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.

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 1
- Create Alerts, on page 2
- Alert Configuration Modal, on page 4
- Generate Test Alerts, on page 10
- Current Alerts, on page 12
- Alert Details, on page 14

Alert Types and Publishers

Alerts in Secure Workload consist of the following components:

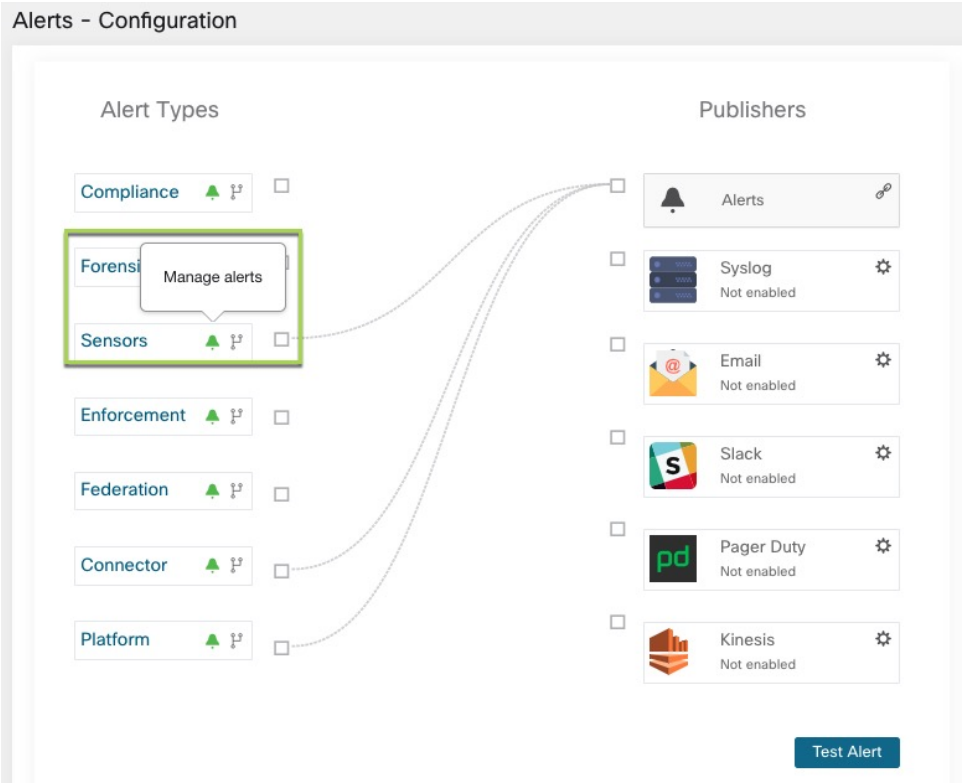
- **Alert Visibility**
  - **Current Alerts**: From the navigation pane, choose **Investigate** > **Alerts**. Preview of alerts is sent to a Data Tap.
- **Alert Sources and Configuration:**
  - **Alerts - Configuration**: Choose **Manage** > **Alerts Configs**. Both alert configurations that are configured using the common modal and alert publisher, and notifier settings are displayed.
- **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

To create alerts or trigger rules, from the navigation pane, choose **Alerts** > **Configuration**:

Figure 1: Create Alert or Trigger Rules



- **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
- Federation
- Admiral
- 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 the option to detect malicious addresses, see Visibility of 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

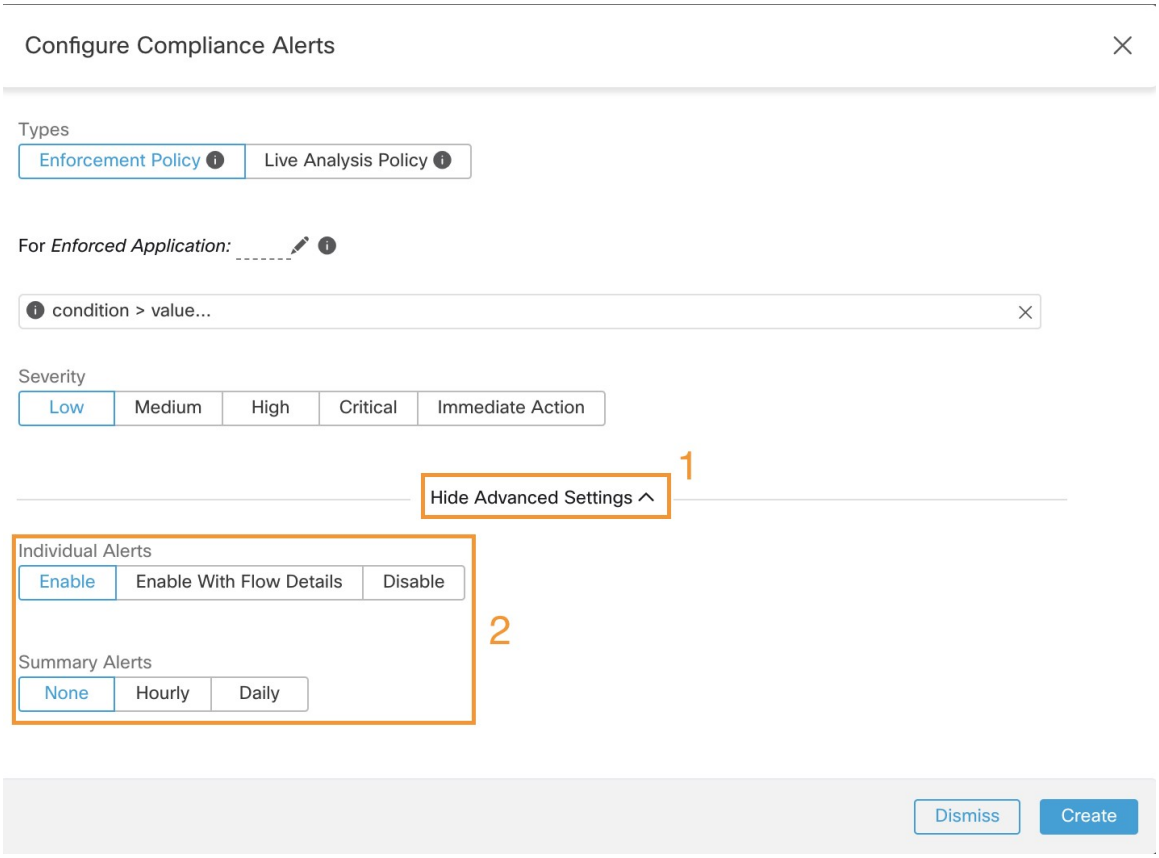
The Alert configuration modal consists of the following sections:

- The types of alert are shown when the configuration of the alert varies by *subject*

Note The types of alert for Neighborhood alerts are not available for Secure Workload 3.7 and earlier.

- The *subject* of the alert. The subject depends on the app, and may be prepopulated when the alert modal is contextual.
- Triggering an alert: *"when will we generate an alert"*. Hover over the icon to find a list of available conditions. The list displays the conditions available specific to the type of alert for configuration.
- Alert severity: If there are many alerts that are generated, alerts with higher severity are displayed preferentially over alerts with lower severity.
- Configuration options for Summary Alert options. Click **Show Advanced Settings** to expand.
- Close Modal: Use **Create** if you are adding a new alert with all configuration options specified or **Dismiss** if you are not adding any new alerts.

Figure 2: Alert Configuration Modal Advanced Options



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.

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 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 specfic 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 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.

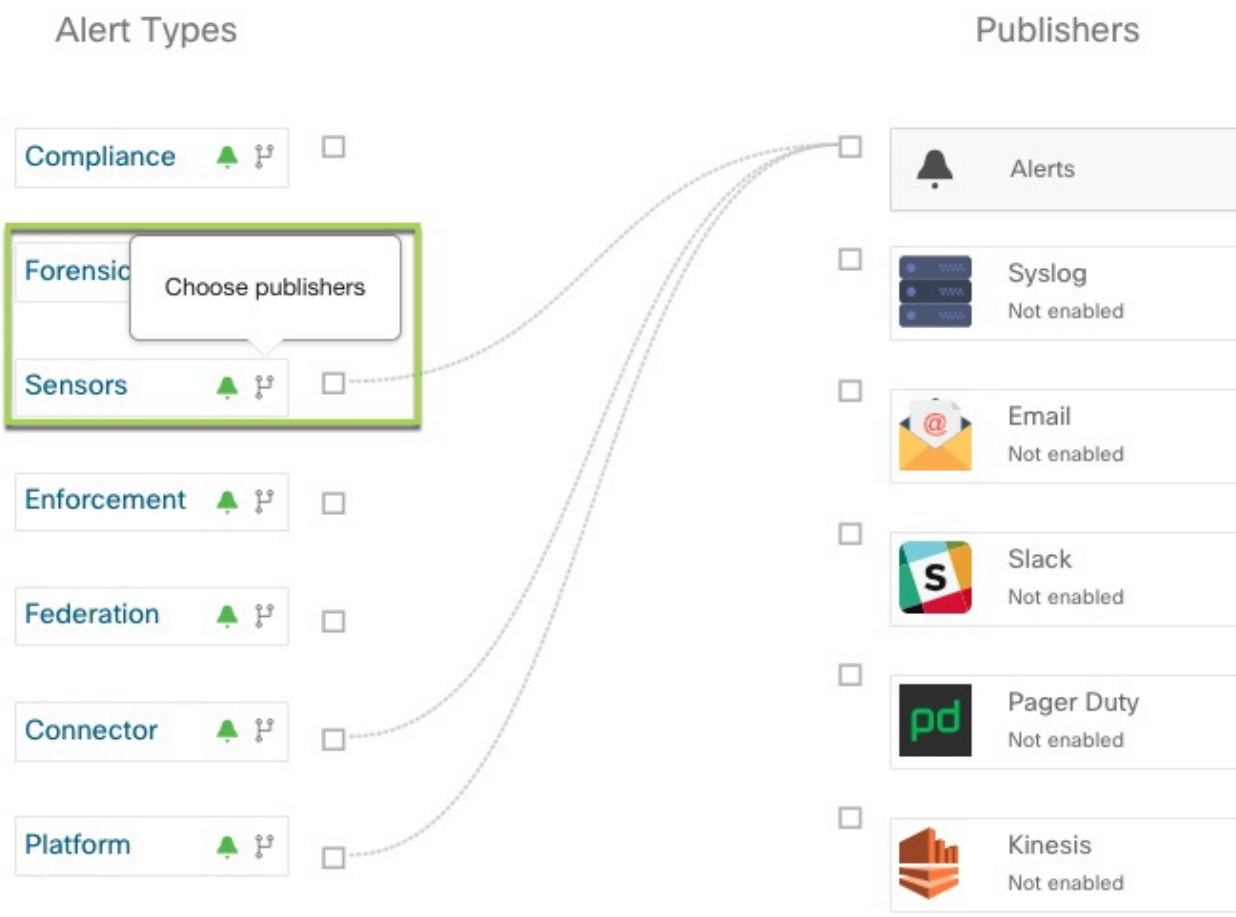
After the Secure Workload Edge appliance is set up, you can configure each notifier with its specific required input. After the Secure Workload Edge appliance is set up, you will be able to see dashed lines connecting Alert Types to Alerts publisher. This is because the notifier is built on the Alerts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

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**.

Figure 3: Choose Alert Publishers



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**.

Note Choosing external data taps can impact on the maximum number of alerts that can be processed. The maximum number of alerts that can be processed can be reduced to up to 14000 alerts per minute batch.

External Syslog Tunneling Moves to TAN

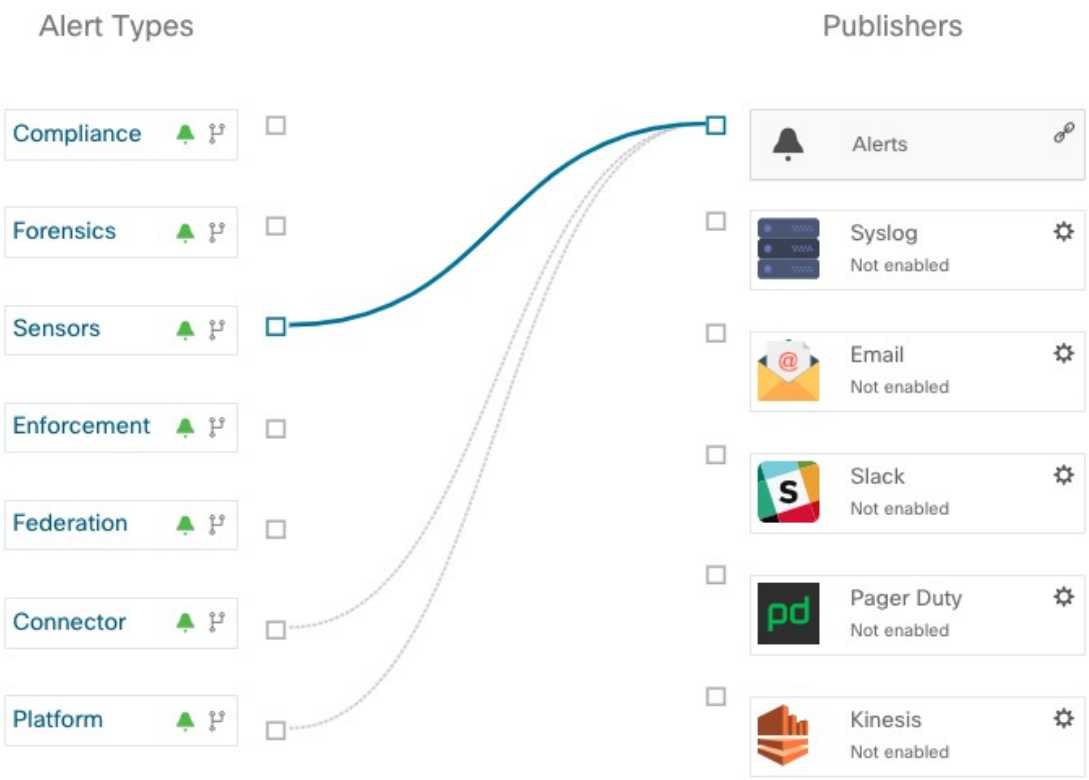
Note Starting the 3.1.1.x release, the syslog tunneling feature moves to TAN. To configure syslog for getting platform level syslog events, you must configure TAN on the Secure Workload Edge appliance on default rootscope. When the Secure Workload Edge appliance is configured on the default rootscope, 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 4: Connection chart

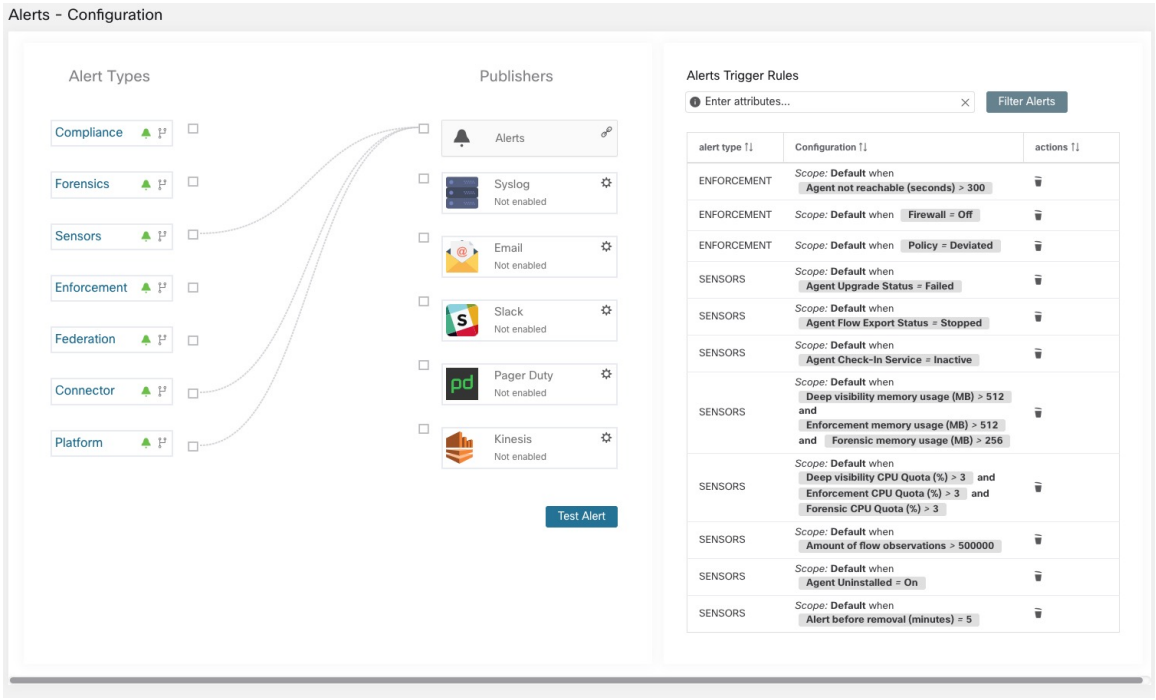


Note User App generated alerts are not shown in the Alert Configuration page. User Apps are able to send messages and alerts to any configured Data Tap.

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:

Figure 5: View Alerts Trigger Rules



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

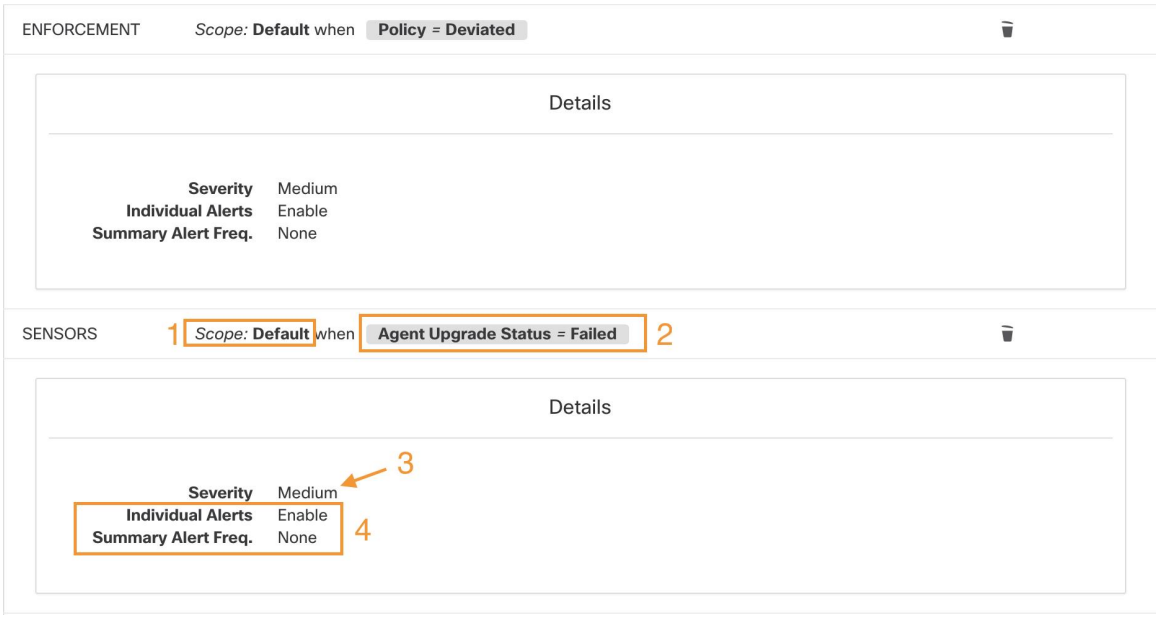
Note Alert trigger condition is an exact match condition.

Alerts Trigger Rules Details

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

You can also view other details such as **Severity**, **Individual Alerts**, and **Summary Alert Frequency**.

Figure 6: Expanded alert configuration



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.

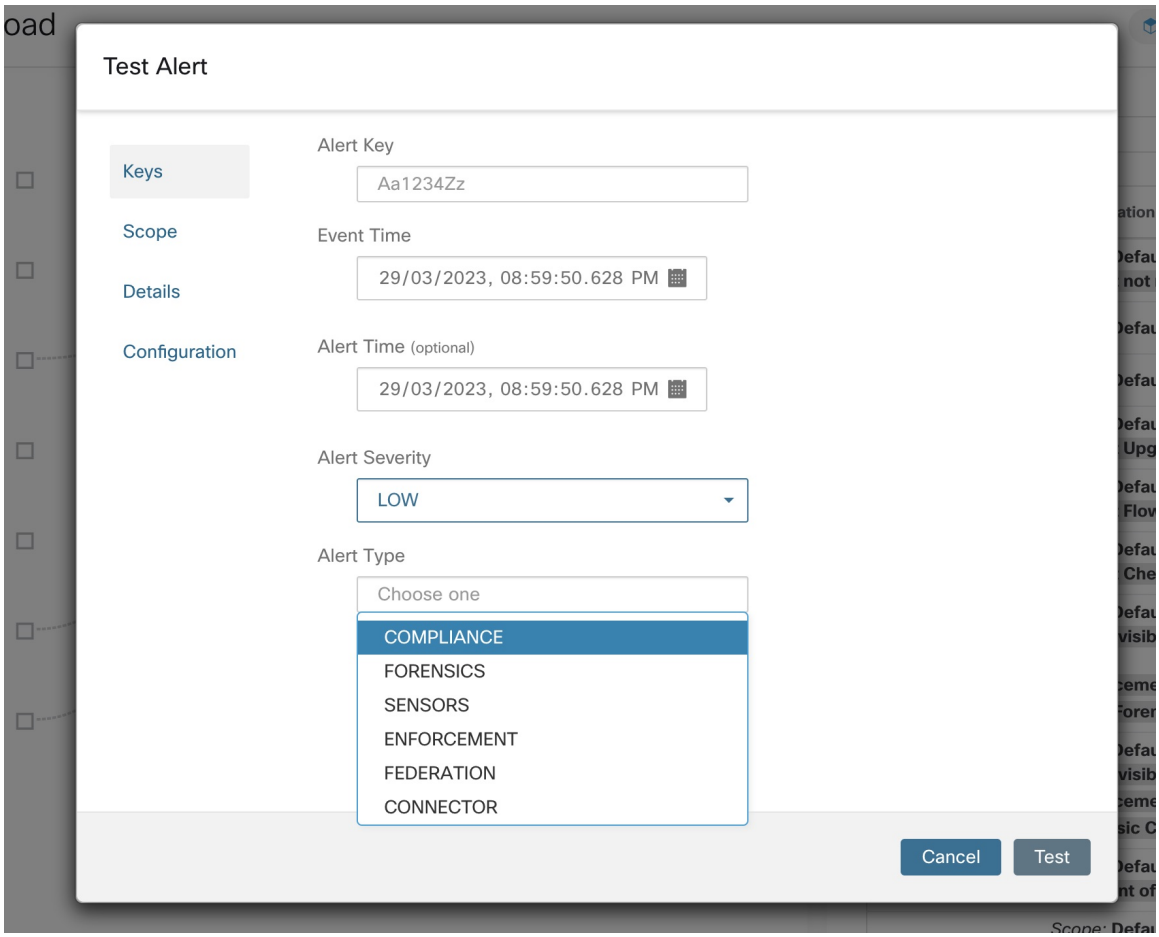
To generate a test alert, follow the steps below:

Procedure

Step 1 From the navigation pane, choose **Manage** > **Workloads** > **Alerts Config**.

Step 2 To configure a test alert, click **Test Alert**.

Figure 7: 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.

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 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.

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

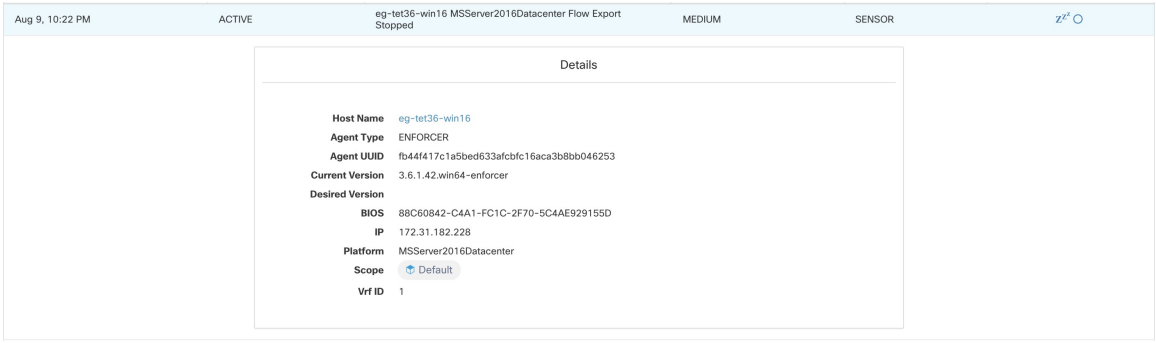
1. Click **Switch to Advanced**.
2. Enter the attributes to filter. Hover over the **info** icon to view the properties to filter.

   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 8: Alert Details



- 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.

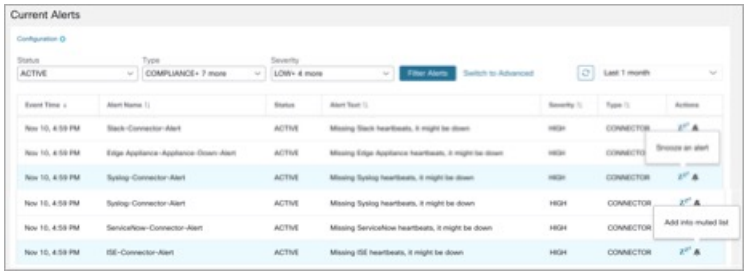
Note Currently, you cannot snooze or mute the user app-created alerts.

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 9: Snooze an Alert



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.

Note 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

Additional alert types for on-prem clusters

- Fabric: fabric-alert-details
- Federation: federation-alert-details
- Platform: 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.

Kafka (DataTaps)

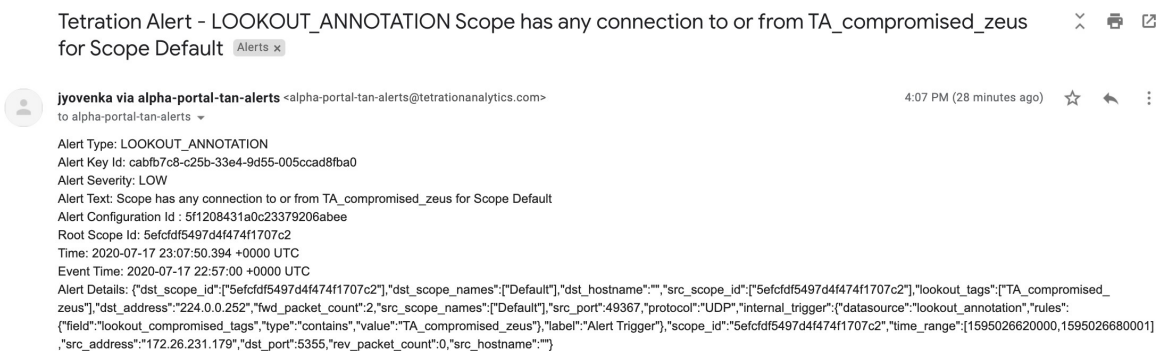
Kafka (DataTap) messages are in JSON format. Example below; see above alert_details for some additional examples.


```
  {
  "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":
'{"app_id":"00000002","app_name":"Default","dst_address":"172.26.230.124","dst_port":137,"ev_packet_count":0,"src_hostname":""}'

  }
```


Email

Information about configuring Email alerts: Email Connector

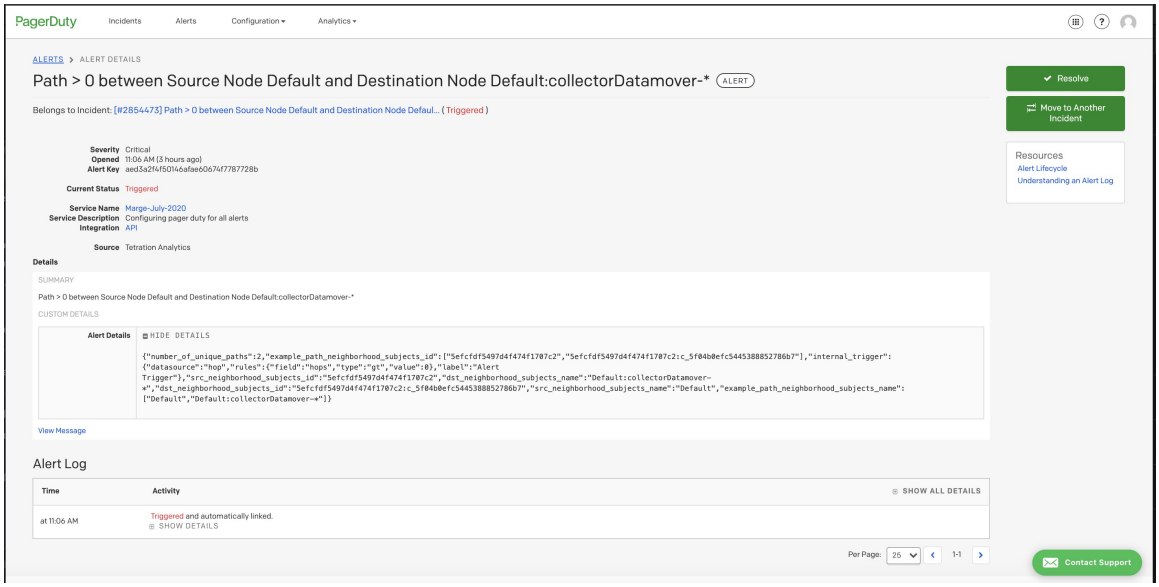
Figure 10: Example of a Cisco Secure Workload Alert



PagerDuty

Information about configuring PagerDuty alerts: PagerDuty Connector

Figure 11: Example of a Secure Workload Alert in PagerDuty



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

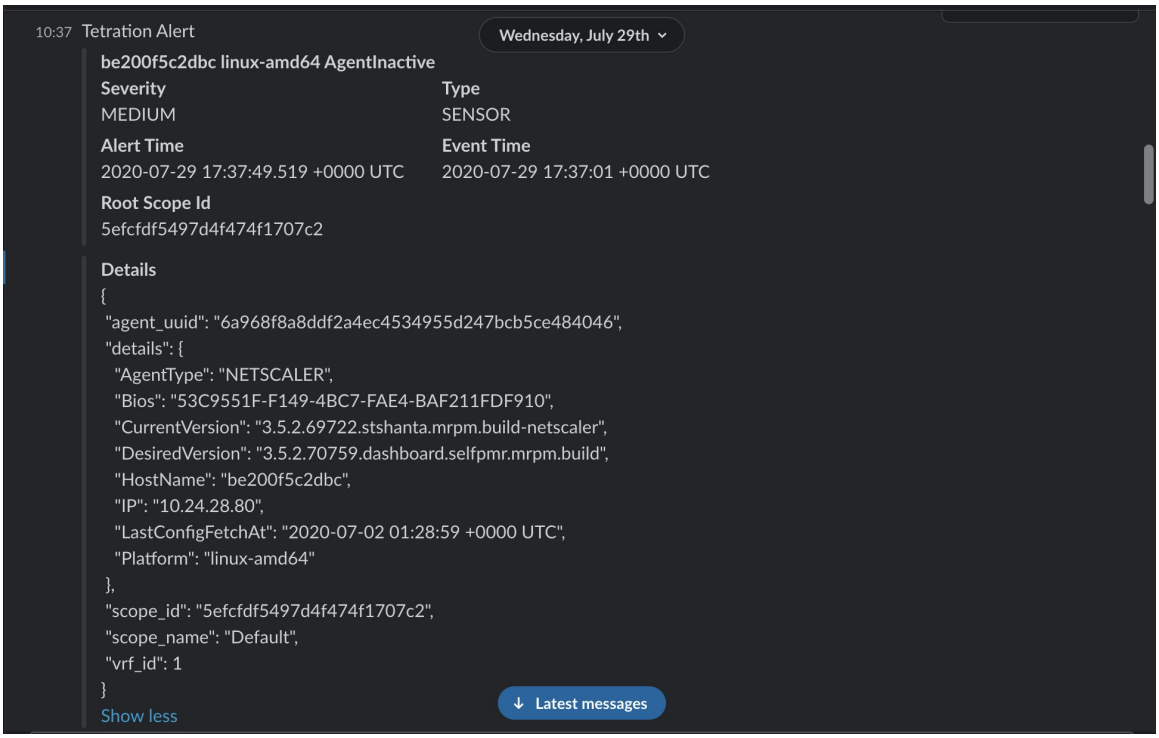
Figure 12: Example of several Secure Workload alerts sent to syslog


```
Aug  2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"3ee0d8b7-bc81-3427-9e84-6b9f8fedb98c","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_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope
_names\":[\"Default\"],\"provider_port\":53,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":37367,\"protocol\":\"UDP\",\"co
nsumer_address\":\"172.31.163.139\",\"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\":63811,\"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_addr
ess\":\"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_po
rt\":53}],\"escaped_count\":6,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"UDP\",\"internal_trigger\":{\"
datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596
393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","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":"8f0cfcb5-f8c1-3130-a069-3721b7d50159","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_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"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\":[\"5efcfdf5497d4f47
4f1707c2\"],\"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\"]}","rootScopeI
d":"5efcfdf5497d4f474f1707c2","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":"159639
3720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"L
OW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope
_names\":[\"Default\"],\"provider_port\":443,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":17792,\"protocol\":\"TCP\",\"c
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
ype\":\"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 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.