



## 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. 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](#)
- [Current Alerts, on page 11](#)
- [Alert Details, on page 13](#)

## Alert Types and Publishers

Alerts in Secure Workload consist of the following components:

### 1. Alert Visibility:

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

### 2. 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.

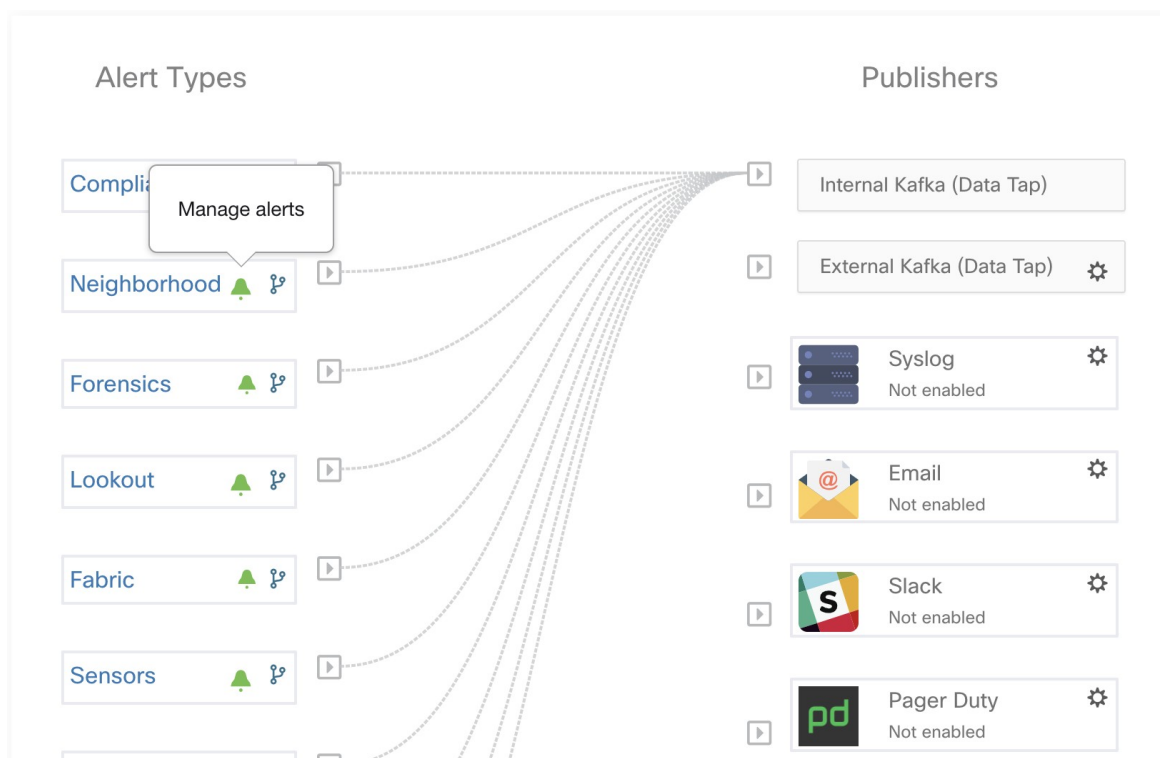
### 3. Send Alerts:

- **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

Figure 1: Create Alert (Trigger Rule)



On the **Alerts - Configuration** page, configure the following Alert Types:

- [Neighborhood](#)
- [Enforcement](#)
- [Sensors](#)
- **Enforcement Alerts**—You can configure three types of alerts:
  - **Agent Reachability**  
This alert type detects when the agent is not reachable and triggers an alert if the agent has not communicated with the Secure Workload cluster for more than the configured number of seconds.
  - **Workload Firewall**  
This alert type is triggered if the enforcement is configured on a workload but the workload firewall is detected to be off. This condition prevents the Secure Workload agent from enforcing the traffic policies.
  - **Workload Policy**

This alert type is triggered if the workload firewall rules are different from the Secure Workload policies applicable to this workload (workload's Concrete policies).

• **Sensors Alerts**—You can configure three types of alerts:

• Agent Upgrade

This alert type is triggered when an agent fails to upgrade to the required version.

• Agent Flow Export

This alert type detects when the agent flow export has stopped. An alert is triggered if the connectivity between the agent and the cluster is blocked.

• Agent Check In

This alert type detects when agent check\_in times out. An alert is triggered if the cluster does not receive a check-in request from an agent after more than 90 minutes.

• **Compliance Alerts**— You can configure two types of 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 at least 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](#)

## Alert Configuration Modal

The Alert configuration modal consists of the following sections:

1. The type of alert. *Note:* This is only shown when the configuration of the alert varies by *subject* (Currently only shown for Neighborhood alerts).
2. The *subject* of the alert: ie. “*what we are going to alert over*” This is dependent on the app, and may be pre-populated when the alert modal is contextual.
3. The condition on which an alert will be triggered: ie. “*when will we generate an alert*”. A list of available conditions can be found by hovering over the  *Note:* this list will show those conditions available specifically for the type of alert currently being configured.

4. Alert severity selection. If there are many alerts generated, alerts with higher severity will be visible in the UI 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**

## 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 |
| Neighborhood | Hourly         | —                     | Yes                   | Summary of Hourly     |
| 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.

## 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 Neighborhood 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, alert-related connectors must be configured. The connectors can only be configured after a Secure Workload Edge Appliance is deployed. For more information on how to deploy the Secure Workload Edge appliance, see [Virtual Appliances for Connectors](#) for details on

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 Internal Kafka(Data Tap). This is due the fact that notifier is build upon the Internal Kafka(Data Tap).

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.

Fabric alerts are produced hourly when the app runs (note that the App Frequency is *hourly*), so in practice Fabric alerts will be produced and sent in batches after each hour of data is processed, even though the individual alert option is a *minute* of data. This means that if the data would produce two alerts per minute, all 120 alerts are actually generated and sent at the end of the hour, and are likely to result in a summary alert showing in the UI.

## 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

The screenshot displays the 'Choose Alert Publishers' configuration page. It is divided into two main sections: 'Alert Types' on the left and 'Publishers' on the right.

**Alert Types:** This section lists nine alert categories, each with a bell icon, a user icon, and a play button:

- Compliance
- Neighborhood
- Forensics
- Lookout
- Fabric
- Sensors
- Enforcement
- Federation
- Connector

A tooltip with the text 'Choose publishers' is positioned over the 'Neighborhood' alert type.

**Publishers:** This section lists seven notification channels, each with a play button and a gear icon:

- Internal Kafka (Data Tap)
- External Kafka (Data Tap)
- Syslog (Not enabled)
- Email (Not enabled)
- Slack (Not enabled)
- Pager Duty (Not enabled)
- Kinesis (Not enabled)

Figure 4: All available publishers will be displayed in this modal

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** Choosing external datataps can impact on the maximum number of alerts that can be processed; maximum number of alerts that can be processed could be reduced to up to 14000 alerts per minute batch.



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

## 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.

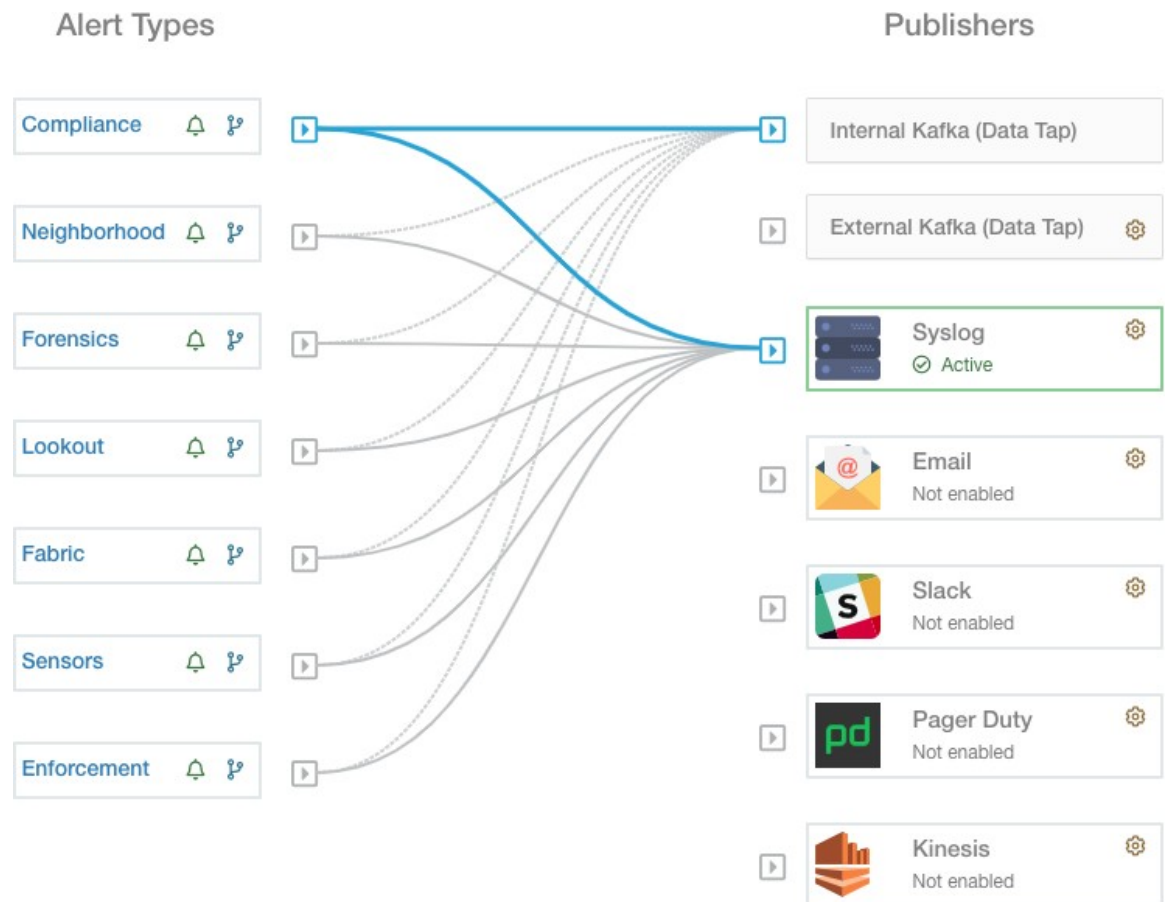
For more information, see [Syslog Connector](#) for details of how to configure syslog.



## Connection Chart

The connection chart displays the connections between **Alert Types** and **Publishers**. Once you choose a publisher for an alert type, a blue line is established between the alert type and publisher. Note that the line pointing to the Internal Kafka (Data Tap) is always a dashed line as it represents an internal mechanism of how alerts notification build upon.

**Figure 5: Connection chart**



As shown in this figure, once Syslog is chosen as a publisher for Neighborhood alerts, a line is established between them. Note that, hovering on the circled area in the figure will highlight the connections that are only associated with Neighborhood alerts.

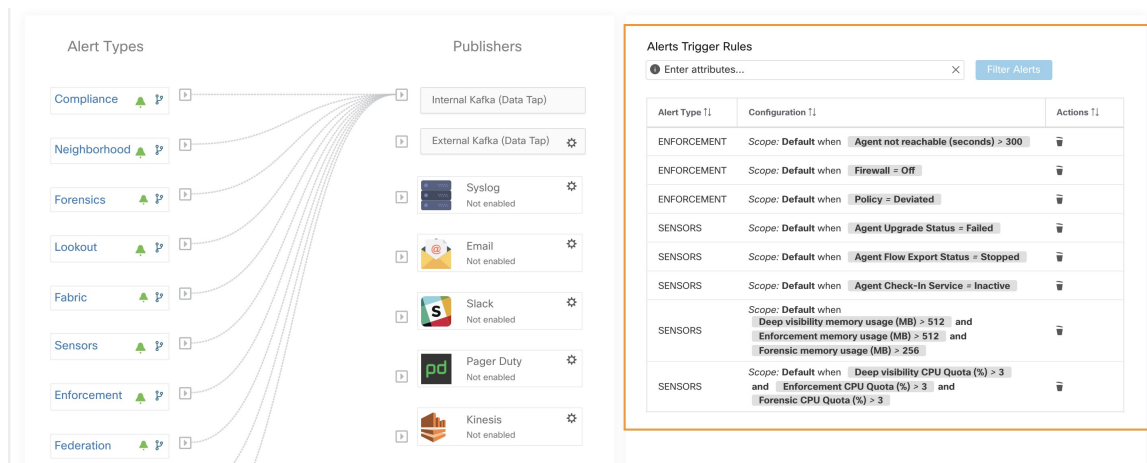


**Note** User App generated alerts are not shown in the Alert Configuration page. User Apps are able to send messages and alerts to any configured Data Tap.

## View Alerts Trigger Rules

You can view a list of all configured Alerts Trigger Rules on the **Alerts - Configuration** page.

Figure 6: Viewing Alerts Trigger Rules



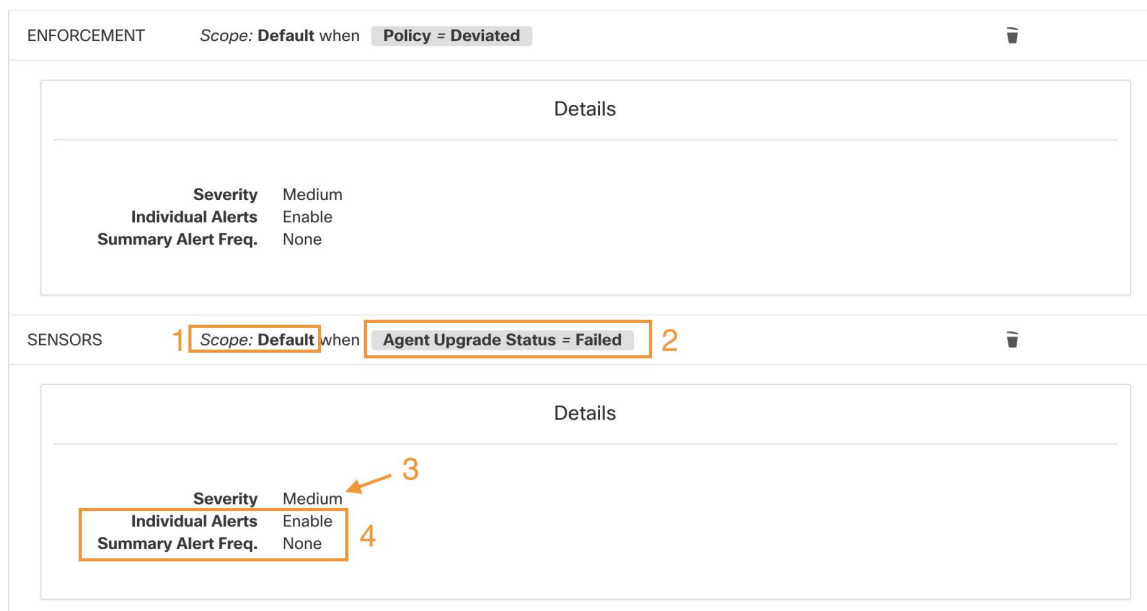
**Note** Alert trigger condition is an exact match condition.

## Alerts Trigger Rules Details

Click on 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 7: Expanded alert configuration



## Current Alerts

When you navigate to the **Investigate > Alerts** page, a list of all active alerts is displayed. 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 on an alert.

**Figure 8: Alert Details**

| Details         |   |
|-----------------|---|
| Host Name       | eg-tet36-win16                          |
| Agent Type      | ENFORCER                                |
| Agent UUID      | fb44f417c1a5bed633efcfc16aca3b8bb046253 |
| Current Version | 3.6.1.42.win64-enforcer                 |
| Desired Version |   |
| BIOS            | 88C60842-C4A1-FC1C-2F70-5C4AE929155D    |
| IP              | 172.31.182.228                          |
| Platform        | MSServer2016Datacenter                  |
| Scope           | Default                                 |
| Vrf ID          | 1                                       |

- Only 60 alerts per minute per root scope are displayed. A higher volume of alerts result in the summary alerts.
- 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**

| Event Time      | Alert Name                          | Status | Alert Text  | Severity | Type      | Actions               |
|-----------------|-------------------------------------|--------|---|----------|-----------|-----------------------|
| Nov 10, 4:59 PM | Stack-Connector-Alert               | ACTIVE | Missing Stack heartbeats, it might be down          | HIGH     | CONNECTOR | [Snooze an alert]     |
| Nov 10, 4:59 PM | Edge Appliance-Appliance-Down-Alert | ACTIVE | Missing Edge Appliance heartbeats, it might be down | HIGH     | CONNECTOR | [Snooze an alert]     |
| Nov 10, 4:59 PM | System-Connector-Alert              | ACTIVE | Missing System heartbeats, it might be down         | HIGH     | CONNECTOR | [Snooze an alert]     |
| Nov 10, 4:59 PM | System-Connector-Alert              | ACTIVE | Missing System heartbeats, it might be down         | HIGH     | CONNECTOR | [Snooze an alert]     |
| Nov 10, 4:59 PM | Serviceflow-Connector-Alert         | ACTIVE | Missing Serviceflow heartbeats, it might be down    | HIGH     | CONNECTOR | [Add into muted list] |
| Nov 10, 4:59 PM | ISE-Connector-Alert                 | ACTIVE | Missing ISE heartbeats, it might be down            | HIGH     | CONNECTOR | [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, FABRIC, 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).                  |
| 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. |

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

| 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.  |

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](#)
- Neighborhood: [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](#)

## 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",

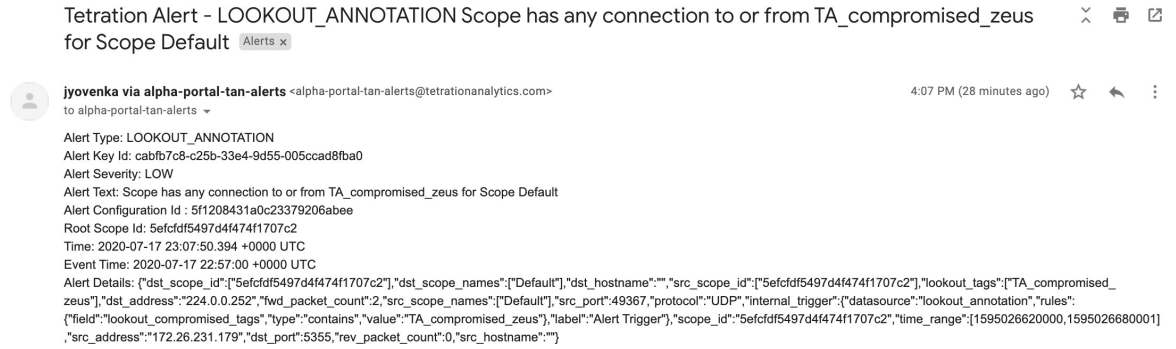
  "alert_text_with_names": "Lookout Annotated Flows contains TA_zeus for Scope Default",
  "root_scope_id": "5efcfd5497d4f474f1707c2",
  "alert_conf_id": "5f10c7141a0c236b78148da1",
  "type": "LOOKOUT_ANNOTATION",
  "event_time": 1595204760000,
  "alert_details":
  {
    "scope_id": "5efcfd5497d4f474f1707c2",
    "time_range": [1592046000, 1592048000],
    "sc_address": "172.26.20.124",
    "bt_port": "137",
    "keypad_conf": "0",
    "sc_hostname": ""
  }
}
```



## Email

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

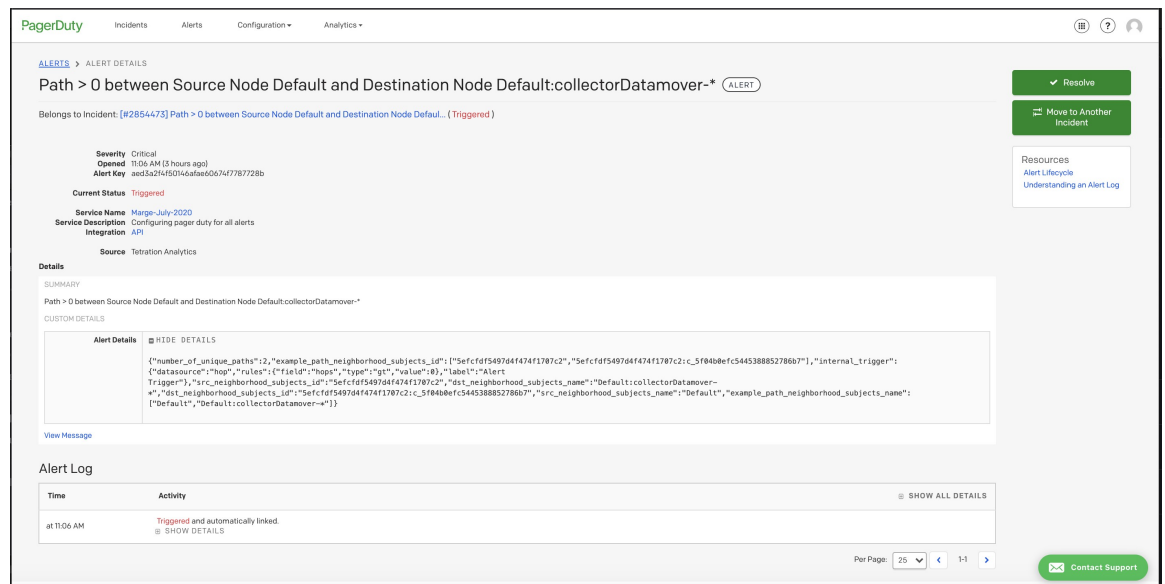
**Figure 10: Example of a Cisco Secure Workload alert when configured to send to email**



## 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-5f035b8e1a8c231d5880d7f8-tac-demo-data-ingest Tetratation Alert[26841]: [DEBUG] {"keyId":"3ee0d8b7-bc81-3427-9e84-6b9f8fedb98c","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"","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":"172.31.163.137","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":26911,"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":"compliance","rules":{"field":"policy_violations","type":"contains","value":"escaped"},"label":"Alert Trigger"},"time_range":{"1596393720000,1596393779999},"policy_category":{"ESCAPED"},"rootScopeId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035b8e1a8c231d5880d7f8-tac-demo-data-ingest Tetratation Alert[26841]: [DEBUG] {"keyId":"8f0cfeb5-f8c1-3130-a069-3721b7d50159","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"","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":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035b8e1a8c231d5880d7f8-tac-demo-data-ingest Tetratation Alert[26841]: [DEBUG] {"keyId":"1ef4a974-be89-31de-abe9-dc71cb170ad","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"","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**

```

10:37 Tetration Alert
be200f5c2dbc linux-amd64 AgentInactive
Severity                                Type
MEDIUM                                 SENSOR
Alert Time                             Event Time
2020-07-29 17:37:49.519 +0000 UTC      2020-07-29 17:37:01 +0000 UTC
Root Scope Id
5efcfd5497d4f474f1707c2

Details
{
  "agent_uuid": "6a968f8a8ddf2a4ec4534955d247bcb5ce484046",
  "details": {
    "AgentType": "NETSCALER",
    "Bios": "53C9551F-F149-4BC7-FAE4-BAF211FDF910",
    "CurrentVersion": "3.5.2.69722.stshanta.mrpm.build-netscaler",
    "DesiredVersion": "3.5.2.70759.dashboard.selfpmr.mrpm.build",
    "HostName": "be200f5c2dbc",
    "IP": "10.24.28.80",
    "LastConfigFetchAt": "2020-07-02 01:28:59 +0000 UTC",
    "Platform": "linux-amd64"
  },
  "scope_id": "5efcfd5497d4f474f1707c2",
  "scope_name": "Default",
  "vrf_id": 1
}
Show less
Latest messages

```

## Kinesis

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

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

