

Configure Alerts

Alerts in Secure Workload help you monitor workload security and respond to potential threats. The various components of alerts work together to provide visibility, alert sources and configuration, and the ability to send alerts from publishers. You can configure alerts, view alerts trigger rules, and choose publishers to send alerts. Alerts that are displayed on the configuration page vary depending on the user's role. Alert publishers can be either Alerts or Notifiers.

Table 1: Feature Information

Feature Name	Release	Feature Description	Where to Find
Alert Enhancements	3.9	On the Investigate > Alerts page. Other enhancements include: • Introduction of Alert Name field: A new	Alert Configuration Modal, on page 6
		field, Alert Name , is introduced to facilitate a structured approach to alert management, allowing you to assign unique names to alerts	
		 Introduction of drop-down for Alert Type: A new drop-down, Alert Type, is introduced in the Alerts – Configs page to facilitate quick filtering. 	
		• Icon Update: The configuration of alerts can now be initiated by selecting the new + icon on the Alerts – Configs page.	
		Multisearch capabilities with enhanced filtering options for alerts.	Current Alerts, on page 14



Note From the Secure Workload 3.0 release, the Secure WorkloadApp Store does not support alerts and compliance apps. You can configure alerts and the compliance alerts on this page without creating an Alert Application instance or Compliance Application instance.

- Alert Types and Publishers, on page 3
- Create Alerts, on page 4
- Alert Configuration Modal, on page 6
- Generate Test Alerts, on page 12
- Current Alerts, on page 14

• Alert Details, on page 16

Alert Types and Publishers

Alerts in Secure Workload consist of the following components:

- Alert Visibility
 - Current Alerts: From the navigation pane, choose Investigate > Alerts. Preview of alerts is sent to a Data Tap.

Figure 1: Current Alerts

ent Alerts							
guration Ø							
15		Type	Severity				
TIVE	×	COMPLIANCE+ 7 more	LOW+ 4 mo	Filter Alerts Switch to Advanced	0	Last 1 month	~
ent Time 🕹	Alert Name	ti.	Status	Alert Text 1	Severity 1	Type 11	Actions
							1000
w 9, 4:55 PM	ISE-Conne	ctor-Alert	ACTIVE	Missing ISE heartbeats, it might be down	HIGH	CONNECTOR	Z _Z , W
w 9, 4:55 PM	Syslog-Co	nnector-Alert	ACTIVE	Missing Syslog heartbeats, it might be down	HIGH	CONNECTOR	Z ^{zz} A
w 9, 4:55 PM	Slack-Conr	nector-Alert	ACTIVE	Missing Slack heartbeats, it might be down	HIGH	CONNECTOR	$Z^{\chi^{\chi}} \not \!$
w 9, 4:55 PM	ServiceNov	w-Connector-Alert	ACTIVE	Missing ServiceNow heartbeats, it might be down	HIGH	CONNECTOR	Z ^{Z²} #
w 9, 4:55 PM	Edge Appli	ance-Appliance-Down-Alert	ACTIVE	Missing Edge Appliance heartbeats, it might be down	HIGH	CONNECTOR	Z ^{Z²} #
	ent Alerts puration 0 is is int Time	Alerts guration O is TVIE v v 4.55 PM 53ec-Conne v v 4.55 PM Slack-Conne v v v 4.55 PM Slack-Conne v v 4.55 PM Edge Apple	Alerts Type ss Type TVE OOMPLIANCE+ 7 more ent Time 4 Alert Name 11 v 9, 4:55 PM SSE-Connector-Alert v 9, 4:55 PM Slack-Connector-Alert v 9, 4:55 PM Stack-Connector-Alert	Alerts Type Severity ss Type LDW+ 4 mo ant Time 4 Atert Name 11 Status v 9, 4:55 PM SBe-Connector-Alert ACTIVE v 9, 4:55 PM Sback-Connector-Alert ACTIVE v 9, 4:55 PM ServiceNow-Connector-Alert ACTIVE v 9, 4:55 PM ServiceNow-Connector-Alert ACTIVE v 9, 4:55 PM ServiceNow-Connector-Alert ACTIVE v 9, 4:55 PM Edge Appliance-Appliance-Down-Alert ACTIVE	ServiceNow Type ServiceNow Filter Alerts Switch to Advanced ss Type ServiceNow Eddward Switch to Advanced ust Type Subscription Switch to Advanced Switch to Advanced ust Mart Text 1: Switch to Advanced Switch to Advanced Switch to Advanced ust Advert Name 1: Status Atert Text 1: Switch to Advanced ust 4.55 PM Status ACTIVE Missing Size heartbeats, it might be down v 8, 4.55 PM Stack-Connector-Alert ACTIVE Missing Size heartbeats, it might be down v 8, 4.55 PM Stack-Connector-Alert ACTIVE Missing Size heartbeats, it might be down v 8, 4.55 PM Stack-Connector-Alert ACTIVE Missing ServiceNow heartbeats, it might be down v 8, 4.55 PM ServiceNow-Connector-Alert ACTIVE Missing Edge Appliance heartbeats, it might be down v 8, 4.55 PM Edge Appliance-Appliance-Down-Alert ACTIVE Missing Edge Appliance heartbeats, it might be down	ent Alerts guration O s s Type TVE COMPLIANCE+ 7 more COMPLIANCE+ 7 mo	ent Alerts puration O s s Type COMPLIANCE+ 7 more

- Alert Sources and Configuration:
 - Alerts Configuration: Choose Manage > Alerts Configs. Both alert configurations that are configured using the common modal and alert publisher, and notifier settings are displayed.

riuure z. Aleris - communation	Fiaure	2: Al	erts -	Config	uration
--------------------------------	--------	-------	--------	--------	---------



• Send Alerts:

- Alerts App: An implicit Secure Workload app that sends generated alerts to a configured Data Tap. The Alerts App handles features such as **Snooze** and **Mute**.
- Alerts Publisher: Limits the number of alerts that are displayed and pushes alerts to Kafka (MDT or DataTap) for external consumption.
- Edge Appliance: Pushes alerts to other systems such as Slack, PagerDuty, Email, and so on.

Create Alerts

From the navigation pane, choose **Alerts** > **Configuration** to configure the following alert types:

Figure 3: Create an Alert



• Enforcement Alerts

- Agent Reachability
- · Workload Firewall
- Workload Policy

Sensor Alerts

- Agent Upgrade
- Agent Flow Export
- Agent Check In
- Agent Memory Usage
- Agent CPU Quota
- · Amount Of Flow Observations
- New Agent Registered
- Pcap Status
- Agent Uninstalled
- Not Recommended Cipher

- Deprecated TLS Version
- Agent Auto Removal

Compliance Alerts

- Enforcement Policy
- Live Analysis Policy



Note

- Alert trigger rules are enforced on the currently selected root scope for the Enforcement and Sensors alert types.
- You must have an enforced capability on the currently selected scope to create an alert trigger rule for the Compliance alert type.

The following Alert Types do not have a configuration modal:

- Forensics
- Connectors
- Traffic

Traffic Alerts

You can create **Traffic** alerts to be notified when workloads communicate with known malicious IPv4 addresses. By default, the option to detect malicious addresses are disabled. To enable, see Visibility of Well-Known Malicious IPv4 Addresses. The available alert conditions are:

- Malicious flows are Observed: Communication to the known malicious IPv4 addresses is observed.
- Malicious flows are Permitted: After the policy analysis and enforcement, this condition notifies about the malicious flows which are permitted.
- Malicious flows are Rejected: After the policy analysis and enforcement, this condition notifies about the malicious flows which are rejected.

Alert Configuration Modal

The Alert configuration modal consists of the following sections:

- The Alert Name
- The Alert Types
- The *subject* of an alert. The subject depends on the app, and may be prepopulated when the alert modal is contextual.
- The **Alert Condition** on which an alert is triggered. Hover over the **info** icon to view a list of available conditions.

- If there are several alerts that are generated, alerts with higher *Severity* are displayed preferentially over alerts with lower severity.
- · Click Show Advanced Settings for more configuration options.



Note

- Upon completion of the upgrade, all existing alert configuration rules in the current tenants are assigned with an Alert Name based on the predefined format. In instances where the Alert Name is absent, the format to be employed is *Alert_SubType_{DatabaseID}*. For example, Workload_Firewall_64bf9b8493dfc94ca0095718.
 - Following deployment or upgrade, all default alert configuration rules—those created during the inception of a new tenant—are assigned with an Alert Name in the predefined format: *Alert_SubType*. For example, Upgrade_Status.

Figure 4: Configure Alerts

e e . mgu	ire Complia	ance Aler	ts		×
Alert Name	• 0				
Alert Type	s 🕕				
Enforcer	ment Policy	Live Anal	lysis Policy		
For Enforce	ed Application	n:/	0		
Alert Cond	lition 🕕				
condition	> value			×	
Severity		1			

Summary Alerts

Summary Alerts are allowed for some applications and configuration options depend on the application.

- **Individual Alerts** refers to alerts that are generated over non-aggregated (or minimally aggregated) information and are likely to have a time range of one minute. Note that this does not necessarily mean the alerts are actually generated and sent at a minute interval; the individual alerts can still be generated at the *App Frequency* interval.
- Summary Alerts refers to alerts generated over metrics produced over an hour or to the summarization of less frequent alerts.

Арр	App Frequency1	Individual Alerts	Hourly Alerts	Daily Alerts
Compliance	Minute	Yes: at app frequency	Summary of Individual	Summary of Individual
Enforcement	Minute	Yes: at app frequency	Summary of Individual	Summary of Individual
Sensors	Minute	Yes: at app frequency	Summary of Individual	Summary of Individual



The Event Time of summary alerts represents the first occurrence of the same type alert over the past hour or a specified interval window.

Summarization Versus Snoozing

Summarization applies to the entire set of alerts generated according the alert configuration, while snoozing applies to a specific alert. This distinction is minor when the alert configuration is very specific, but is notable when the alert configuration is broad.

- For example, Compliance configuration is quite broad: an application workspace, and on which type of violation an alert should be generated. Thus, summarization would apply to all alerts triggered by a 'escaped' condition, while snoozing would apply to a very specific consumer scope, provider scope, provider port, protocol, and the escaped condition.
- On the opposite end, a platform alert configured to alert on a path between source scope and destination scope with a hop count less than some amount, will generate a very specific alert.

Other distinctions:

- Snoozing only results in an alert being sent when a new alert is generated after the snooze interval has passed. There is no indication of how many suppressed alerts might have occurred during the snooze interval.
- A summary alert is generated at the specified frequency, as many as alerts were generated within that interval. Summary alerts provide a count of the number of alerts triggered within the window, along with aggregated or range metrics.

Secure Workload Alerts Notifier (TAN)



Note

te Starting Secure Workload Release 3.3.1.x, TAN is moving to Secure Workload Edge Appliance.

Alert Notifiers provide capabilities to send alerts through various tools such as Amazon Kinesis, Email, Syslog, and Slack in the currently selected scope. As a Scope Owner or Site Admin, each notifier can be configured with required credentials and other information specific to the notifier application.

Configure Notifiers

To configure notifiers, you must configure the alert-related connectors. The connectors can only be configured after a Secure Workload Edge Appliance is deployed. For more information on deploying Secure Workload Edge appliance, see Virtual Appliances for Connectors.

After the Secure Workload Edge appliance is set up, you can configure each notifier with its specific required input. After the Secure Workload Edge appliance is set up, you will be able to see dashed lines connecting Alert Types to Alerts publisher. This is because the notifier is built on the Alerts publisher.

After the Secure Workload Edge appliance is set up, you can configure each notifier with the required input. After the Secure Workload Edge appliance is set up, you are able to view the dashed lines connecting Alert Types to Publisher. This is due the fact that notifier is built on the Publisher.

App Frequency is approximately how often the application runs and generates alerts. For example, Compliance has a flexible run frequency, and may actually compute alerts over a couple minutes together.

Choose Alert Publishers

Scope Owners and Site Admins can choose Publishers to Send alerts. Publishers include Kafka (Data Tap) and Notifiers.

All the available Publishers are displayed in the **Alerts - Configuration** window, including the **Alerts** and **Active Notifiers**. You can toggle the **Send** icon to choose the **Publishers** for the alert type. **Minimum Alert Severity** refers to the severity level an alert must reach to be sent through the **Publishers**.



Figure 5: Choose Alert Publishers



Note

TaaS clusters have a maximum number of alerts that can be processed of up to 14000 alerts per minute batch. This could also be reduced by choosing external data taps.

External Syslog Tunneling Moves to TAN



Starting the 3.1.1.x release, the syslog tunneling feature moves to TAN. To configure syslog for getting platform level syslog events, you must configure TAN on the Secure Workload Edge appliance on default rootscope. When the Secure Workload Edge appliance is configured on the default rootscope, you can set up the syslog server. To enable platform alerts, enable syslog notifications for Platform. This can be done by enabling Platform Syslog connection.

For details about how to configure syslog, see Syslog Connector.

Connection Chart

The connection chart displays the connections between **Alert Types** and **Publishers**. After you choose a publisher for an alert type, a blue line is established between the alert type and publisher. Note that the line pointing to the Internal Kafka (Data Tap) is always a line created using dashes as it represents an internal mechanism of how alert notifications are built upon.



Figure 6: Connection Chart

L

View Alerts Trigger Rules

You can view a list of all the configured Alerts Trigger Rules on the **Alerts - Configuration** page. You can also perform the following tasks:

- You can filter the rules by Alert Type and other properties.
- In the Actions column, click the pencil icon to modify the details such as Alert Name, Alert Types, Alert Condition, Severity and so on.
- Click See All Configured [alert type] Alerts to view all the alerts of the selected Alert Type in a new tab.

Figure 7: View Alerts Trigger Rules

All	*	Enter attributes	×	Fil	ter Alerts
Alert Type †↓	Alert N	ame †l	Configuration 1	Acti	ions †1
ENFORCEMENT	Agent_ 7dc4a	Not_Reachable_653 5da30b497a94de63	Scope : Default when Agent not Reachable (seconds) > 300	¥	/
ENFORCEMENT	Worklo 4a5da	ad_Firewall_6537dc 30b497a94de64	Scope : Default when Firewall = Off	¥	/
ENFORCEMENT	Worklo s_653 de65	ad_Policy_Deviation 7dc4a5da30b497a94	Scope : Default when Policy = Deviated	¥	/
SENSORS	Upgrad 5da30	le_Status_6537dc4a b497a94de66	Scope : Default when Agent Upgrade Status = Failed	¥	/
SENSORS	lface_l 6537d 67	Flow_Export_Status_ c4a5da30b497a94de	Scope : Default when Agent Flow Export Status = Stopped	¥	/
SENSORS	Upgrad 37dc4	le_Srv_Check_In_65 a5da30b497a94de68	Scope : Default when Agent Check-In Service = Inactive	¥	/
SENSORS	Agent c4a5d	Mem_Usage_6537d 130b497a94de69	Scope : Default when Deep Visibility Memory Usage (MB) > 512 and Enforcement Memory Usage (MB) > 512 and Forensic Memory Usage (MB) > 256	¥	/
SENSORS	Agent, 4b5da	Cpu_Quota_6537dc 30b497a94de6a	Scope : Default when Deep Visibility CPU Quota (%) > 3 Enforcement CPU Quota (%) > 3 Forensic CPU Quota (%) > 3	¥	/
SENSORS	Amt_C	f_Flow_Obs_6537dc	Scope : Default when	¥	/

The Alerts Trigger Rules window is used to filter alerts trigger rules by Alert Type and trigger condition.



Note Alert trigger condition is an exact match condition.

Alerts Trigger Rules Details

Click a row in the Alerts Trigger Rules section to view the configuration details.

- 1. Alert Type: Type of the alert.
- 2. Alert Name: Name of the alert.

3. Configuration: The condition when an alert is triggered in a particular scope.

You can also view other details such as **Severity**, **Individual Alerts**, and **Summary Alert Frequency**. *Figure 8: Alert Configuration Details*

AII	Enter attribute	s		× Filter Alerts
Alert Type 1↓	Alert Name 🗍	Configurat	tion 1	Actions 1
ENFORCEMENT	Agent_Not_Reachable_	Scope : D Agent r	efault when not Reachable (seconds) > 300	1/
		Detail	s	
	Individ	Severity M Jual Alerts E	ledium nable	
	Summary /	Alert Freq. N	lone	
SENSORS	Summary J Upgrade_Status_6537dc4a	Alert Freq. N Scope : D Agent L	lone Iefault when Jpgrade Status = Failed	1/
SENSORS	Summary / Upgrade_Status_6537dc4a	Alert Freq. N Scope : D Agent I Detail	lone lefault when Jpgrade Status = Failed S	1/
SENSORS	Summary / Upgrade_Status_6537dc4a	Alert Freq. N Scope : D Agent I Detail	lone lefault when Jpgrade Status = Failed S Medium	17

Generate Test Alerts

The primary usage of generating a test alert is to verify the connectivity with the publisher. You can configure a test alert to send alerts based on the alert type and linked publisher in the alert configuration.



Note

- Generating test alerts is not from the actual sources and is generated for test purpose only.
 - Test alerts can be generated for alert types which are linked to at least one publisher.

To generate a test alert, follow the steps below:

Procedure

- **Step 1** From the navigation pane, choose **Manage** > **Workloads** > **Alerts Config**.
- **Step 2** To configure a test alert, click **Test Alert**.

est Alert		
	Alert Name 🜒	
Keys	Name for the alert	
Scope	Alert Key	
Details	Aa1234Zz	
Details	Event Time	
Configuration	10/11/2023, 05:15:37.705 PM	
	Alert Time (optional)	
	10/11/2023, 05:15:37.705 PM	
	Alert Severity	
	LOW	
	Alert Type	
	Choose one	
	COMPLIANCE	
	FORENSICS	
	SENSORS	
	ENFORCEMENT	
	CONNECTOR	

Figure 9: Test Alert Configuration

- **Step 3** Under the **Keys** tab, enter the value for Alert Key and choose the values for Event Time, Alert Time, Alert Severity and Alert Type.
- **Step 4** Under the **Scope** tab, the values of Scope ID and Tenant ID are autogenerated based on the current scope.
 - **Note** If the Tenant ID is the same as Tenant ID VRF, then the system automatically checks the Tenant ID VRF check box.
- **Step 5** Under the **Details** tab, enter the values for Alert Text, Event Notes, Alert Details, and Alert Configuration ID.
 - **Note** Alert Details can be string or data in JSON format.

Options for JSON content are:

- a. Containing fields expected by that type of alert.
- Any sample JSON data, if that alert type does not expect default json fields.
 Sample JSON:

{"alert name ":"sample","alert category":{"severity": "dummy"}}

Step 6 Under the **Configuration** tab, choose the value for Individual Alert, Alert Frequency, and Summary Alert Frequency.

For individual alerts, choose ENABLE or DISABLE from the drop-down.

Alert frequency is autoselected with frequency as INDIVIDUAL.

Note It supports only individual alerts and does not consider summarization.

Summary alert is autoselected to NONE.

Step 7 To generate the test alert, click **TEST**.

Note A test alert is generated and sent to the configured publisher.

Current Alerts

Navigate to the **Investigate** > **Alerts** page to view the list of all active alerts. You can filter the alerts by **Status**, **Type**, **Severity**, and Time Range.

Only alerts with severity set to IMMEDIATE_ACTION, CRITICAL, HIGH, MEDIUM, or LOW are displayed on the **Current Alerts** page. All alerts irrespective to the severity values are sent to the configured Kafka broker.

Figure 10: Current Alerts

	Type	s	everity						
~	COMPLIANCE+ 7 more	~][LOW+ 4 more	~	Filter Alerts	Switch to Advanced	0	Last 1 month	
Alert Name	11	8	itatus	Alert Text 1			Severity 1	Type 11	Actions
ISE-Conne	ctor-Alert	A	CTIVE	Missing ISE heartbea	its, it might be dow	n	HIGH	CONNECTOR	Z ^{Z²} #
Syslog-Co	nnector-Alert	A	CTIVE	Missing Syslog heart	beats, it might be d	lown	HIGH	CONNECTOR	$Z^{\chi^{\chi}} \not \!$
Slack-Con	nector-Alert	A	CTIVE	Missing Slack hearth	eats, it might be do	own	HIGH	CONNECTOR	$\mathbb{Z}^{\mathbb{Z}^{X}} \bigstar $
ServiceNov	w-Connector-Alert	A	CTIVE	Missing ServiceNow	heartbeats, it migh	t be down	HIGH	CONNECTOR	Z ^{Z²} &
Edge Appli	ance-Appliance-Down-Alert	A	CTIVE	Missing Edge Applia	nce heartbeats, it n	night be down	HIGH	CONNECTOR	Z ^{Z²} #
	Alert Name ISE-Conne Syslog-Co Slack-Con ServiceNov Edge Appli	Type ODMPLIANCE + 7 more Alert Name 11 ISE-Connector-Alert Syslog-Connector-Alert Slack-Connector-Alert Slack-Connector-Alert Slack-Connector-Alert ServiceNow-Connector-Alert Edge Appliance-Appliance-Down-Alert	Type S COMPLIANCE+ 7 more S Alert Name S ISE-Connector-Alert A Syslog-Connector-Alert A Slack-Connector-Alert A ServiceNow-Connector-Alert A ServiceNow-Connector-Alert A Edge Appliance-Appliance-Down-Alert A	Type Severity OOMPLIANCE+ 7 more LOW+ 4 more Alert Name 11 Status ISE-Connector-Alert ACTIVE Syslog-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE	Type Severity COMPLIANCE+ 7 more LOW+ 4 more Alert Name 11 Status Alert Name 11 Status ISE-Connector-Alert ACTIVE Syslog-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE	Type Severity OOMPLIANCE+ 7 more LOW+ 4 more Alert Name 11 Blatus Alert Text 11 Blatus ISE-Connector-Alert ACTIVE Missing State Active Syslog-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Stack-Connector-Alert ACTIVE Missing Stack heartbeats, it might be down the stream the stack is might be down to the stream the stack is might be down to the state st	Type Severify COMPLIANCE+ 7 more LOW+ 4 more Alert Name 11 Status Alert Name 12 Status Alert Text 13 Status Status Alert Text 13 ISE-Connector-Alert ACTIVE Missing Size heartbeats, it might be down Sizek-Connector-Alert ACTIVE Missing Sizek heartbeats, it might be down Sizek-Connector-Alert ACTIVE Missing Sizek heartbeats, it might be down ServiceNow-Connector-Alert ACTIVE Missing ServiceNow heartbeats, it might be down Edge Appliance-Appliance-Down-Alert ACTIVE Missing Edge Appliance heartbeats, it might be down	Type Severity Filter Alerts Switch to Advanced ✓ COMPLIANCE+ 7 more LOW+ 4 more Filter Alerts Switch to Advanced C Alert Name 11 Status Alert Text 11 Severity 11 Severity 11 ISE-Connector-Alert ACTIVE Missing Size heartbeats, it might be down HIGH Syslog-Connector-Alert ACTIVE Missing Sizek heartbeats, it might be down HIGH Sizek-Connector-Alert ACTIVE Missing Sizek heartbeats, it might be down HIGH Sizek-Connector-Alert ACTIVE Missing SeviceNow heartbeats, it might be down HIGH Sizek-Connector-Alert ACTIVE Missing SeviceNow heartbeats, it might be down HIGH Edge Appliance-Appliance-Down-Alert ACTIVE Missing Edge Appliance heartbeats, it might be down HIGH	Type Severity Filter Alerts Switch to Advanced Last 1 month Alert Name 11 Status Alert Text 11 Switch to Advanced Swerity 11 Type 11 ISE-Connector-Alert ACTIVE Missing ISE heartbeats, it might be down HIGH CONNECTOR Syslog-Connector-Alert ACTIVE Missing Syslog heartbeats, it might be down HIGH CONNECTOR Stack-Connector-Alert ACTIVE Missing Syslog heartbeats, it might be down HIGH CONNECTOR Stack-Connector-Alert ACTIVE Missing Stack heartbeats, it might be down HIGH CONNECTOR Stack-Connector-Alert ACTIVE Missing Stack heartbeats, it might be down HIGH CONNECTOR Stack-Connector-Alert ACTIVE Missing ServiceNow heartbeats, it might be down HIGH CONNECTOR Edge Appliance-Appliance-Down-Alert ACTIVE Missing ServiceNow heartbeats, it might be down HIGH CONNECTOR

Filter Alerts by Time Range

- 1. Choose a range from the drop-down list. The default value is 1 month.
- 2. Click **Custom** and fill in the **From** and **To** dates to configure a custom range. Click **Apply**. Note that when a custom time range is selected, the **Refresh** button is disabled.

Advanced Filtering

- 1. Click Switch to Advanced.
- 2. Enter the attributes to filter. Hover over the **info** icon to view the properties to filter.

The alert filters are not retained when you switch back to the basic options.

View Additional Alert Details

You can view more details by clicking an alert.

Figure 11: Alert Details

00	ana
Name	SLACK
Туре	SLACK
Appliance ID	653a32375da30b0faaa111ef
Connector ID	653a34111af9610a1686ef48
Connector IP	172.21.158.125/24
Last Checkin At	Nov 07 2023 10.03.51 AM UTC

- Only 60 alerts per minute per root scope are displayed. A higher volume of alerts result in an alert type called Summary Alerts, with a count of alerts that are not displayed.
- There is a maximum number of alerts that are displayed at any point in time; older alerts are dropped as new alerts come in.

For more information, see Limits.

Snooze Alerts

The Alerts App allows alerts of the same type to be snoozed for a chosen amount of time. The type of the alert is defined differently depending on the workspace that the alert has currently been configured for. For example, the Compliance alert type is defined as the four tuples: consumer scope, provider scope, protocol, and provider port.



Note Currently, you cannot snooze or mute the user app-created alerts.

Snooze or Mute an Alert

Snooze Alerts:

- 1. Under Actions, click the Snooze icon.
- 2. Choose an interval from the drop-down.
- 3. Click Snooze.

Figure 12: Snooze an Alert

urrent Alerts						
Configuration ()						
Status	Type	Severty				
ACTIVE	COMPLIANCE+ 7 more	 LOW+ 4 mp 	Ve v Filter Alerta Switch to Advanced		Last 1 month	~
Event Time +	Alart Hama 1	Status	Alart Taxt 1.	Security 1	Type 1:	Actions
Nov 10, 4:50 PM	Stack-Connector-Alert	ACTIVE	Missing Sack heartbeats. It might be down	1804	CONNECTOR.	1" A
Nov 10, 4:59 PM	Edge Appliance - Appliance - Ocean - Alen	ACTN	Missing Edge Appliance heartheam, it might be about	1824	CONNECTO	Snonze an allert
Nov 10, 4:59 PM	Syslog-Connector-Alert	ACTIVE	Missing Systep tearbeats, it night its down	1824	CONNECTOR	2" 4
Nov 10, 4:59 PM	Syslog-Connector-Alert	ACTIVE	Missing Sysing Rear/beats, it might be down	HIGH	CONNECTOR	2" A
Nov 10, 4:58 PM	ServiceNow-Connector-Alert	ACTIVE	Missing ServiceNow heartbeats, it might be down	HIGH	CONNECTOR	Add into muled
Nov 10, 4:59 PM	ttill-Connector-Alert	ACTIVE	Missing ttill heartbeats, it might be down	нон	CONNECTOR	2° #

Mute Alert:

Use the mute option to stop receiving alerts.

- 1. Under Actions, click the Mute icon.
- 2. To confirm, click Yes.

To unmute, remove the alert from the muted list. Use the **Status** filter drop-down to view all **MUTED** alerts and unmute the required alter.



You can view up to 5000 muted or snoozed alerts in a scope.

Admiral Alerts

Admiral is an integrated alerting system, which replaces Bosun from earlier releases. For more information, see the Admiral Alerts section.

Alert Details

Common Alert Structure

All alerts follow an overall common structure. The structure corresponds to the json message structure available through Kafka DataTaps.

Field	Format	About
root_scope_id	string	Scope Id corresponding to top scope in scope hierarchy.
key_id	string	id field used for determining 'similar' alerts. Identical key_id's can be snoozed.
type	string	Type of the alert. Fixed set of string values: COMPLIANCE, USERAPP, FORENSICS, ENFORCEMENT, SENSOR, PLATFORM, FEDERATION, CONNECTOR
event_time	long	timestamp of when the event triggered (or if event spanned a range, then the beginning of the range). This timestamp is in epoch milliseconds (UTC).

Field	Format	About
alert_time	long	Timestamp of when the alert was first attempted to be sent. This will be after the timerange of the event. This timestamp is in epoch milliseconds (UTC).
alert_text	string	Title of the alert.
alert_text_with_names	string	Same content as alert_text but with any id fields replaced by corresponding name. This field may not exist for all alerts.
severity	string	Fixed set of string values: LOW, MEDIUM, HIGH, CRITICAL, IMMEDIATE_ACTION. This is the severity of the alert. For some types of alerts these values are configurable.
alert_notes	string	Usually not set. May exist in some special cases for passing additional information through Kafka DataTap.
alert_conf_id	string	id of the alert configuration that triggered this alert. May not exist for all alerts.
alert_details	string	Structured data. Stringified json. See feature details for specific alert type, since the exact structure of this field varies based on the type of alert.
alert_details_json	json	Same content of alert_details, but not stringified. Only present for compliance alerts, and only available through Kafka.
tenant_id	string	May contain vrf corresponding to root_scope_id. Or may contain 0 as the default value. Or may not be present at all.
alert_id	string	Internal generated temporary id. Best ignored.
alert_name	string	Name of the alert.

Compliance: lab-compliance-alert-details

- · Forensics: External Integration and Forensic event fields
- Sensor: Sensor Alert Details
- Enforcement: Enforcement Alert Details
- Connector: Alert Details
- Federation: federation-alert-details
- Platform: Alert Details

General Alert Format by Notifier

The following are the examples of how alerts display across various notifier types.



Note

Starting Secure Workload 3.9, notifier details include Alert Name.

Kafka (DataTaps)

Kafka (DataTap) messages are in JSON format. Example below; see above alert details for some additional examples.

```
"severity": "LOW",
   "tenant id": 0,
   "alert time": 1595207103337,
   "alert text": "Lookout Annotated Flows contains TA_zeus for
<scope_id:5efcfdf5497d4f474f1707c2>",
   "key id": "0a4a4208-f721-398c-b61c-c07af3be9413",
  "alert id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION_PARQUET',
 location name='lookout annotation', location grain='HOURLY',
root scope id='5efcfdf5497d4f474f1707c2'}/bd33f37af32a5ce71e888f95ccfe845305e61a12a7829ca5f2d72bf96237d403",
   "alert text with names": "Lookout Annotated Flows contains TA zeus for Scope Default",
   "root scope id": "5efcfdf5497d4f474f1707c2",
   "alert conf id": "5f10c7141a0c236b78148da1"
   "type": "LOOKOUT ANNOTATION",
   "event_time": 1595204760000,
   "alert details":
Names (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 1999 (1999) 199
```

Tigge/\}/\tage id\:\'54665936674E1062\\/\time rage\':[135046000,135048000]/\tacadiese\':\'172.26230.124\\/\tat port/\'137,\\texpadet.cont/\'10/\tac hatrave\':\/\\''

}

Email

Information about configuring Email alerts: Email Connector

Figure 13: Example of a Cisco Secure Workload Alert

	Tetration Alert - LOOKOUT_ANNOTATION Scope has any connection to or from TA_comp for Scope Default Alerts ×	promised_zeus	~	ē	Ø
•	jyovenka via alpha-portal-tan-alerts <alpha-portal-tan-alerts@tetrationanalytics.com> to alpha-portal-tan-alerts ↓</alpha-portal-tan-alerts@tetrationanalytics.com>	4:07 PM (28 minutes ago)	☆	4	:
	Alert Type: LOOKOUT_ANNOTATION Alert Key Id: cabfb7c8-c25b-33e4-9d55-005ccad8fba0 Alert Severity: LOW Alert Text: Scope has any connection to or from TA_compromised_zeus for Scope Default Alert Configuration Id : 5f1208431a0c23379206abee Root Scope Id: 5efcdfd5497d4f74f1707c2 Time: 2020-07-17 23:07:50.394 +0000 UTC Event Time: 2020-07-17 23:07:50.394 +0000 UTC Alert Details: ("dst_scope_id": ("5efcdfd5497d4f47f1707c2"), "dst_scope_names": ("Default"), "dst_hostname": "" "src_scope_id": ("5efcdfd5497d4f47f1707c2"), Alert Details: ("dst_scope_id": ("5efcdfd5497d4f47f1707c2"), "dst_scope_names": ("Default"), "dst_hostname": "" "src_scope_id": ("5efcdfd5497d4f47f1707c2"), "rerc_address": "172.26.231.179", "dst_port": 5355", "rev_packet_count": 0, "src_hostname": "" "	c2"],"lookout_tags".["TA_com ce"."lookout_annotation","rule Tiime_range".[159502662000(promise es": 0,15950	≥d_ 026680(001]

PagerDuty

Information about configuring PagerDuty alerts: PagerDuty Connector

Figure 14: Example of a Secure Workload Alert in PagerDuty

igerDuty Inciden	ts Alerts Configuration - Analytics -	(III) (?) (
ALERTS > ALERT DETAIL	\$	
Path > 0 betw	een Source Node Default and Destination Node Default:collectorDatamover-* (ALERT)	✓ Resolve
Belongs to Incident: [#28	54473] Path > 0 between Source Node Default and Destination Node Defaul (Tiggered)	Hove to Another Incident
Severity Cr Opened 11: Alert Key ae Current Status Tri	11cal 0 & AM (Movers agg) 0 & Sec (Resources Alert Lifecycle Understanding an Alert Log
Service Name Ma Service Description Co Integration AF	rige-July-2020 Influeiros plage duty for all alerts	
Source Ter	tration Analytics	
Details		
SUMMARY		
Path > 0 between Source No	de Default and Destination Node Default-collectorDatamover-*	
CUSTOM DETAILS		
Alert Details	BHDE BETAILS ("make_crimusiue_paths"12,"example_path_meighborhood_subjects_did":("Sefcid194074447441707c2":c_5f040befc544538885278807"),"internal_trigger": ("datasource":""http://mom_roites':("filedid":"http://mom_roites':"Net":"Net:"Net	
View Message		
Alert Log		
Time	Activity © SHOW ALL DETAILS	
at 11:06 AM	Triggened and automatically linked. B SHOW DETAILS	
	Per Page: 25 v (1-1)	Contact Suppo

Alerts sent to PagerDuty is a re-trigger of the same alert based on the key_id.

Severity is mapped to PagerDuty severity as follows:

Secure Workload Severity	PagerDuty Severity
IMMEDIATE_ACTION	critical
CRITICAL	critical
HIGH	error
MEDIUM	warning
LOW	info

Syslog

Information about configuring Syslog alerts, and adjusting severity mapping: Syslog Connector

Figure 15: Example of several Secure Workload alerts sent to syslog

Aug 2 18:45:21 tan-5f835bae1a8c231d5880d7f8-tac-demo-data-ingest Tetration Alert[2684]: [DEBUG] {"keyId":"See0d8b7-bc81-3427-9e84-6b9f8fedb98c", "eventTime":"159639 3720000", "tenatId":"0, "type":"COMPLIANCE", "alertDetalls": \"\"oronsumer_scope_ids\":I\\"befrdf567df47d7272\",\"oronsumer_scope_ids\":I\\"befrdf567df47d7272\",\"oronsumer_scope_ids\":I\\"befrdf567df47d7272\",\"oronsumer_scope_ids\":I\\"befrdf567df47d7272\",\"oronsumer_scope_ids\":I\\"befrdf567df47d7272\",\"oronsumer_scope_ids\":I\\"befrdf57df47d722\",\"oronsumer_scope_ids\":I\\"befrdf567df47d7272\",\"oronsumer_scope_ids\":I\\"befrdf57df47d722\",\"oronsumer_scope_ids\":I\\"befrdf567df47d722\",\"oronsumer_scope_ids\":I\\"befrdf57df47d722\",\"oronsumer_scope_ids\":I\\"befrdf57df47d722\",\"oronsumer_sdfers\\":U\DPI\",\"oronsumer_adfress\":\"II\"befrdf587df47d747d72\",\"oronsumer_adfress\":\"II\"befrdf587df47d722\",\"oronsumer_adfress\":\"II\"befrdf587df47d722\",\"oronsumer_adfress\":\"II\"befrdf587df47d747d72\",\"oronsumer_adfress\":\"II\"befrdf587df47d747d72\",\"oronsumer_adfress\":\"II\"2.31.63.13\\",\"provider_port\":S3J,\"oronsumer_port\":S3J,\"oronsumer_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"III\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"IIII\"3.6\",\"provider_adfress\":\"IIIII\"3.6\",\"provider_adfress\":\"IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26041]: [DEBUG] {"keyId":"1ef4a974-be89-31de-abe9-dc71cb0170ad","eventTime":"159639 3720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"L
OW", tenantId::0", "type":"COMPLIANCE", "alertDetails":"{\"consumer_sqope_ids\":[\"befcfdf5477df4f17df22\"],\"consumer_scope_names\":[\"Default\"],\"prvider_scope names\":[\Default\"],\"prvvider_port\":#43, "paplication_id\":"5f4b0b75f642d4636279\",\"consumer_stituent_flows\":[\"consumer_port\":#779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T779,\"protocol\":"T
onsumer address\":\"172.26.231.193\",\"provider address\":\"172.31.163.133\",\"provider port\":443}],\"escaped count\":1,\"provider scope ids\":[\"5efcfdf5497d4f474f
1707c2\"],\"policy type\":\"ENFORCED POLICY\",\"protocol\":\"TCP\",\"internal trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy violations\",\"t
vpe\":\"contains\",\"value\":\"escaped\";\"label\":\"Alert Trigger\"},\"time range\":[1596393720000,1596393779999],\"policy category\":[\"ESCAPED\"]}","rootScopeId"
:"5efcfdf5497d4f474f1707c2", "alertConfId":"5f15cca71a0c231ebd66ca3b", "alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}

Slack

Information about configuring Slack alerts: Slack Connector

Figure 16: Example of a Secure Workload alert sent to slack channel

10:37	Tetration Alert	Wednesday, July 29th >	
	be200f5c2dbc linux-amd64 AgentInactive	e	
	Severity	Туре	
	MEDIUM	SENSOR	
	Alert Time		
	2020-07-29 17:37:49:519 +0000 0TC	2020-07-29 17:37:01 +0000 01C	
	Root Scope Id		
	Details		
	{ "agent uuid": "6a968f8a8ddf2a4ec45349	055d247bcb5ce484046"	
	agent_uuld : 6a968t8a8ddt2a4ec4534955d247bcb5ce484046 , "details": { "AgentType": "NETSCALER",		
	"Bios": "53C9551F-F149-4BC7-FAE4-B	AF211FDF910",	
	"CurrentVersion": "3.5.2.69722.stshanta	.mrpm.build-netscaler",	
	"DesiredVersion": "3.5.2.70759.dashboa	rd.selfpmr.mrpm.build",	
	"HostName": "be200f5c2dbc",		
	"LastConfigFetchAt": "2020-07-02 01:28	3:59 +0000 UTC".	
	"Platform": "linux-amd64"		
	"scope_id": "5efcfdf5497d4f474f1707c2"	ı ,	
	"scope_name": "Default",		
	"vrf_id": 1		
	} Show less	↓ Latest messages	
	5110111035		

Kinesis

Information about configuring Kinesis alerts: Kinesis Connector

Kinesis alerts are similar to Kafka alerts, as these are both message queues.

Kinesis

I