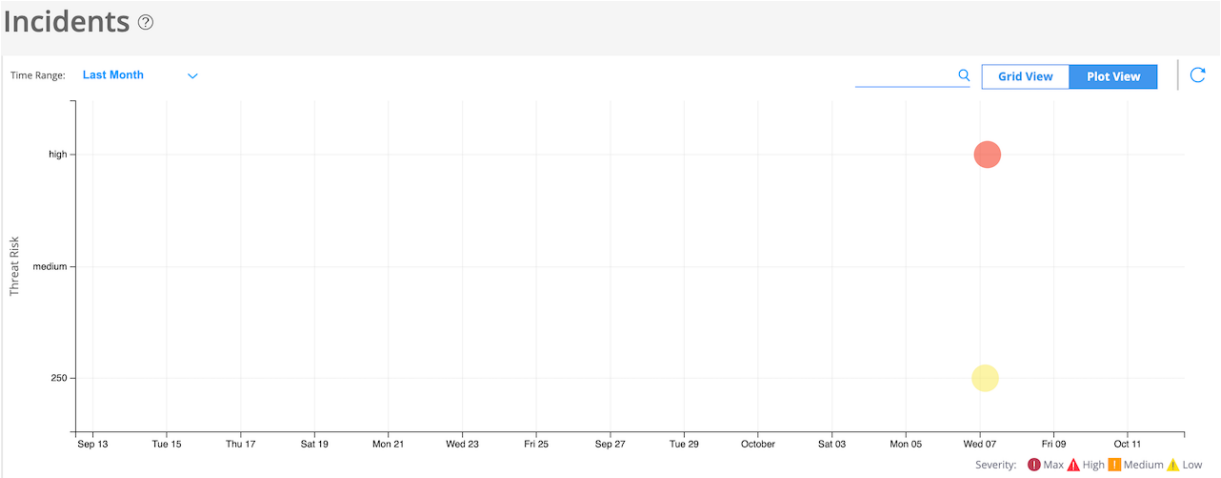
Table 23: Options for Each Incident *(continued)*

Option	Description
Create Ticket	You can create a ServiceNow ticket for an incident. You must have already configured ServiceNow settings to create a ServiceNow ticket. See "About the ServiceNow Configuration Page" on page 34. To create a ServiceNow ticket: 1. Select **Create Ticket**. The Create ServiceNow Ticket page appears, as shown in Figure 5 on page 67. **Figure 5: Create ServiceNow Ticket Page**  2. In the Urgency field, select the priority of the ticket from the list. 3. In the Short description field, provide a short description about the incident. 4. In the Description field, provide a more detailed description about the incident. 5. Click **Submit**.

Plot View

Click the **Plot View** link for a brief summary of incidents represented in a soar bubble chart. Each bubble represents a host and the bubble size is proportional to the number of threats, as shown in Figure 6 on page 68.

Figure 6: Incident Plot View



You can view data for a custom time range, last 24 hours, last week, last month, and last year.

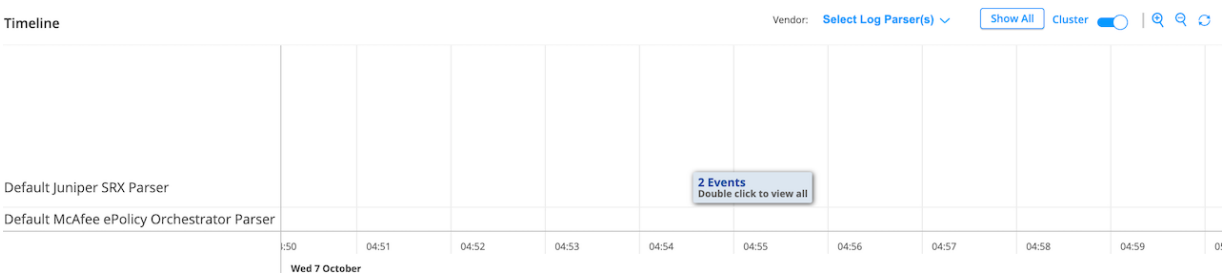
Timeline View

You can view all incidents on a timeline graph. Hover over each event to see more details about an incident. In the Select Log Parser(s) list, you can select the required log parser. You can select either one or all the log parsers. By default, the timeline graph shows all of the configured vendors in the log source.

Click **Show All** to see all events associated with an endpoint in the selected time range.

You can enable the **Cluster** option to cluster events belonging to the same time, as shown in Figure 7 on page 69.

Figure 7: Cluster View of Incidents



You can also zoom in, zoom out, and reset the data in the timeline graph. The reset option shows events for the corresponding incidents.

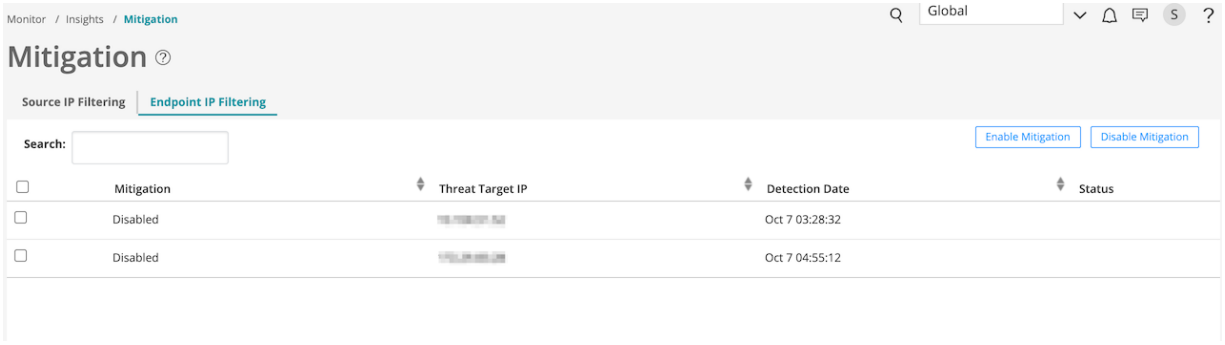
RELATED DOCUMENTATION

- About the ServiceNow Configuration Page | **34**
- About the Incident Scoring Rules Page | **59**
- Create an Incident Scoring Rule | **60**

How to Monitor Mitigation

Using the Mitigation page, you can view the list of endpoints and threat sources that are mitigated by Security Director Insights. To access this page, select **Monitor** > **Insights** > **Mitigation**. You can select an event and disable the mitigation, if enabled, and vice versa, as shown in Figure 8 on page 69.

Figure 8: Mitigation Page



You can mitigate threat source IP addresses through ATP Cloud or Policy Enforcer. You must configure ATP Cloud or Policy Enforcer to enable the mitigation. For more information about mitigation settings, see “Configure Mitigation Settings” on page 29.

You can perform the following actions from the Mitigation page:

- Source IP filtering—Select the **Source IP Filtering** option to view only the threat source IP addresses that are mitigated by Security Director Insights.
- Endpoint IP filtering—Select the **Endpoint IP Filtering** option to view only the endpoint IP addresses that are mitigated by Security Director Insights.
- Search—You can search for data based on the mitigation status, threat source or target IP addresses, and detection date.
- Enable mitigation—If mitigation is disabled for an IP address, select an event for which you want to enable mitigation and click **Enable Mitigation**. The Status column shows whether the enable task is successful.
- Disable mitigation—If you want to disable mitigation for an IP address, select an event for which you want to disable mitigation and click **Disable Mitigation**. The Status column shows whether the disable task is successful or not.

RELATED DOCUMENTATION

Configure Mitigation Settings | 29