



Configure Alerts

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



Note The alerts and compliance apps are removed from the Secure WorkloadApp Store starting release 3.0. 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 1](#)
- [Create Alerts, on page 2](#)
- [Alert Configuration Modal, on page 3](#)
- [Generate Test Alerts, on page 9](#)
- [Current Alerts, on page 11](#)
- [Alert Details, on page 13](#)

Alert Types and Publishers

Alerts in Secure Workload consist of many integrated components. Alerts are classified as:

Visibility:

- **Current Alerts:** Navigate to **Investigate > Alerts**. Preview of alerts sent to a Data Tap is available.

Alert Sources and Configuration:

- **Alerts - Configuration:** Navigate to **Manage > Alerts Configs**. Both alert configurations that are configured using the common modal, and alert publisher and notifier settings are displayed. It is determined by the app or component and commonly used as an interface (referred to as *Alert Configuration Modal*) that has features such as configuration of the Data Tap and summary alert options.

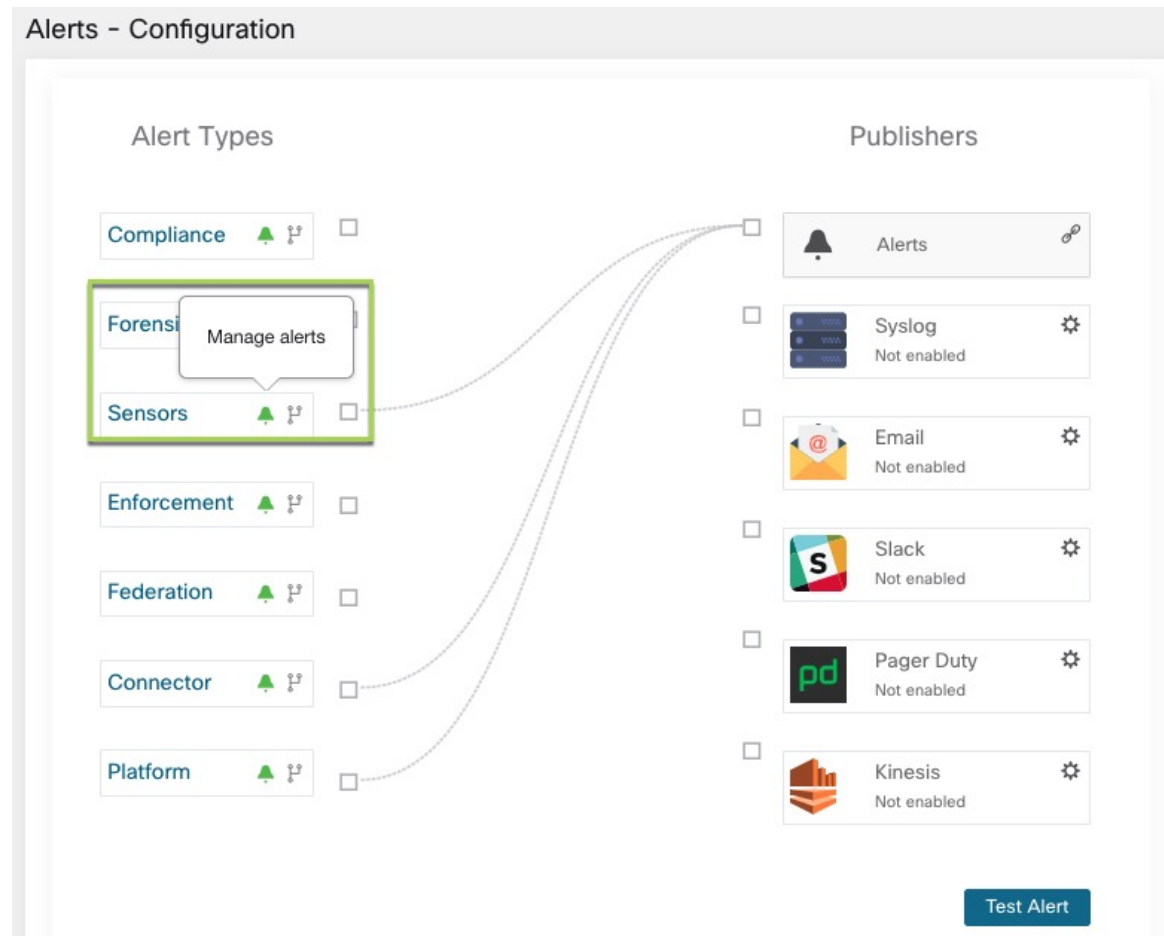
Send Alerts:

- **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, determining which alerts must be **sent**.

- **Alerts Publisher:** Limits how many alerts 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

Figure 1: Create Alert (Trigger Rule)



Several components use a common *Alert Configuration Modal* for configuring alerts. Currently, the following types are included:

- [Enforcement](#)
- [Sensors](#)



Note Only users with at least Enforced capability on the currently selected scope are able to create an alert trigger rule for the Compliance alert type.



Note Alert trigger rules are enforced on the currently selected root scope for the Enforcement and Sensors alert types.

The following types do not have a configuration modal.

- [Forensics](#)
- [Connectors](#)
- Federation
- Admiral

Alert Configuration Modal

The Alert configuration modal consists of the following sections:


1. The type of alert. Note that the alert type is displayed only when the configuration of the alert varies by *subject*.
2. The *subject* of the alert. The subject is dependent on the app, and may be pre-populated when the alert modal is contextual.
3. The condition on which an alert is triggered: Hover over the  icon to find a list of available conditions. Note that the list displays the conditions available specific to the type of alert currently being configured.
4. Alert severity: If there are many alerts generated, alerts with higher severity are displayed preferentially over alerts with lower severity.
5. Additional configuration options consisting of Summary Alert options. Click **Show Advanced Settings** to expand.
6. Close Modal: “Create” if adding a new alert and all configuration options specified. Or “Dismiss” if not adding a new alert.

Figure 2: Alert configuration modal advanced options

Configure Compliance Alerts
✕

Types

Enforcement Policy ⓘ
Live Analysis Policy ⓘ

For Enforced Application: _____ ⓘ

ⓘ condition > value...
✕

Severity

Low
Medium
High
Critical
Immediate Action

Hide Advanced Settings ^ 1

Individual Alerts

Enable
Enable With Flow Details
Disable

Summary Alerts

None
Hourly
Daily

2

Dismiss
Create

Summary Alerts

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

- *Individual Alerts* generally refers to alerts which 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 will 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.

App	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



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

Note on 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 will only result 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 will be generated at the specified frequency, so long as any 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 With 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 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, alert-related connectors must be configured. The connectors can only be configured after a Secure Workload Edge Appliance is deployed. See [Virtual Appliances for Connectors](#) for details on how to deploy Secure Workload Edge appliance.

After the Secure Workload Edge appliance is set up, you can configure each notifier with its specific required input. Note that once Secure Workload Edge appliance is set up, you will be able to see dashed lines connecting Alert Types to Alerts publisher. This is due the fact that notifier is build upon the Alerts publisher.

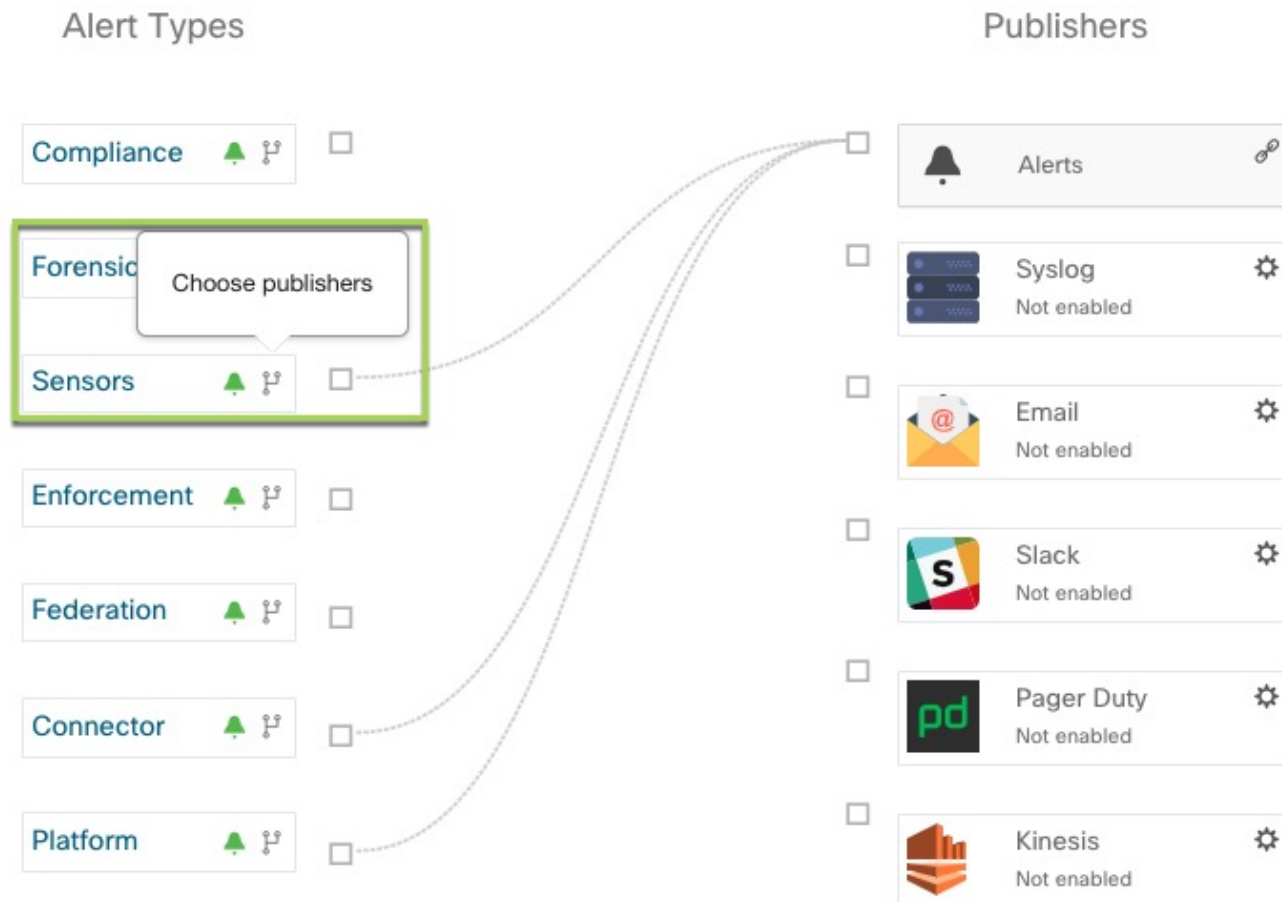
Refer to Connectors for Alert Notifications for details on how to configure each alert notifier.

App Frequency is approximately how often the app 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 includes Kafka (Data Tap) and notifiers.

Figure 3: Choose Alert Publishers



All 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 to which an alert must reach to be sent through the 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 datataps.

External syslog tunneling moving to TAN



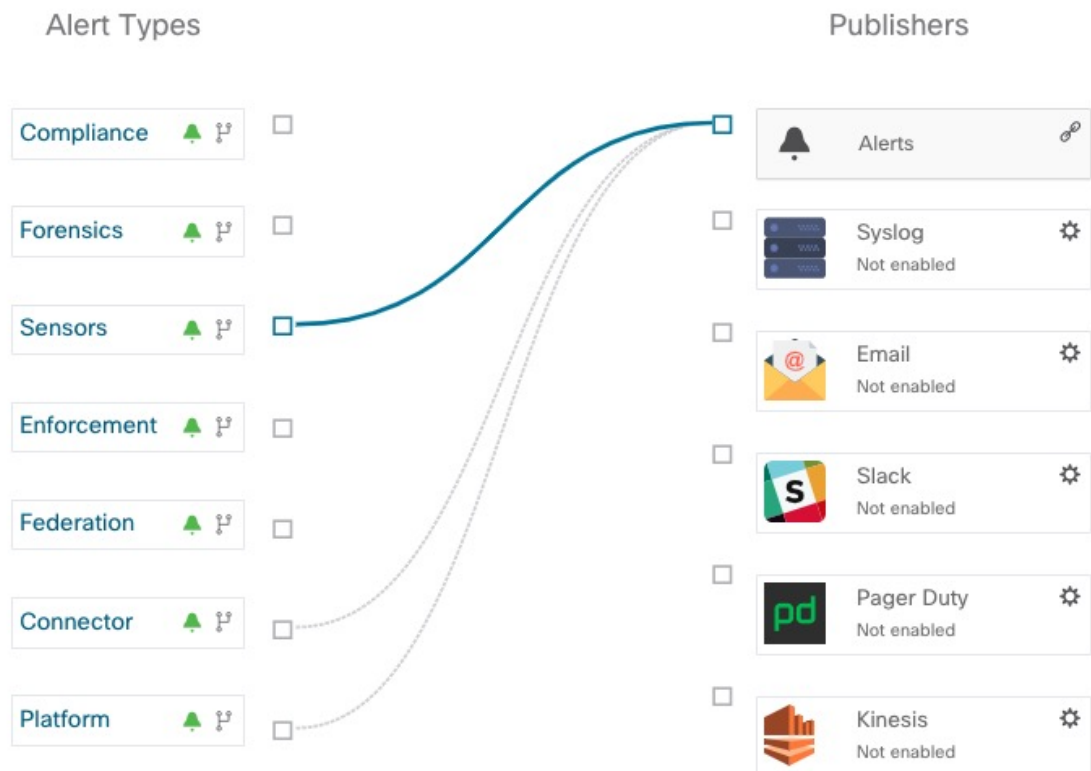
Note Starting 3.1.1.x release, the syslog tunneling feature will move to TAN. To configure syslog for getting platform level syslog events, user would need to configure TAN on Secure Workload Edge appliance on Default Rootscope. Once Secure Workload Edge appliance is configured on Default Rootscope, syslog server can be setup as shown below. To enable platform alerts, enable syslog notifications for Platform. This can be done by enabling Platform Syslog connection.

See [Syslog Connector](#) for details of how to configure syslog.

Connection Chart

The connection chart displays the connections between alert types and publishers. Once you choose a publisher for an alert type, a line will be established between that alert type and the publisher. Note that the line pointing to the Alerts publisher will always be dashed line since it represent an internal mechanism of how alerts notification build upon.

Figure 4: Connection chart



View Alerts Trigger Rules

A list of all Alerts Trigger Rules configured are displayed.

Figure 5: View Alerts Trigger Rules

The screenshot shows the 'Alerts - Configuration' window. On the left, there are 'Alert Types' (Compliance, Forensics, Sensors, Enforcement, Federation, Connector, Platform) and 'Publishers' (Alerts, Syslog, Email, Slack, Pager Duty, Kinesis). Lines connect 'Sensors' to 'Alerts', 'Federation' to 'Alerts', and 'Connector' to 'Alerts'. On the right, the 'Alerts Trigger Rules' table is displayed with a search bar and a 'Filter Alerts' button.

alert type	Configuration	actions
ENFORCEMENT	Scope: Default when Agent not reachable (seconds) > 300	
ENFORCEMENT	Scope: Default when Firewall = Off	
ENFORCEMENT	Scope: Default when Policy = Deviated	
SENSORS	Scope: Default when Agent Upgrade Status = Failed	
SENSORS	Scope: Default when Agent Flow Export Status = Stopped	
SENSORS	Scope: Default when Agent Check-In Service = Inactive	
SENSORS	Scope: Default when Deep visibility memory usage (MB) > 512 and Enforcement memory usage (MB) > 512 and Forensic memory usage (MB) > 256	
SENSORS	Scope: Default when Deep visibility CPU Quota (%) > 3 and Enforcement CPU Quota (%) > 3 and Forensic CPU Quota (%) > 3	
SENSORS	Scope: Default when Amount of flow observations > 500000	
SENSORS	Scope: Default when Agent Uninstalled = On	
SENSORS	Scope: Default when Alert before removal (minutes) = 5	

Alerts Trigger Rules window can be used to filter alerts trigger rules by alert type, alert frequency and alert trigger condition.



Note Alert trigger condition is an exact match condition.

Alerts Trigger Rules Details

Click on a row in the Alerts Trigger Rules table to expand and view the configuration details.

Figure 6: Expanded alert configuration

ENFORCEMENT *Scope: Default* when **Policy = Deviated**

Details

Severity	Medium
Individual Alerts	Enable
Summary Alert Freq.	None

SENSORS **1** *Scope: Default* when **Agent Upgrade Status = Failed** **2**

Details

Severity	Medium	3
Individual Alerts	Enable	
Summary Alert Freq.	None	4

1. Subject: *what an alert is about.*
2. Trigger: *when an alert is generated.*
3. Severity: Decides which alerts are displayed if there are many alerts generated at the same time.
4. Individual Alerts and Summary Alert Frequency: Decides whether individual and/or summary alerts are generated.

Generate Test Alerts

You can configure the sample alert to send out alerts based on the alert type and linked publisher in the alert configuration. The primary use is to verify the connectivity with the publisher.



Note

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

To generate a test alert follow the below steps.

Procedure

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

Figure 7: Test Alert Configuration

The screenshot shows a 'Test Alert' configuration window. On the left is a sidebar with four tabs: 'Keys', 'Scope', 'Details', and 'Configuration'. The 'Keys' tab is selected. The main area contains the following fields:

- Alert Key:** A text input field containing 'Aa1234Zz'.
- Event Time:** A date-time picker showing '29/03/2023, 08:59:50.628 PM'.
- Alert Time (optional):** A date-time picker showing '29/03/2023, 08:59:50.628 PM'.
- Alert Severity:** A dropdown menu currently set to 'LOW'.
- Alert Type:** A dropdown menu with 'Choose one' at the top and a list of options: 'COMPLIANCE', 'FORENSICS', 'SENSORS', 'ENFORCEMENT', 'FEDERATION', and 'CONNECTOR'. 'COMPLIANCE' is currently selected.

At the bottom right of the dialog are two buttons: 'Cancel' and 'Test'.

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 auto generated based on the current scope.

Note If the Tenanat ID is 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 a string value or data in JSON format.

Options for JSON content are:

- a. Containing fields expected by that type of alert.
- b. 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 alert, choose *ENABLE* or *DISABLE* from the drop down.

Alert frequency is auto-selected with frequency as *INDIVIDUAL*.

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

Summary alert is auto selected 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

You can filter the alerts by type, status (active or snoozed), and severity (immediate_action, critical, high, medium, or low). By default, the listed alerts are filtered to display the active alerts that are sorted in descending order.



Warning Only alerts that contain the severity value of IMMEDIATE_ACTION, CRITICAL, LOW, MEDIUM, or HIGH are shown on the **Alerts** page. All alerts irrespective to the severity values are sent to the configured kafka broker.

Figure 8: Current Alerts Listing

Event Time	Status	Alert Text	Severity	Type	Actions
Aug 9, 10:22 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:20 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:18 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:16 PM	ACTIVE	eg-tet36-win10 MSWindows10Pro Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:12 PM	ACTIVE	eg-tet36-win19-2 MSServer2019Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:12 PM	ACTIVE	eg-tet36-win19 MSServer2019Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:12 PM	ACTIVE	eg-tet36-win12r2 MSServer2012R2Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:10 PM	ACTIVE	eg-tet36-win12r2 MSServer2012R2Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O
Aug 9, 10:10 PM	ACTIVE	eg-tet36-win19 MSServer2019Datacenter Flow Export Stopped	MEDIUM	SENSOR	? O

View Additional Alert Details

Click the alert to view more details.

Figure 9: Alert Details

**Note**

- Only 60 alerts per minute per root scope are displayed on the UI. A higher volume of alerts result in the summary alert on the UI.
 - Preference is provided to Critical alerts, and then to those with High severity, followed by Medium severity, and finally Low severity.
 - There is a maximum number of alerts that are displayed on the UI at any point in time; older alerts will be dropped as new alerts come in.
- See [Limits](#).

Snooze Alerts

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

**Note**

Currently, user app created alerts cannot be snoozed or ignored (muted).

Snooze or Mute an Alert

To snooze an alert:

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

To mute an alert:

Instead of snoozing, you can use the mute option to stop receiving alerts of the selected type permanently. The muted alert types can be removed from the muted list to continue to receive the alerts.

1. Under **Actions**, click the **Mute** icon for the required alert type.

2. You no longer receive alerts of the selected type. To confirm, click **Yes**.

To continue to receive these alerts, remove the alert type from the muted list. To find the list of muted alert types, choose **MUTED** from the **Status** drop-down menu (In previous releases of Secure Workload, enter **Status=MUTED** in the filter field).

Unsnnooze or Unmute an Alert

1. Use the **Status** drop-down to filter **Snoozed** and **Muted** alerts.
 - Choose **Snoozed** (In previous releases of Secure Workload, enter **Status=SNOOZED** in the filter field).
 - Choose **Muted** (In previous releases of Secure Workload, enter **Status=MUTED** in the filter field).
2. Under **Actions**, click either the unsnooze or unmute icon, as required.
3. To confirm the action, click **Yes**.

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, but each type of alert will vary in its alert details.

The common structure is as follows. This 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

Field	Format	About
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).
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. String-i-fied 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 string-i-fied. 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 default value. Or may not be present at all.

Field	Format	About
alert_id	string	Internal generated temporary id. Best ignored.

The fields within *alert_details* vary based on the type of alert. See each feature section for explanation and list of fields:

- 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

Variation across notifier types. The following contains examples of how alerts display across various notifier types.

Kafka (DataTaps)

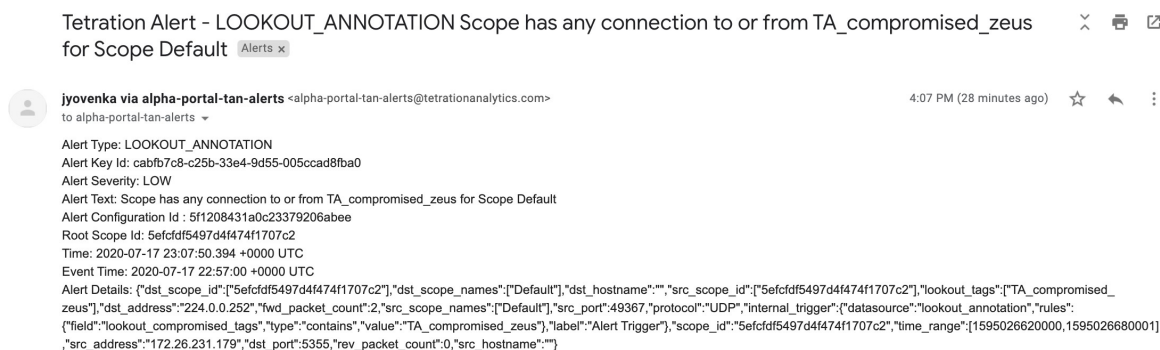
Kafka (DataTap) messages are in JSON format. Example below; see above *alert_details* for some additional examples.

```
{
  "severity": "LOW",
  "tenant_id": 0,
  "alert_time": 1595207103337,
  "alert_text": "Lookout Annotated Flows contains TA_zeus for
<scope_id:5efcfd5497d4f474f1707c2>",
  "key_id": "0a4a4208-f721-398c-b61c-c07af3be9413",
  "alert_id": "/Alerts/5efcfd5497d4f474f1707c2/DataSource(location_type='TETRATION_PARQUET',
location_name='lookout_annotation', location_grain='HOURLY',
root_scope_id='5efcfd5497d4f474f1707c2')/bd33f37af32a5ce71e888f95ccfe845305e61a12a7829ca5f2d72bf96237d403",
  "alert_text_with_names": "Lookout Annotated Flows contains TA_zeus for Scope Default",
  "root_scope_id": "5efcfd5497d4f474f1707c2",
  "alert_conf_id": "5f10c7141a0c236b78148da1",
  "type": "LOOKOUT_ANNOTATION",
  "event_time": 1595204760000,
  "alert_details":
  "Trigger": "Trigger", "scope_id": "5efcfd5497d4f474f1707c2", "time_range": [1595204760000, 1595204800000], "sc_addresses": "172.26.20.124", "bit_rot": "13", "event_alert_conf": "0", "scope_name": "Trigger"
}
```

Email

Information about configuring Email alerts: [Email Connector](#)

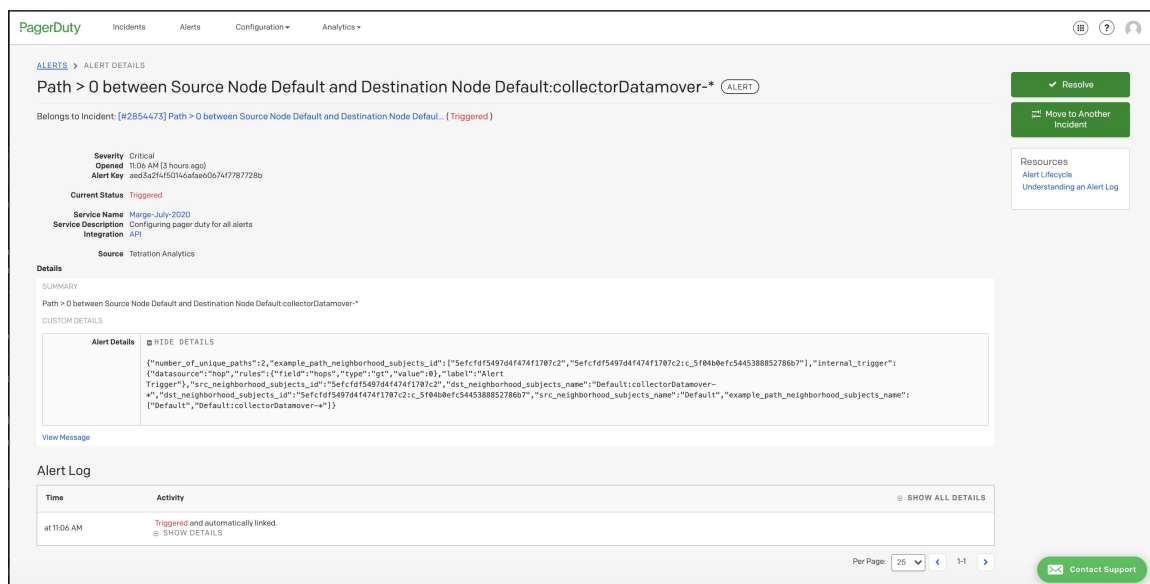
Figure 10: Example of a Cisco Secure Workload alert when configured to send to email



PagerDuty

Information about configuring PagerDuty alerts: [PagerDuty Connector](#)

Figure 11: Example of a Secure Workload alert in PagerDuty



Alerts sent to PagerDuty will be considered 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

Secure Workload Severity	PagerDuty Severity
MEDIUM	warning
LOW	info

Syslog

Information about configuring Syslog alerts, and adjusting severity mapping: [Syslog Connector](#)

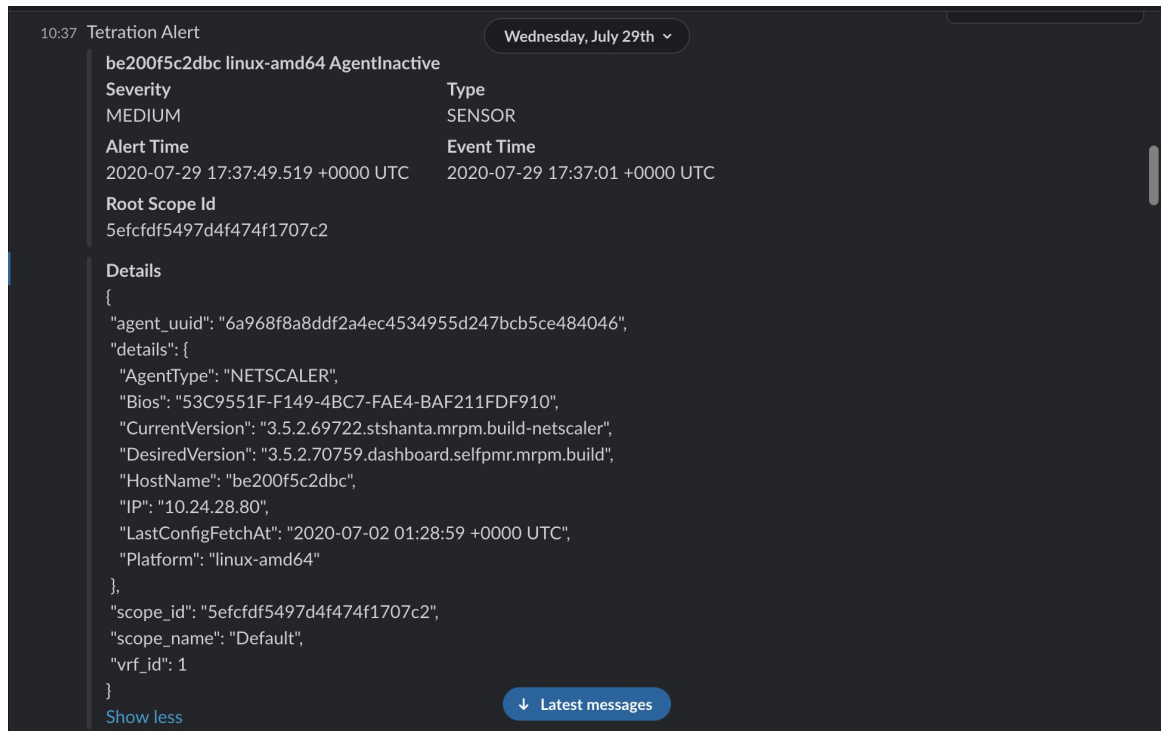
Figure 12: Example of several Secure Workload alerts sent to syslog

```
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"9ee0d8b7-bc81-3427-9e84-6b9f8fedb98c","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":{"consumer_scope_ids":{"5efcfd5497d4f474f1707c2"},"consumer_scope_names":{"Default"},"provider_scope_names":{"Default"},"provider_port":53,"application_id":{"5f04b0b9755f024d4e36a279"},"constituent_flows":[{"consumer_port":{"37367},"protocol":{"UDP"},"consumer_address":{"172.31.163.133"},"provider_address":{"171.70.168.183"},"provider_port":53},{"consumer_port":{"39652},"protocol":{"UDP"},"consumer_address":{"172.31.163.137"},"provider_address":{"171.70.168.183"},"provider_port":53},{"consumer_port":{"6881},"protocol":{"UDP"},"consumer_address":{"172.31.163.136"},"provider_address":{"171.70.168.183"},"provider_port":53},{"consumer_port":{"57418},"protocol":{"UDP"},"consumer_address":{"172.31.163.138"},"provider_address":{"173.36.131.10"},"provider_port":53},{"consumer_port":{"12599},"protocol":{"UDP"},"consumer_address":{"172.31.163.141"},"provider_address":{"173.36.131.10"},"provider_port":53},{"consumer_port":{"7385},"protocol":{"UDP"},"consumer_address":{"172.31.163.140"},"provider_address":{"173.36.131.10"},"provider_port":{"53}},"escaped_count":6,"provider_scope_ids":{"5efcfd5497d4f474f1707c2"},"policy_type":{"ENFORCED_POLICY"},"protocol":{"UDP"},"internal_trigger":{"datasource":{"field":{"policy_violations"},"type":{"contains"},"value":{"escaped"},"label":{"Alert Trigger"},"time_range":{"1596393720000,1596393779999},"policy_category":{"ESCAPED"}}},"rootScopeId":{"5efcfd5497d4f474f1707c2"},"alertConfId":{"5f15cca71a0c231ebd66ca3b"},"alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"8f0fcfb5-f8c1-3130-a669-3721b7d50159","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":{"consumer_scope_ids":{"5efcfd5497d4f474f1707c2"},"consumer_scope_names":{"Default"},"provider_scope_names":{"Default"},"provider_port":{"5660},"application_id":{"5f04b0b9755f024d4e36a279"},"constituent_flows":[{"consumer_port":{"17131},"protocol":{"TCP"},"consumer_address":{"172.26.231.193"},"provider_address":{"172.31.163.140"},"provider_port":{"5660}},"escaped_count":1,"provider_scope_ids":{"5efcfd5497d4f474f1707c2"},"policy_type":{"ENFORCED_POLICY"},"protocol":{"TCP"},"internal_trigger":{"datasource":{"compliance"},"rules":{"field":{"policy_violations"},"type":{"contains"},"value":{"escaped"},"label":{"Alert Trigger"},"time_range":{"1596393720000,1596393779999},"policy_category":{"ESCAPED"}}},"rootScopeId":{"5efcfd5497d4f474f1707c2"},"alertConfId":{"5f15cca71a0c231ebd66ca3b"},"alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"1ef4a974-be89-31de-abe9-dc71cb0170ad","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":{"consumer_scope_ids":{"5efcfd5497d4f474f1707c2"},"consumer_scope_names":{"Default"},"provider_scope_names":{"Default"},"provider_port":{"443},"application_id":{"5f04b0b9755f024d4e36a279"},"constituent_flows":[{"consumer_port":{"17792},"protocol":{"TCP"},"consumer_address":{"172.26.231.193"},"provider_address":{"172.31.163.133"},"provider_port":{"443}},"escaped_count":1,"provider_scope_ids":{"5efcfd5497d4f474f1707c2"},"policy_type":{"ENFORCED_POLICY"},"protocol":{"TCP"},"internal_trigger":{"datasource":{"compliance"},"rules":{"field":{"policy_violations"},"type":{"contains"},"value":{"escaped"},"label":{"Alert Trigger"},"time_range":{"1596393720000,1596393779999},"policy_category":{"ESCAPED}}},"rootScopeId":{"5efcfd5497d4f474f1707c2"},"alertConfId":{"5f15cca71a0c231ebd66ca3b"},"alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
```

Slack

Information about configuring Slack alerts: [Slack Connector](#)

Figure 13: Example of a Secure Workload alert sent to slack channel



Kinesis

Information about configuring Kinesis alerts: [Kinesis Connector](#)

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