Events

Skylar One version 12.5.22

Table of Contents

Chapter 1

Overview of Events

Overview

This chapter describes how to use Skylar One to manage events that appear on the **Events** page.

This chapter covers the following topics:

What is an Event?

One of the quickest ways to monitor the health of your network is to look at events. You can view events on the **Events** page in Skylar One.

Events are alerts that are triggered when a specific condition is met. For example, an event can signal if a server has gone down, if a device is exceeding CPU or disk-space thresholds, or if communication with a device has failed. Alternatively, an event can simply display the status of a managed element.

An ***alert*** defines a formula that Skylar One evaluates each time data is collected. If the formula evaluates to true during data collection, Skylar One generates an alert. Not every alert triggers an event. An alert

must have an ***event policy*** in Skylar One that defines the conditions for the event, and when an alert meets the conditions in the event policy, Skylar One generates an event.

Skylar One generates log messages from incoming trap and syslog data, and also when Skylar One executes user-defined policies. Skylar One then uses these log messages to generate events. Skylar One examines each log message and compares it to each event definition. If a log message matches an event's definition, Skylar One generates an event instance and displays the event on the **Events** page.

Each event includes a description of the problem, where the problem occurred (device, network hardware, software, policy violation), a pre-defined severity, the time of first occurrence, the time of most recent occurrence, and the age of the event. You can find more information on the **Event Investigator** page for an event.

Skylar One includes pre-defined events for the most commonly encountered conditions in the most common environments. You can also create custom events for your specific environment or edit the pre-defined events to better fit your specific environment.

How Are Events Triggered?

Skylar One examines log messages to generate instances of events. When Skylar One monitors a system, Skylar One generates log messages when the collected data meets user-defined thresholds. Additionally, a monitored system can send log messages to Skylar One asynchronously. Skylar One examines each log message and compares it to each existing event definition. If a log message matches an event's definition, Skylar One generates an event instance and displays the event on the **Events** page.

Skylar One includes logic that correlates and groups related logs and messages into a single event. Skylar One includes pre-defined events for many syslog, internal, trap, and dynamic messages.

Event Sources

Skylar One generates events by collecting logs and messages from the following:

- ***Syslog***. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices such as managers of managers (MoM). A syslog is an unsolicited message from a device to Skylar One. Syslog is a standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools. For more information on syslogs, see the section on *syslog messages*.
- ***Internal***. Message is generated by a ScienceLogic process. The message is about the Skylar One system itself, instead of the devices that the Skylar One system monitors.
- ***Trap***. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like managers of managers (MoMs). An SNMP trap is an unsolicited message from a device to Skylar One. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device. For more information on traps, see the section on *SNMP Traps*.

- ***Dynamic***. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell Skylar One how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. Skylar One examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, Skylar One generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees Fahrenheit. If the chassis temperature exceeds 100 degrees at some point in the future, Skylar One inserts a message in the associated device's log files. Skylar One then matches that message with an existing event, and then triggers the event. For more information, see the section on *Dynamic Application Development*.
- ***Email***. Message is generated by an email message sent to Skylar One. For more information on generating events with email messages, see the section on *events from email*.
- ***API***. Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the section on *snippet actions*. For more information on snippet Dynamic Applications, see the section on *developing snippet Dynamic Applications*. For more information on the ScienceLogic API, see the section on *generating events with the ScienceLogic API*.
- ***ScienceLogic Agent***. Message is generated by log file messages collected by a Skylar One agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by an agent, see the section on *Monitoring Device Logs Using an Agent*.
- ***Rules Engine***. Message is generated through internal policy evaluations, complex correlation rules, or rule-based logic. Users cannot create or edit event policies with a ***Source*** of *Rules Engine*.
- ***Skylar Automated RCA***. Message is generated by Skylar Automated RCA alerts. Skylar One receives an alert from Skylar Automated RCA and creates an event from it. For more information, see the *Skylar AI documentation*.
- ***Skylar AI***. Message is generated by Skylar AI alerts. Skylar One receives an alert from Skylar AI and creates an event from it. For more information, see the *Skylar AI documentation*.

Viewing Events

The **Events** page displays a list of currently active events, from critical to healthy. From this page, you can acknowledge, clear, and view more information about an event. You can also view events by organization to focus on only the events that are relevant to you.

For more information about using the **Events** page, see the section on *Viewing the List of Events*.

In addition, you can:

- *View a list of events for a single device*
- *View a list of events for a single organization*
- *Acknowledge or clear the events*
- *Align an external ticket with the events*

Event Correlation

In Skylar One, event correlation means the ability to build parent-child relationships between devices and between events. When events are correlated, only the parent event is displayed on the **Events** page. The child events are rolled up under the parent event and are not displayed on the **Events** page. For the parent event, the value in the ***Count*** column is incremented to indicate the number of correlated child events. In addition to creating parent-child relationships between devices and between events, you can define event categories that allow Skylar One to more efficiently align events.

Skylar One performs some event correlation automatically. You can also manually configure devices and events so that Skylar One treats specified events as parent events and specified events as child events. For more information, see the section on *event correlation*.

Defining Events

The **Event Policies** page (Events > Event Policies) displays a list of all event policies in Skylar One. This page also allows you to define new event definitions and edit existing event definitions.

Skylar One includes pre-defined events for the most commonly encountered conditions on the most common platforms. Skylar One allows you to customize these events and also to define new events. You do this in the **Event Policies** page.

If your organization requires Skylar One to monitor a condition for which Skylar One does not already include an event policy, you can define a custom event policy to meet your needs.

For more information, see the section on *defining and editing event policies*.

Event States

Although not displayed on the **Events** page, events have four distinct states:

- ***Active***. Skylar One has created an event record. The event might appear on the **Events** page, or it might be masked or nested as a topology event, and therefore not appear on the **Events** page.
- ***Masked***. The event record is active and appears on the **Events** page as a masked event. On the **Events** page, masked events can be caused by event masks or topology events. Masked events are nested under the event with the highest severity or under the parent event. You can click the masked events icon ( ) to view details about the masked events.
- ***Cleared***. The event has been removed from the **Events** page. When you clear an event, you remove only a single instance of the event from the current display on the **Events** page. If the event occurs again on the same entity, it reappears on the **Events** page.
- ***Prepending***. An alert triggered the event, but additional criteria must be met before Skylar One creates an event record. Prepending events are grayed out in device logs.

Chapter 2

Viewing Events

Overview

You can view a list of all events in Skylar One or view a list of events for a single device. This section describes how to perform both tasks.

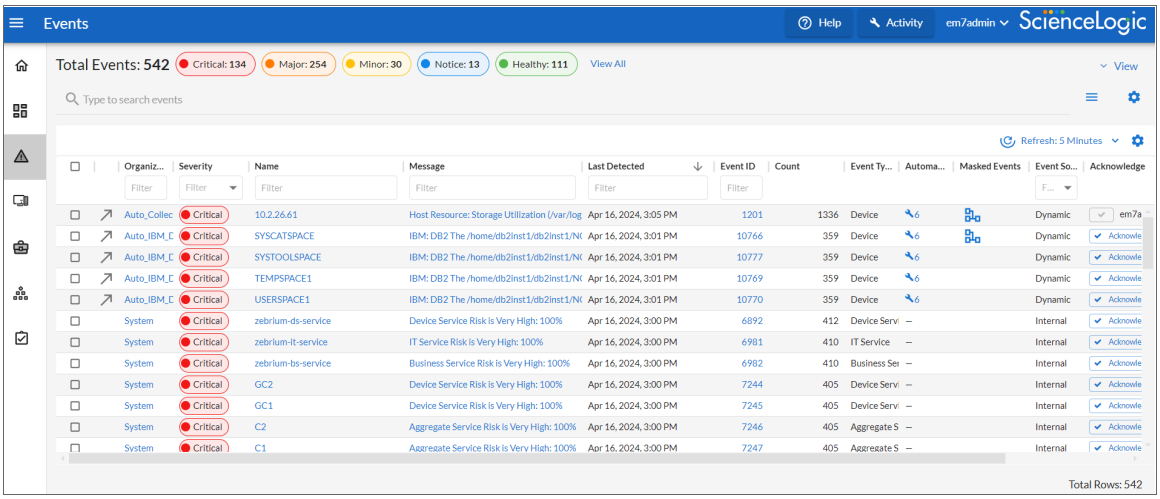
This chapter covers the following topics:

Viewing the List of Events

The **Events** page displays a list of currently active events, from critical to healthy. From this page, you can acknowledge, clear, and view more information about an event. You can also view events by organization to focus on only the events that are relevant to you.

By default, the events listed on the **Events** page are sorted by severity, highest to lowest, and then secondarily sorted by the events' last occurrences, most recent to least recent. This ensures that the most severe and most recent events appear at the top of the page. If you prefer, you can change the sorting preferences, and Skylar One recalls those changes the next time you return to the **Events** page.

To navigate to the **Events** inventory page, click the Events icon (⚠).



TIP: You can use the ***Search*** field to look for specific items in the list using either a basic or advanced search. For more information, see the topics *Using Basic Search* and *Performing an Advanced Search*.

TIP: You can sort the list by a column's values by clicking on its column heading. You can also filter the items on the page by typing or selecting filter options in one or more of the filters found above the columns. For more information, see the topic on *Filtering Inventory Pages*.

TIP: You can rearrange the columns in the list by clicking and dragging the column to a new location. You can adjust a column's width by clicking and dragging the right edge of the column. For more information about editing and adding columns, see the topic on *Editing the Settings for an Inventory Page*.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the topic on *Adjusting the Row Density*.

For each event, the **Events** page displays the following information:

- ***Organization***. The organization with which the event is associated. Click the organization hyperlink to view more information about the organization. You can optionally filter the list of events so that only events for a specific organization appear on the **Events** page; for more information, see the section *Filtering Events by Organization and Service*.
- ***Severity***. The severity of the event. For more information about severity values, see the section *Understanding Event Severity*. You can optionally filter the list of events so that only events of a specific severity level appear on the **Events** page. For more information, see the section *Filtering Events by Severity*.
- ***Name***. The name of the entity associated with the event. Click the name hyperlink to view more information about the entity.
- ***Message***. The message generated for the event. Click the message hyperlink to go to *the Event Investigator*, where you can view more information about the event, including a description, its probable cause, and possible resolutions, among other details. You can also view the **Event Investigator** page by clicking the actions icon ( ) for the event and selecting *View Event*.
- ***Last Detected***. The date and time at which the event last occurred on the entity.
- ***Age***. The number of days, hours, and minutes since the first occurrence of the event. This is also the time since the event occurred without the event having been cleared.
- ***Ticket ID***. The ticket ID of the ticket that has been created for the event, if applicable.
- ***Count***. The number of times the event has occurred.
- ***Event Note***. Click the note icon ( ) to view any existing user-defined notes about the event or to create or edit a note about the event. When you do so, the **Edit Event Note** modal page appears, where you can create or edit a note and save your changes. For more information, see *Viewing and Editing Event Notes*.

  NOTE: You can also view, create, or edit event notes by clicking the actions icon ( ) for the event and selecting *Edit Event Note*.

- ***Masked Events***. If the event has occurred multiple times on the same device that uses the ***event mask*** setting, click the masked events icon ( ) to go to the **Masked Events Overview** modal, where you can view details about the masked events. For more information, see the section *Filtering for Masked Events*.

- ***Automated Actions***. The number of times the event has triggered the execution of an automation policy. If the event has triggered one or more automated actions, click the number hyperlink to go to the **Event Actions Log**, where you can view a log of all automated actions that have occurred for the event. For more information, see the section *Viewing Automated Actions*.

> **NOTE:** You can also view the **Event Actions Log** modal page by clicking the actions icon ( ) for the event and selecting *View Automation Actions*.

- ***Event ID***. The unique ID for the event, generated by Skylar One. Click the ID hyperlink to go to *the Event Investigator*.
- ***Event Source***. The system or application that generated this event. For more information, see the section on *Event Sources*.
- ***Event Type***. The type of entity associated with the event. Possible values are:
  - Aggregate Services
  - Assets
  - Business Services
  - Device Services
  - Devices
  - Interfaces
  - IP networks
  - IT Services
  - Organizations
  - User Accounts
  - Vendors
  - Virtual Interfaces
- ***External Ticket***. The numeric ID associated with a ticket from an external ticketing system outside of Skylar One. Click the ticket reference value to view the external ticket in a new window. You can display up to three ***External Ticket*** columns.

> **NOTE:** To link an external ticket to an event, you must create a custom run book automation policy and a custom run book action or use the ScienceLogic APIs. For help with these tasks, contact ScienceLogic Customer Support.

- ***Acknowledge***. If the event has not been acknowledged, this column displays an **[Acknowledge]** button; click the button to acknowledge the event. If the event has been acknowledged, this column displays a check-mark character and specifies the user who acknowledged the event. For more information, see *Acknowledging and Clearing Events*.
- ***Clear***. Click the **[Clear]** button to clear the event. When you do so, the event is removed from the **Events** page.

> **NOTE:** If you have defined any base or extended custom attributes, you can also add those custom attributes as columns that appear on the **Events** page.

Events That Do Not Appear on the Events Page

In Skylar One, there are four types of events that might not appear on the **Events** page (or the **Event Console** page):

- Rolled-up events
- Suppressed events
- Topology events
- Event masks

For more information about these event types, see the section on *Event Correlation*.

Understanding Event Severity

Each event in Skylar One is color-coded to make it easy for you to determine its severity:

Color	Severity	Description
Red	Critical	Indicates a condition that can seriously impair or curtail service and requires immediate attention (for example, service or system outages).
Orange	Major	Indicates a condition that impacts service and requires immediate investigation.
Yellow	Minor	Indicates a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
Blue	Notice	Indicates a condition that users should be aware of but does not affect service.
Green	Healthy	Indicates that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.

Searching and Filtering the List of Events

This section explains how to filter the list of events so you can quickly locate and address any potential issues in your environment.

Filtering Events by Organization and Service

You can view events from all organizations or services, or filter down to just the organizations or services you want to monitor for events.

To view events by organization or service:

1. On the **Events** page, click the **View** menu.
2. Select the **Group by organization** and/or the **Group by business service** toggle. The relevant panel appears on the left with a list of events sorted by severity for each organization and/or service.
3. On the left panel, click the check mark icon ( ) to filter the list of events based on the organization or service you selected.

> **TIP:** In the right-hand panel, click the name of a service to go to the **Service Investigator** page for that service. Click the name of an organization to go to the **Organizational Summary** page for that organization.

4. To hide the **Organizations** or **Business Services** panels, click the left arrow icon ( ). Click the right arrow icon ( ) to expand the panel again.

Filtering Events by Severity

The **Events** page displays a list of currently active events, which can be sorted by any column, such as severity from critical to healthy. You can filter the list of events by severity by clicking one or more of the five colored buttons near the top of the **Events** page.

When you click a severity button, the list displays only events with the severity you selected. The severity button you clicked remains in color, while the other buttons turn gray.

For more information about severity values, see the section *Understanding Event Severity*.

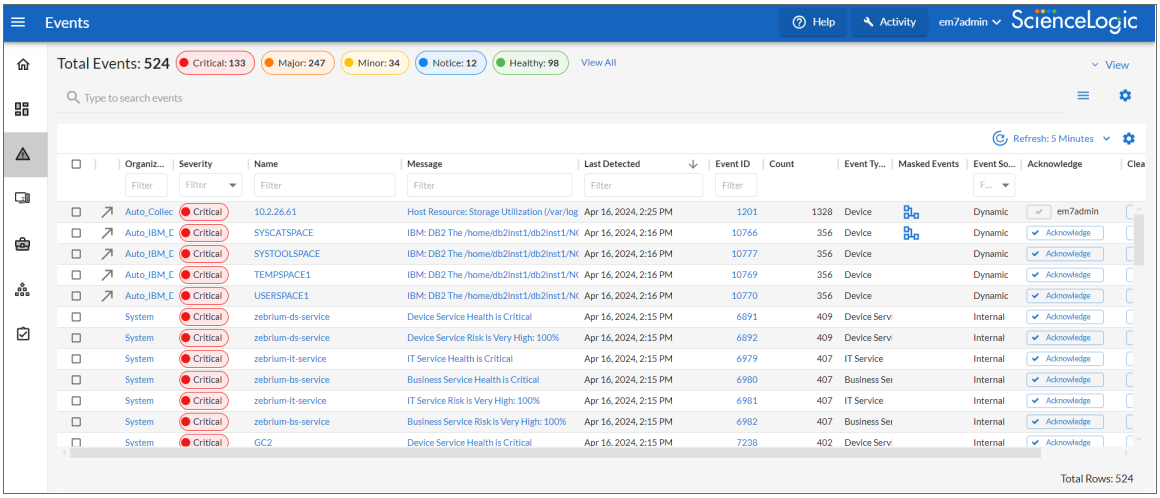
> **TIP:** To clear a severity filter, click the **View All** link next to the severity buttons.

> **TIP:** To add color-coded highlights to rows on the events inventory table that correspond to the severity color of the event, click the grid settings ( ) icon, select *Event Table Preferences*, and then toggle on ***Row Severity Highlighting***.

Filtering for Masked Events

When a device uses the ***event mask*** setting, events that occur on a single device within a specified span of time are grouped together, and only the event with the highest severity is displayed on the **Events** page. This allows related events that occur in quick succession on a single device to be rolled up and posted together under one event description. For example, if a device cannot connect to the network, multiple other services on the device raise events. Skylar One displays the event with the highest severity and rolls up all the other events.

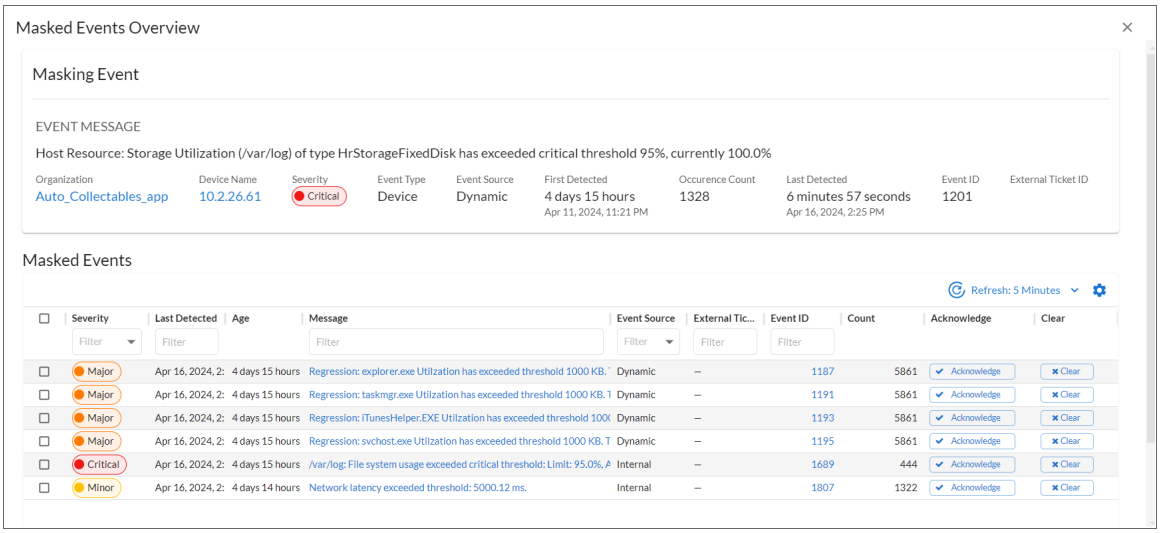
On the **Events** page, any event that contains masked events includes a masked events icon ( ) in the ***Masked Events*** column:



TIP: To add the ***Masked Events*** column from the table on the **Events** page, click the grid settings ( ) icon, select *Event Table Preferences*, and then toggle on ***View Event Masking***. To remove the ***Masked Events*** column, toggle off ***View Event Masking***. If you remove the ***Masked Events*** column, any events that would have appeared on this table appear in the main event console instead.

To view more information about masked events:

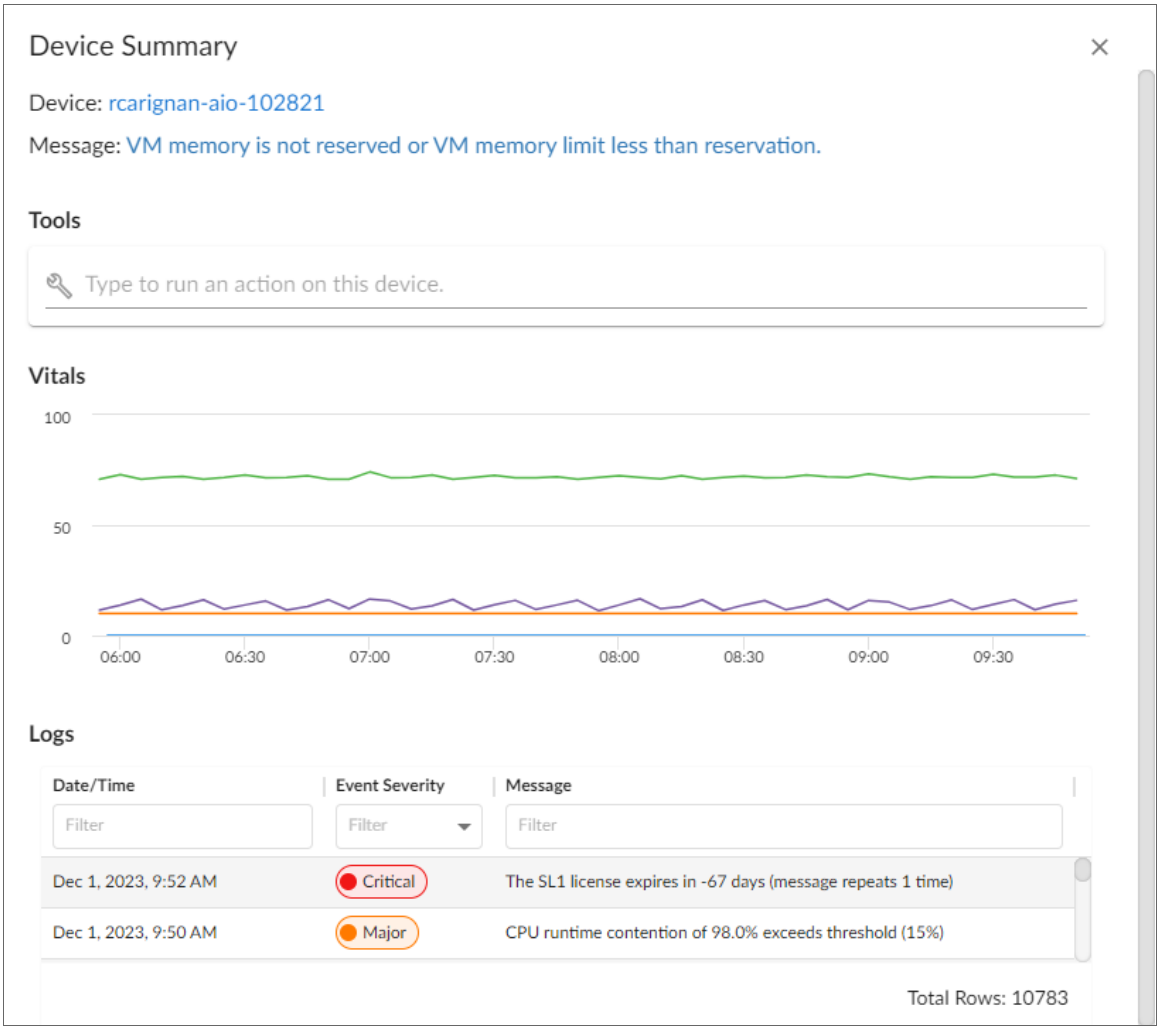
1. On the **Events** page, click the masked events icon ( ) in the ***Masked Events*** column for the relevant event. The **Masked Events Overview** modal for that event appears.
2. The **Masked Events Overview** modal includes the following details about the masking and masked events:



- ***Masking Event***. This section includes information about the masking event, which is the event that appears on the **Events** page.
- ***Masked Events***. This section includes information about the masked events, which are related events that are configured to be maskable and grouped together under the masking event if they occur within a specified period of time.

Viewing Additional Data about an Event

On the **Events** page and the **Devices** page, you can click the open icon (↗) next to an event or device to open a **Device Summary** modal:



NOTE: On the **Events** page, the **Device Summary** modal displays only for events that are aligned with devices.

The detail window for that device contains the **Tools** pane, the **Vitals** pane, and the **Logs** pane:

- The **Tools** pane enables you to run a set of diagnostic tools or user-initiated actions in the **Activity Center**, or to click on custom links that will open in a separate browser window. Click the search bar to search for tools, actions, or custom links that are available for the device.

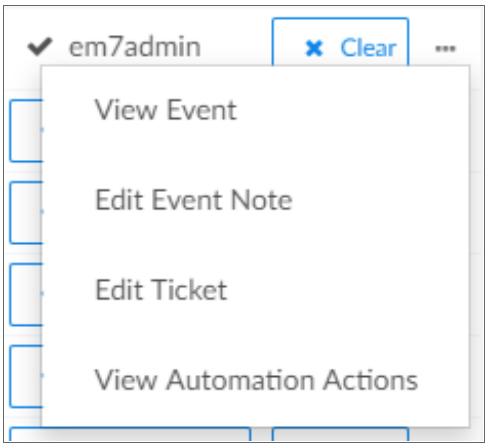
- The **Vitals** pane displays graph data for the past four hours of CPU usage, memory usage, and latency for that device, where relevant. You can zoom in on a shorter time frame in the **Vitals** graph by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- The **Logs** pane displays a list of events associated with that device.

TIP: To open the detail or Investigator page for an item, click the link for the item name at the top of the detail window.

Viewing Automation Actions

To view a log of automated actions that have occurred for an event, on the **Events** page, click the actions icon (⋮) for the event and select *View Automation Actions*. When you do so, the **Event Actions Log** modal appears.

NOTE: You can also view the **Event Actions Log** modal by clicking the hyperlink in the ***Automated Actions*** column for a particular event on the **Events** page.



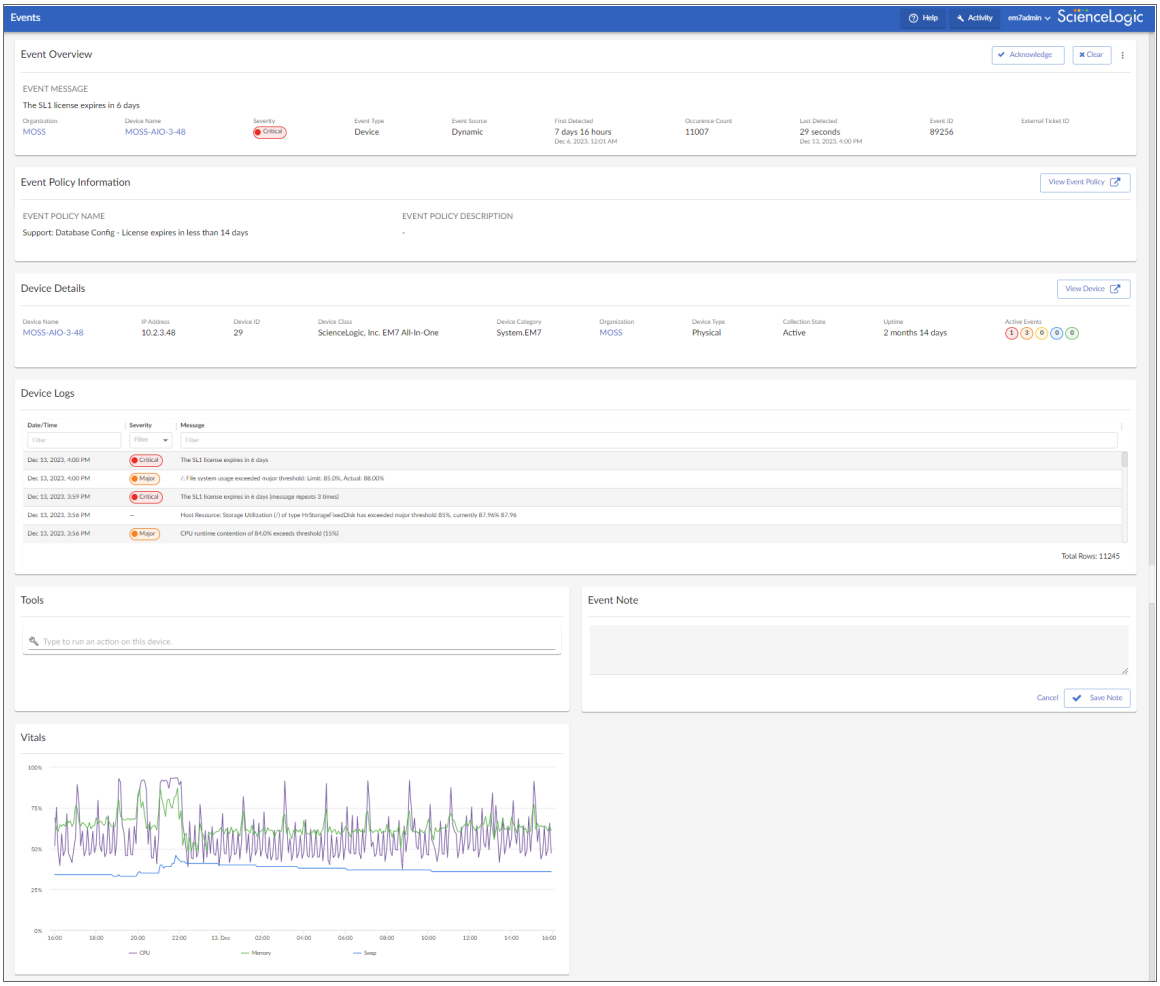
The **Event Actions Log** displays a history of all automation actions that Skylar One executed in response to the event.

Each entry in the **Event Actions Log** modal includes:

- The date and time when the action was executed
- The automation policy that triggered the action
- The name of the action policy
- The result of the action

Using the Event Investigator

The **Event Investigator** page provides details about the event as well as the device associated with the event, where relevant. The **Event Investigator** page includes the **Event Overview**, **Masked Events**, **Event Policy Information**, **Device Details**, **Device Logs**, **Tools**, **Event Note**, and **Vitals** widgets.



TIP: To get to the **Event Investigator** page, click the linked text in the ***Message*** column of the **Events** page, or click the actions icon (⋮) for the event and select *View Event*. Alternatively, you can click the ID associated with the event in the ***Event ID*** column.

The top pane of the **Event Investigator** page contains basic event details. From this pane, you can also acknowledge the event, clear the event, or click the actions icon (⋮) and select *Create Ticket* to create a ticket for that event. If an event was acknowledged by another user and you have the relevant permissions, you can click the **[Reacknowledge]** button to acknowledge that event.

> **TIP:** On the **Event Investigator** page, click the name of an aligned device or service to go to the Investigator page for that device or service. When you do so, information about the event appears in a panel at the top of the page. This panel gives you the option to view conflicts and resolutions for that event.

The **Event Investigator** page includes the following widgets:

- ***Event Overview***. Displays additional information about the event, such as details about the type of event, the source of the event, the time and date the event was first detected, the number of concurrences, and more.
- ***Masked events***. A list of all masked events for the device, where relevant. When a device uses the ***event mask*** setting, events that occur on a single device within a specified span of time are grouped together, and only the event with the highest severity is displayed in the **Events** page. This allows related events that occur in quick succession on a single device to be rolled up and posted together under one event description.
- ***Event Policy Information***. Displays information about the event policy and any descriptions associated with the event.
- ***Device Details***. A Consolidated widget that displays information about the device, such as the class and category the device belongs to, the type of device, the number of active events for each severity level, and more.
- ***Device Logs***. A list of log entries from the device's log, sorted from newest to oldest by default.
- ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions. This pane is the same as the **Tools** pane of the Event Drawer. For more information, see the section on *Using the Action Runner*.
- ***Event Note***. A text field where you can add new text and edit existing text related to the event and the device associated with the event. For more information, see *Viewing and Editing Event Notes.*
- ***Vitals***. A widget that displays the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- ***Skylar Analytics Summary***. Displays a graph of data from Skylar AI-sourced events corresponding with the event ID.

Using the Action Runner

You can access the **Action Runner** from either the **Events** page or the **Event Investigator** page. The **Action Runner** enables you to run a set of diagnostic tools or user-initiated actions, or to click on custom links that will open related records in external systems in a separate browser window.

NOTE: The tools and actions that are available in the **Action Runner** are based on the device type and your user permissions, as determined by your organization assignment and access hooks. For example, if a device does not have an IP address, only the Availability tool will be available.

NOTE: For more information about user-initiated actions, see the section on *User-Initiated Automations*.

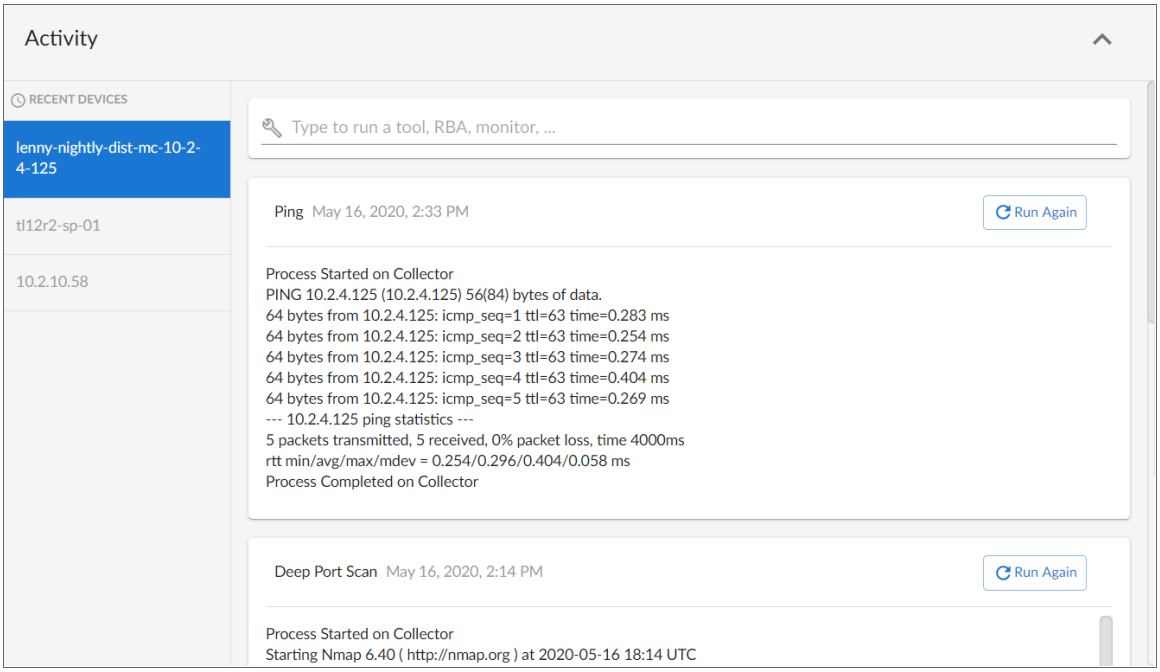
To use the **Action Runner**:

1. Access the **Action Runner** for events in one of the following ways:
    - On the **Action Runner** page, open the **Event Drawer** for a particular event. Click the search bar in the **Tools** pane.
    - On the **Action Runner** page, click the search bar in the **Tools** pane.
    - Click the **[Activity]** button in the top navigation bar of any page in Skylar One. Click the search bar.
2. When you click the search bar, a list displays the default tools, actions, or custom links that are available for the selected device. Click one of these tools, actions, or custom links, or use the search bar to search for a tool or action that is not listed. The following default tools are available in the **Action Runner**:
    - ***Availability***. Displays the results of an availability check of the device, using the port and protocol specified in the ***Availability Port*** and ***Availability Protocol*** fields on the **[Settings]** tab for this device.
    - ***Ping***. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by Skylar One to communicate with the device) and waits for a reply. Skylar One then displays the number of seconds it took to receive a reply from the device and the number of bytes returned from the device. If the device has an IPv6 address, Skylar One uses the appropriate IPv6 ping command.
    - ***Who Is***. Displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
    - ***Port Scan***. Displays a list of all open ports on the device at the time of the scan.
    - ***Deep Port Scan***. Displays a list of all open ports and as much detail about each open port as the deep port scanner can retrieve.
    - ***ARP Lookup***. Displays a list of IP addresses for the device and the resolved Ethernet physical address (MAC address) for each IP address.
    - ***ARP Ping***. Displays the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it uses the ARP protocol instead of ICMP. The ARP Ping tool can be used only on the local network.

- *Trace Route*. Displays the network route between Skylar One and the device. The tool provides details on each hop to the endpoint. If the device has an IPv6 address, Skylar One uses the appropriate IPv6 traceroute command.

> **TIP:** The tools found in the **Action Runner** can also be found in the Device Toolbox in the classic Skylar One user interface.

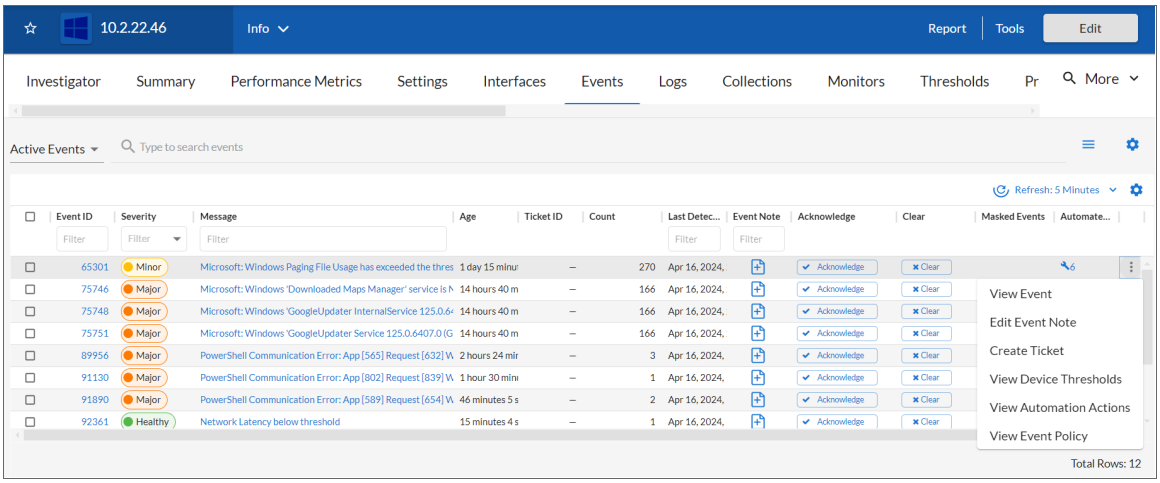
3. If you clicked a custom link, the link opens in a new browser window or tab. If you clicked on a tool or action, then its progress and results appear in a log in the **Activity Center** page as it runs.
4. After the tool or action has run, if you want to run it again, click the **[Run Again]** button. This button appears only for activities completed during your current session.



> **NOTE:** The left pane of the **Activity Center** page displays a list of devices for which you have most recently used the **Action Runner**, with the current device at the top of the list. To use the **Action Runner** for any of the other recently used devices, or to view historical logs for the tools or actions that have been run on those devices, click on the device name.

Viewing Events for a Single Device

On the **[Events]** tab of the **Device Investigator**, you can view a list of events associated with the device.



TIP: You can rearrange the columns in the list by clicking and dragging the column to a new location. You can adjust a column's width by clicking and dragging the right edge of the column. For more information about editing and adding columns, see the topic on *Editing the Settings for an Inventory Page*.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the topic on *Adjusting the Row Density*.

TIP: You can toggle between *Active events* and *Cleared events* by using the drop-down to the left of the ***Search*** field. On this tab, you can also acknowledge and clear an event if you have permission for those actions.

For each event, the **[Events]** tab displays the following information:

- ***Event ID***. The unique ID for the event, generated by Skylar One. The ID appears as a hyperlink. To view the **Event Investigator** page for the event, click the ***ID*** hyperlink. For more information about the **Event Investigator** page, see the section on *Using the Event Investigator*.
- ***Severity***. The severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Message***. The message generated for the event. The message appears as a hyperlink. To view the **Event Investigator** page for the event, click the ***Message*** hyperlink. For more information about the **Event Investigator** page, see the section on *Using the Event Investigator*.
- ***Age***. The amount of time (in days, hours, and minutes) since the event first occurred or since its last occurrence without having been cleared.
- ***Ticket ID***. If a ticket has been created for the event, this column displays the ticket ID of that ticket.

- ***Count***. The number of times this event has occurred, the number of child events associated with the event, or the number of masked events associated with the event.
- ***Last Detected***. The date and time at which the event last occurred on the device.
- ***External Ticket***. The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in Skylar One). If this field displays a value, you can click on that value to spawn a new window and view the external ticket. You can display up to three ***External Ticket*** columns.

> **NOTE:** To link an external ticket to an event, you must create a custom run book automation policy and a custom run book action or use the ScienceLogic APIs. For help with these tasks, contact ScienceLogic Customer Support.

- ***Event Note***. A user-defined note to accompany the event. To create or edit a note, click the note icon ( ). The **Edit Event Note** modal appears, where you can create or edit a note and save your changes.
- ***Acknowledge***. If the event has been acknowledged, this column displays a check mark and the username of the user who acknowledged the event. If the event has not yet been acknowledged, this column displays an **[Acknowledge]** button; click the **[Acknowledge]** button to acknowledge the event. When you ***acknowledge*** an event, you let other users know that you are aware of that event and are working on a response.
- ***Clear***. Click the **[Clear]** button to clear the event. When you ***clear*** an event, you let other users know that this event has been addressed. Clearing an event removes a single instance of the event from the **[Events]** tab. If the same event occurs again on the same device, it will reappear in the **[Events]** tab, even if you have previously cleared that event.
- ***Event Source***. The system or application that generated this event. For more information, see the section on *Event Sources*.
- ***Masked Events***. If the event has occurred multiple times on the same device that uses the ***event mask*** setting, click the masked events icon ( ) to open the **Masked Events Overview** modal. In this modal, you can view details about the masked events. For more information, see the section *Filtering for Masked Events*.
- ***Automated Actions***. The number of times the event has triggered the execution of an automation policy. If the event has triggered one or more automated actions, click the number hyperlink to go to the **Event Actions Log**, where you can view a log of all automated actions that have occurred for the event. For more information, see the section *Viewing Automation Actions*.

> **NOTE:** You can also view the **Event Actions Log** modal by clicking the actions icon ( ) for the event and selecting *View Automation Actions*.

Clicking the actions icon ( ) next to an event gives you the following options, based on your permissions:

- *View Event*. Navigates to the **Event Investigator** page for that event.
- *Edit Event Note*. Lets you update the Note associated with this event.

- *Create Ticket*. Opens a new ticket in the Skylar One **Ticket Editor**, if you are using Skylar One for your ticketing.
- *Edit Ticket*. Opens an existing ticket in the Skylar One **Ticket Editor**, if you are using Skylar One for your ticketing.
- *Create External Ticket*. Creates a new ticket for the event if you are using an external ticketing system instead of Skylar One.
- *View Event Policy*. Opens the **Event Policy Editor** page for the policy aligned with this event.
- *View Device Thresholds*. Opens the **Device Thresholds** page for the device on which the event occurred.
- *Suppress Event for this Device*. Suppresses the current event on the current device. When you suppress an event, you are specifying that, if this event occurs again in the future on the same device, the event does not appear again in the **Events** page or the **[Events]** tab for the device.
- *View Automation Actions*. Displays a log of automations that have occurred for that event. This option is hidden if the event does not have any automation actions aligned to it.

Event Throttling

When Skylar One detects syslog messages or traps coming from a single device at a rate greater than 25 messages per second, Skylar One throttles the messages.

When Skylar One throttles messages from a single IP address, those messages are deleted from the ScienceLogic database. The messages are not passed to the event engine, are not logged, and are not processed as events.

When Skylar One throttles messages, Skylar One also triggers events:

- ***Event with a Severity of Critical and the message "Inbound Message Flood"***. This event is triggered when a single IP exceeds the threshold of syslog messages or trap messages at least once per minute for the last 10 minutes. The default threshold is 25 messages per second.
- ***Event with a Severity of Notice and the message "Inbound Message Spikes".*** This event is triggered when a single IP exceeds the threshold of syslog messages or trap messages. The default threshold is 25 messages per second.

Message throttling is enabled by default. To disable message throttling, contact ScienceLogic Customer Support.

To adjust the threshold for message throttling, contact ScienceLogic Customer Support.

To whitelist an IP address so that message throttling does not apply to that IP, contact ScienceLogic Customer Support.

NOTE: Skylar One does not support message throttling on IPv6 devices monitored by CentOS5 Data Collectors.

Viewing Events from the Event Console

To view a list of all active events on the **Event Console** page, go to Events > Classic Events, or the Events tab in the classic user interface.

> **NOTE:** To view the **Event Console** page, non-administrator user accounts must be granted one or more access keys that include the following access hook: Events/Event:View. Non-administrator user accounts can then view events that have the same organization as the user. For more information on Access Keys, see the section on *Access Keys*.

Each event is color-coded to make it easy for you to determine severity. For more information about severity values, see the section *Understanding Event Severity*.

Events in the **Event Console** are rolled up. This means that if the same event occurs multiple times on a single device, you see only one entry in the **Event Console**, and the value in the ***Count*** column indicates the number of times the event has occurred.

On the **Event Console** page, you can use the following tools for searching and filtering the list of events that displays in the page:

- The ***Global Search*** drop-down list and field, which can filter the entire list of events by one of the columns or by device group ID or device group name. You can save the results of a Global Search as a **Custom View**.
- The ***filter-while-you-type*** fields, which can filter the list of events by one or more of the event parameters.
- The ***Advanced Filter Tool***, where you can enter more complex filters, based on your current Skylar One configuration.

> **NOTE:** The settings in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page (Events > Actions > Console Preferences) affect the scope of the ***filter-while-you-type*** fields and the ***Advanced Filter Tool***. If you select the ***Group by Organization*** checkbox in the **Account Preferences** page or the **Event Console Preferences** page, events in the **Event Console** are grouped by organization. The ***filter-while-you-type*** fields and the advanced filter tool appear for each organization grouping and act only on the events in that organization grouping. You cannot apply a single filter to events in multiple organizations. For more details on the **Account Preferences** page and the **Event Console Preferences** page, see the section on *Customizing the Display in the Event Console*.

The **Event Console** displays a legend, showing the number of events of each severity.

- If you select the ***Group by Organization*** checkbox in the **Account Preferences** page (Preferences > Account > Preferences) or in the **Event Console Preferences** page (Events > Actions > Console Preferences), the **Event Console** displays the legend for each organization.

- If you do not select the ***Group by Organization*** checkbox, the **Event Console** displays the legend for all events in all organizations (that you are allowed to view).
- For each severity, the legend indicates the number of events displayed on the current page. The second number, in parentheses, indicates the additional number of events with the same severity that are not displayed in the current page. These additional events either display on a subsequent page or do not display because of the current filters applied to the page or because of the setting in the ***Default Severity Filter*** field in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page. For example, "3 (+7) Healthy" means that the current page displays three events with a severity of "Healthy" and that seven more events with a severity of "Healthy" exist but are not displayed in the current page.

Events That Are Not Displayed in the Event Console

In Skylar One, there are four types of events that might not appear on the **Events** page (or the **Event Console** page):

- Rolled-up events
- Suppressed events
- Topology events
- Event masks

For more information about these event types, see the section on *Event Correlation*.

Information about Each Event Displayed in the Event Console

For each event, the **Event Console** can display the following information:

> **TIP:** To sort the list, click on a column heading. The list will be sorted by the column value, in ascending order. To sort the list by descending order, click the column heading again. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering the Items on a Classic Page* in the ***Introduction to Skylar One*** manual.

- ***Organization***. Specifies the organization that the event is associated with. If you want to group all events based on their organizations, select the ***Organizational Grouping Events*** checkbox in the **Account Preferences** page (Preferences > Account > Preferences) or the ***Group by Organization*** checkbox in the **Event Console Preferences** page (Events > Actions > Console Preferences).
- ***Contact Information***. If you have grouped events by organization, this column displays the contact information for each organization.
- ***Severity Counts***. If you have grouped the events by organization, this column displays the number of events for each severity that are associated with the organization.
- ***Report Icon***. Icon that leads you to more information about the element or policy associated with the event.

- ***Name***. Name of the entity associated with the event.
- ***Type***. Type of entity associated with the event. The possible options are:
    - Aggregate Services
    - Assets
    - Business Services
    - Device Services
    - Devices
    - Interfaces
    - IP networks
    - IT Services
    - Organizations
    - User Accounts
    - Vendors
    - Virtual Interfaces
- ***Event Message***. Message generated for the event.
- ***Severity***. Severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Acknowledged***. If the event has been acknowledged, this column displays a red check-mark character and specifies the user who acknowledged the event. If the event has not been acknowledged, this field displays a gray check-mark character. To acknowledge an event, click in this column.
- ***Note***. User-defined note to accompany the event. To create or edit a note, select the wrench icon (🔧) in this column. The **Add a Note** modal page appears, where you can create or edit a note and save your changes.
- ***Ticket***. If a ticket has been created for the event, this column displays the ticket ID of that ticket.
- ***External Ticket***. The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in Skylar One). If this field displays a value, you can click on that value to open a new window and view the external ticket.

> **NOTE:** To link an external ticket to an event, you must create a custom run book automation policy and a custom run book action or use the ScienceLogic APIs. For help with these tasks, contact ScienceLogic Customer Support.

- ***Age/Elapsed*** . Number of days, hours, and minutes since the first occurrence of the event. This is also the time since the event occurred without the event having been cleared.

- ***Last Detected***. Date and time the event last occurred on this entity.
- ***EID***. Unique ID for the event, generated by Skylar One.
- ***Source***. System or application that generated this event. For more information, see the section on *Event Sources*.
- ***Count***. Number of times this event has occurred or number of child events associated with the event or number of masked events associated with the event.
- ***Notify***. Number of times the event has triggered the execution of an Automation Policy.
- ***Information icon*** (). Displays the **Event Information** page, where you can view an overview of the selected event, suppress the selected event, or edit the definition of the selected event.
- ***View Notifications icon*** (). Leads to the **Event Actions Log**, where you can view details about each automation policy that has triggered for the event.
- ***Ticket icon*** (). Depending upon the setting ***Ticket Life Ring Button Behavior*** (found in System > Settings > Behavior), one of the following happens:
    - The **Ticket Editor** page appears. If a ScienceLogic ticket is already aligned with this event, you can view details about the ticket. If a ScienceLogic ticket is not yet aligned with this event, you can define a ticket, and the Skylar One system automatically associates the new ticket with the selected event.
    - If an external ticket is aligned with an event, when you select the life-ring icon () for that event (from the **Event Console**), Skylar One opens a new window and displays the external ticket (as specified in the *force_ticket_uri* field). If an external ticket is not yet aligned with an event, when you select the life-ring icon () for that event, Skylar One sets a "request" flag for the ticket and displays an acknowledgment that a new ticket has been requested. You can then use the "request" in run book logic to create the ticket on the external system.

Global Search Field

You can use the ***Global Search*** field in the upper left of the page to filter the entire list of displayed events by a single parameter. Skylar One updates the **Event Console** and displays only events that have a matching parameter.

To use the ***Global Search*** field, enter values in the ***Search*** drop-down list and the ***Text*** field:

- ***Search***. You can select one of the following search parameters:
    - *Organization*. Appears only if you have not selected the ***Group by Organization*** checkbox in the **Account Preferences** page (Preferences > Account > Preferences) or in the **Event Console Preferences** page (Events > Actions > Console Preferences). Name of the organization associated with the event.
    - *Name*. Name of the entity associated with the event.
    - *Type*. Type of entity associated with the event.
    - *Event Message*. Message generated for the event.
    - *Severity*. Severity of the event. For more information about severity values, see the section *Understanding Event Severity*.

- *Acknowledged*. If the event has been acknowledged, search for the user who acknowledged the event.
- *Note*. User-defined note associated with the event.
- *Ticket*. If a ticket has been created for the event, this parameter searches by the ticket ID of that ticket.
- *External Ticket*. The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in Skylar One).
- *Age/Elapsed*. You can enter time in seconds, and the **Event Console** page displays only events that last occurred within that number of seconds or less.
- *Event ID*. Unique ID for the event, generated by Skylar One.
- *Source*. System or application that generated this event. For more information, see the section on *Event Sources*.
- *Count*. Number of times this event has occurred.
- *Notify*. Number of times the event has triggered the execution of an Automation Policy.
- *Device Group ID*. Unique ID for the device group associated with the event.
- *Device Group Name*. Name of the device group associated with the event.

- ***Text***. For each search parameter, you must enter text to match. Skylar One searches for events that match the text, including partial matches. Text matches are not case-sensitive. You can use special characters in each filter.

To perform another search on the results of the previous search:

1. Click the plus-sign (+) to the left of the ***Refresh Timer***.
2. This adds another ***Search*** field and ***Text*** field to the top of the page. This second search searches only the results from the first search.
3. You can add as many ***Search*** and ***Text*** fields as you need.

NOTE: You can save the results of a ***Global Search*** as a custom view.

Advanced Filter

On the **Event Console** page, you can specify one or more parameters to filter the list of events. Only events that meet all the filter criteria are displayed.

In some fields, you can use the **Advanced Filter Tool** to make selections instead of manually typing in a string to use as a filter.

The settings in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page (Events > Actions > Console Preferences) affect the scope of the **Advanced Filter Tool**. If you select the ***Group by Organization*** checkbox in the **Account Preferences** page or the **Event Console Preferences** page:

- Events on the **Event Console** page are grouped by organization.
- The **Advanced Filter Tool** appears for each organization grouping and acts only on the events in that organization grouping. You cannot apply a single advanced filter to events in multiple organizations.
- You cannot filter by organization using the **Advanced Filter Tool**.
- The possible filter options are pre-filtered by each organization.

TIP: To select multiple entries in the **Advanced Filter Tool**, hold down the **Ctrl** key and left-click the entries.

TIP: To reset each field to empty and apply no filters, click the **[Reset]** button.

For each filter except ***Severity*** and ***Last Detected***, you must enter text to match against. Skylar One searches for events that match the text, including partial matches. For the ***Type*** and ***Source*** filters, you can enter text to match against or you can select from the list of possible values. Text matches are not case-sensitive. You can use special characters in each filter.

To access the **Advanced Filter Tool**:

1. Go to the **Event Console** page (Events > Classic Events, or the Events tab in the classic user interface).
2. Click on the funnel icon ( ).
3. The **Advanced Filter Tool** displays advanced filters for each column in your default display. To change the columns that are displayed on the **Event Console** page, see the section *Customizing the Display in the Event Console*.

   NOTE: Unlike the "filter while you type" feature, the **Advanced Filter Tool** is not applied to the list of events until you select the **[Apply]** button.

4. In the **Advanced Filter Tool**, filter by one or more of the available filters.
5. Click **[Apply]** to apply the advanced filters. Click **[Reset]** to clear the advanced filters and start again.
6. Click **[Reset]** for the **Event Console** page to return to the default list of events.

TIP: You can perform an advanced filter and then perform a second advanced filter on the results of the first advanced filter. You can perform an advanced filter multiple times, to perform multiple filters.

Custom View

You can save a filtered list of events created with the *Global Search tool*. When you do so, you create a ***custom view***. You can then return to the page at any time and display the custom view, without having to

filter the list again.

To save a custom view:

1. Go to the **Event Console** page (Events > Classic Events, or the Events tab in the classic user interface).
2. Using the *Global Search tool*, filter the list of events.
3. In the ***Custom View*** drop-down field, select *new custom view*.
4. Click the **[Save]** button.
5. Skylar One prompts you to enter a name for the new custom view.
6. The new custom view now appears in the ***Custom View*** drop-down list.
7. To edit the custom view, select it from the ***Custom View*** drop-down list, make changes with the ***Global Search*** tool, and then click the **[Save]** button for the custom view to save your changes.
8. To display the custom view, select it from the ***Custom View*** drop-down list.
9. To delete the custom view, select it from the ***Custom View*** drop-down field and then click the **[Delete]** button. The custom view no longer appears in the ***Custom View*** drop-down list.

Viewing Events for a Single Device in the Classic Skylar One User Interface

To view a list of events for a single device in the classic user interface, you can go to the **Viewing Active Events** page in the **Device Reports** panel.

> **NOTE:** To view the **Viewing Active Events** page, non-administrator user accounts must be granted one or more access keys that include all the following access hooks: Registry, Registry>Devices>Device Manager, Dev:Events Summary, Dev:View Summary, and Event:View (From Dev Properties). For more information on Access Keys, see the section on *Access Keys*.

To view a list of events for a single device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Find the device that you want to view events for and select its bar graph icon ( ).
3. In the **Device Reports** panel, select the **[Events]** tab.
4. The **Viewing Active Events** page appears.

   This page displays all of the currently active events for the device. For each event, the page displays:

   - ***Event Message | Severity***. Message generated by event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). The message is color-coded for severity. For more information about severity values, see the section *Understanding Event Severity*.

- ***Acknowledged***. Specifies whether a ScienceLogic user has acknowledged this event.
- ***Age/Elapsed***. Number of days, hours, and minutes since the first occurrence of the event.
- ***Ticket***. Ticket ID associated with this event, if applicable.
- ***Last Detected***. Date and time of last occurrence of the event.
- ***EID***. Unique ID for the event, generated by Skylar One.
- ***Source***. Source of the log message that triggers the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). For more information, see the section on *Event Sources*.
- ***Count***. Number of times this event has occurred.
- ***View Notifications icon*** ( ). Leads to the **Event Actions Log**, where you can view details about each automation policy that has triggered for the event.
- ***Statistics icon*** ( ). Displays the **Event Statistics** page, where you can view historical statistics for the selected event.
- ***Information icon*** ( ). Displays the **Event Information** page, where you can view an overview of the selected event, suppress the selected event, or edit the definition of the selected event.

NOTE: To view a list of all cleared events for the device, select the **[Cleared]** button. To return to the list of active events, select the **[Active]** button.

Viewing Events for a Single Organization

One of the easiest ways to monitor the health of your network is to look at events. Events are messages that are triggered when a specific condition is met. For example, an event can signal that a server has gone down, that a device's hard drives are getting too full, or simply display the status of a device.

Each instance of an event in Skylar One is associated with an organization. Each occurrence of an event is grouped by organization (the organization associated with the device where the event occurred or the organization associated with the policy that generated the event).

In the **Organizational Administration** panel, you can view a list of events associated with a specific organization.

To view a list of events associated with a specific organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization with associated events that you want to view.
3. If a value appears in the *Events* column, click the event icon ( ).
4. The **Organizational Events** page appears for the organization.

This page displays a list of all active events associated with the organization or the organization's elements. For each event, the page displays:

- ***Name***. Name of the element associated with the event.
- ***Event Message | Severity***. Message generated by event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). The message is color-coded for severity.
- ***Acknowledged***. Specifies whether a ScienceLogic user has acknowledged this event.
- ***Age/Elapsed***. Number of days, hours, and minutes since the first occurrence of the event.
- ***Ticket***. Ticket ID associated with this event, if applicable.
- ***Last Detected***. Date and time of last occurrence of the event.
- ***EID***. Unique ID for the event, generated by Skylar One.
- ***Source***. Source of the log message that triggers the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). For more information, see the section on *Event Sources*.
- ***Count***. Number of times this event has occurred.
- ***View Notifications icon*** (). Leads to the **Event Actions Log**, where you can view details about each automation policy that has triggered for the event.
- ***Statistics icon*** (). Displays the **Event Statistics** page, where you can view historical statistics for the selected event.
- ***Information icon*** (). Displays the **Event Information** page, where you can view an overview of the selected event, suppress the selected event, or edit the definition of the selected event.

NOTE: To view a list of all cleared events for the organization, click the **[Actions]** menu and select ***View Cleared Events***. To return to the list of active events, click the **[Actions]** menu and select ***View Active Events***.

Viewing Event Details in the Event Console

In the classic Skylar One user interface, you can view details about an event, suppress an event, and access the event policy from the **Event Information** page.

NOTE: To view the **Event Information** page, non-administrator user accounts must be granted one or more access keys that include the following access hook: Events/Event:View. Non-administrator user accounts can then view details for all events in the same organization as the user.

To access the **Event Information** page:

1. Go to the **Event Console** page (Events > Classic Events, or the Events tab in the classic user interface).
2. Find the event you are interested in and select its information icon (). The **Event Information** page appears:

The **Event Information** page displays the following details about the event:

- ***Event ID***. Unique ID for the event, generated by Skylar One.
- ***Event Message***. Message generated by the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit).
- ***Severity***. Severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***For Element***. Name of the element associated with the event.
- ***First Occurrence***. Number of days and hours since the first occurrence of the event, and date and time of first occurrence of the event.
- ***Last Occurrence***. Number of days and hours since the last occurrence of the event, and date and time of last occurrence of the event.
- ***Occurrence Count***. Number of times this event has occurred on this entity.
- ***Acknowledged On***. Date and time the event was acknowledged.
- ***Acknowledged By***. Username of user who acknowledged the event.
- ***Policy Name/ID***. Name of the event policy, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit) and policy ID.
- ***Policy Type***. Source of the log message that triggers the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). For more information, see the section on *Event Sources*.
- ***Ticket Description***. Description field from the associated ticket, if applicable.
- ***Probable Cause & Resolution Text***. This pane displays additional information about the event, as defined in the **Event Policy Editor**page (Registry > Events > Event Manager > create or edit).
- ***Correlation Reason***. This field displays the user-defined notes about event categories and event correlation. You can enter up to 256 characters in this field. To save your changes, select the **[Save Correlation Reason]** button.
- ***Note***. This field displays the user-defined note associated with the event. To add or edit a note, enter text in this field and then select the **[Save Note][Save Note]** button.

Depending on your Access Keys, the **[Actions]** menu displays one or more of the following entries:

- ***Create a Ticket***. Leads to the **Ticket Editor** page, where you can define a new ticket based on the event.
- ***Edit Aligned Ticket***. Leads to the **Ticket Editor** page, where you can edit an existing ticket that is based on the event.
- ***Edit Aligned Event Policy***. Leads to the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit), where you can edit the properties of the event definition.
- ***Edit Device Thresholds***. Leads to the **Device Thresholds** page, where you can define and edit storage and performance thresholds for a device.
- ***Suppress Event for This Device***. Suppresses the current event on the current device. When you suppress an event, you are specifying that in the future, if this event occurs again on the same device, the event does not appear in the **Event Console** or the **Viewing Events** page.
- ***Refresh This Page***. Updates the page with the latest information.

- ***View Device Summary***. Leads to the **Device Summary** page for the device, where you can view overview information on the health of the device, a list of events and tickets associated with the device, a list of elements associated with the device, a list of monitoring policies for the device, and hardware and bandwidth usage for the device.

Customizing the Display in the Event Console

You can customize the appearance of the **Event Console** page in the classic Skylar One user interface from two places:

- The **Account Preferences** page. In this page, you can select the columns that display on the **Event Console** page.
- The **[Actions]** menu in the **Event Console** page. When you select the *Console Preferences* entry, Skylar One displays the **Preferences** modal page, where you can define the appearance and behavior of the **Event Console** page.

Account Preferences

On the **Account Preferences** page, you can change your password and customize some of the behavior and appearance of Skylar One. The customizations that you choose appear each time you log in to Skylar One. They do not affect how Skylar One appears to other users.

In the **Account Preferences** page, you can customize how the **Event Console** page appears.

> **NOTE:** To access the **Account Preferences** page, non-administrator user accounts must be granted one or more access keys that include the following access hook: MyPreferences. Non-administrator user accounts can then view and edit the settings in the **Account Preferences** page. For more information on Access Keys, see the section on *Access Keys*.

To access the **Account Preferences** page:

1. Go to the **Account Preferences** page (Preferences > Account > Preferences).
2. In the **Account Preferences** page, you can edit one or more of the fields described below.
3. You can use the **Change Password** pane to change your password. Passwords must be between seven and 64 characters in length. The following fields appear:
   - ***Existing Password***. Type your current password.
   - ***New PasswordNew Password***. Type your new password.
   - ***Confirm PasswordConfirm Password***. Retype your new password.
   - **[Save]**. Select this button to save changes in the **Change Password** pane.
4. You can define the appearance and behavior of some pages in Skylar One from the **Interface Settings** pane, which contains the following fields:
   - ***Default Page***. Select the page that automatically appears by default when you log in to Skylar One. Options include:

    - *None*. Skylar One displays the ScienceLogic logo when you log in.
    - *Event Console*. Skylar One displays the **Event Console** when you log in.
    - *Ticket Console*. Skylar One displays the **Ticket Console** when you log in.
    - *Device Views*. Skylar One displays the **Device Group Map** page (Classic Maps > Device Maps > Device Groups) when you log in.
    - *Dashboard*. Skylar One displays the selected Dashboard when you log in.
- ***Theme***. Select the backgrounds, colors, and graphics that appear when you log in. Theme entries are defined on the **Themes** page (Settings > Themes).
- ***Page Refresh Rate***. Select how often the **Events**, **Tickets**, and **Views** pages in Skylar One are refreshed. Options range from 10 seconds to 60 minutes.
- ***Page Result Count***. Select the number of results you want to display on each page that contains lists of entities. Options range from 25 to 500.
- ***Table Row Height***. Affects the row height of all pages that display a table in the main content pane. You can also change this setting in the *Event Console Preferences* page, the **Ticket Console Preferences** page, and the user **Account Preferences** page. Changing the setting for row height in the current page, the **Event Console Preferences** page, the **Ticket Console Preferences** page, or the user **Account Preferences** page affects the row height in all pages that display a table in the main content pane. Choices are:
    - *Small*. Sets row height to 17 px and font size to 11 px.
    - *Medium*. Sets row height to 27 px and font size to 12 px.
    - *Large*. Sets row height to 35 px and font size to 13 px.
- ***Default Severity Filter***. Select the minimum event severity that you want to display in the **Event Console** page. Only events of the selected severity and greater appear in the page. Options include:
    - *Healthy*. Displays all events, including events with a severity of Healthy.
    - *Notice*. Displays all events with a severity of Notice, Minor, Major, and Critical.
    - *Minor*. Displays all events with a severity of Minor, Major, and Critical.
    - *Major*. Displays all events with a severity of Major and Critical.
    - *Critical*. Displays all events with a severity of Critical.
- ***Preferred IF Label***. Select how interfaces will be labeled in all pages and reports that reference network interfaces. Options include:
    - *Interface Alias*. Easy-to-remember, human-readable name for the network interface.
    - *Interface Name*. The name of the network interface.
- ***Default Interface Graph Display***. Select the default unit of measure for the Hourly Interface Usage graph in the **Device Summary** page. Options include:

- *Interface Default*. The Hourly Interface Usage graph displays the amount of traffic in the unit of measure specified in the ***Measurement*** field in the **Interface Properties** page for the interface.
- *% Utilization*. The Hourly Interface Usage graph displays utilization in percent.

- ***Default Date Format***. Select the default date format for use throughout Skylar One.
- ***Date Format String.*** Select the date format for use throughout Skylar One. If defined, this date format overrides the default date format. You can use any date variables supported by the PHP date function in this field.

5. Use the **Checkboxes** pane to configure features that are toggled on or off:
   - ***Disable NavBar Auto-hide***. If you select this checkbox, the NavBar pane persists after you select a link. This option is selected by default.
   - ***View Assigned Tickets Only***. If you select this checkbox, by default, only tickets assigned to you are displayed in the **Ticket Console** page.
   - ***Show Masked Events***. If you select this checkbox, all events that have been grouped together with a device's ***Event Mask*** setting are displayed in the **Event Console** page. If you do not select this checkbox, these events are grouped together and rolled-up under the event with the highest severity, and you can click on the magnifying-glass icon (🔍) to view the masked events.
   - ***Organizational Grouping Events***. If you select this checkbox, events are grouped by organization. The ***filter-while-you-type*** fields and the Advanced Filter Tool appear for each organization grouping and act only on the events in that organization grouping. You cannot apply a single filter to events in multiple organizations.
   - ***Collapse Organization Events***. If you select this checkbox, all organizations with assigned events are displayed but contracted; the **Event Console** page displays only a list of contracted organizations, which you can expand by clicking the plus sign (+). The default behavior of Skylar One is to expand each organization and display the list of events for each organization.
   - ***Show Severity Badges***. If you select this checkbox:
     - The value in the ***Severity*** column is displayed as a color-coded badge on the **Event Console** page and the **Ticket Console** page.
     - The value in the ***Current State*** column is displayed as a color-coded badge on the **Device Manager** page.

     If you do not select the ***Show Severity Badges*** checkbox:
     - On the **Event Console** page, the value in the ***Event Message*** column and the value in the ***Severity*** column are painted with the severity color.
     - On the **Ticket Console** page, the value in the ***Description*** column and the ***Severity*** column are painted with the severity color.
     - On the **Device Manager** page, the value in the ***Device Name*** column and the value in the ***Current State*** column are painted with the severity color.

- *Ticket Comment Reverse Sort*. If you select this checkbox, the *Notes* section of a ticket sorts the ticket's notes from newest to oldest. If you do not select this checkbox, ticket notes display from oldest to newest.
- *Disabled Ticket Comment Cloaking*. If you select this checkbox, then any comments you add to a ticket are viewable to all other users (i.e., not cloaked) by default.
- *Scale Percent Graphs to 100%*. If you select this checkbox, then any graphs that display percentage on the y-axis display from 0% to 100%, regardless of the highest actual value. If you do not select this checkbox, then the y-axis displays from 0% to the highest actual value.
- *Code Highlighting*. If you select this checkbox, HTML, PHP, Python, and SQL code that displays in Skylar One is highlighted. You can customize the highlight colors in the **Code Highlighting** page. If selected, syntax highlighting appears in:
    - The **Snippet Editor & Registry** page for snippet Dynamic Applications (System > Manage > Applications > create/edit > Snippets)
    - The **Dashboard Widget Editor** page (System > Customize > Dashboards > Widgets > create/edit)
    - The **Database Tool** page (System > Tools > DB Tool)

      NOTE: The **Database Tool** page is available only in versions of Skylar One prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

    - The **Action Policy Editor** page for "Snippet" and "SQL Query" type actions (Registry > Run Book > Actions > create/edit)
    - The **Report Template Editor** page (Reports > Management > Report Manager > create/edit)
- *Hide Empty Networks*. If you select this checkbox, the **IPv4 Networks** page hides networks that do not include any devices or interfaces.

6. In the **Event Console Columns** pane, select the columns that you want to display by default in the **Event Console** page.

NOTE: You can also edit the list of columns to display in the **Event Console** page from the **Event Console Preferences** modal page. When you edit the list of columns in the **Event Console Preferences** modal page, the selected list of columns automatically updates in the **Account Preferences** page, and vice versa.

7. In the **Ticket Console Columns** pane, select the columns that you want to display by default in the **Ticket Console** page.

> **NOTE:** You can also edit the list of columns to display in the **Ticket Console** page from the **Ticket Console Preferences** modal page. When you edit the list of columns in the **Ticket Console Preferences** modal page, the selected list of columns automatically updates in the **Account Preferences** page, and vice versa.

8. In the **Device Manager Columns** pane, select the columns that you want to display by default in the **Device Manager** page.

> **NOTE:** You can also edit the list of columns to display in the **Device Manager** page from the **Device Manager Preferences** modal page. When you edit the list of columns in the **Device Manager Preferences** modal page, the selected list of columns automatically updates in the **Account Preferences** page, and vice versa.

9. Select the **[Save]** button to save your changes.

Event Console Preferences

On the **Event Console Preferences** page, you can customize the display and behavior of the **Event Console** page.

> **NOTE:** To access the **Event Console Preferences** page, non-administrator user accounts must be granted one or more access keys that include the following access hook: Events/Event:View. Non-administrator user accounts can then view and edit settings in the **Event Console Preferences** page. For more information on Access Keys, see the section on *Access Keys*.

To access the **Event Console Preferences** page:

1. Go to the **[Events]** tab.
2. In the **Event Console** page, click the **[Actions]** menu and select *Console Preferences*.
3. The **Event Console Preferences** page appears.
4. In the **Event Console Preferences** page, you can customize the following:
   - ***Console Refresh Rate***. Select how often the **Event Console** page is refreshed. Options range from 10 seconds to 60 minutes.
   - ***Default Severity Filter***. Select the minimum event severity that you want to display in the **Event Console** page. Only events of the selected severity and greater appear in the page. Options include:
     - *Healthy*. Displays all events, including events with a severity of Healthy.
     - *Notice*. Displays all events with a severity of Notice, Minor, Major, and Critical.

- *Minor*. Displays all events with a severity of Minor, Major, and Critical.
- *Major*. Displays all events with a severity of Major and Critical.
- *Critical*. Displays all events with a severity of Critical.

- ***Table Row Height***. Affects the row height of all pages that display a table in the main content pane. You can also change this setting in the *Event Console Preferences* page, the **Ticket Console Preferences** page, and the user **Account Preferences** page. Changing the setting for row height in the current page, the **Event Console Preferences** page, the **Ticket Console Preferences** page, or the user **Account Preferences** page affects the row height in all pages that display a table in the main content pane. Choices are:
  - *Small*. Sets row height to 17 px and font size to 11 px.
  - *Medium*. Sets row height to 27 px and font size to 12 px.
  - *Large*. Sets row height to 35 px and font size to 13 px.
- ***Group by Organization***. If you select this checkbox, events are grouped by organization. The ***filter-while-you-type*** fields and the Advanced Filter Tool appear for each organization grouping and act only on the events in that organization grouping. You cannot apply a single filter to events in multiple organizations.
- ***Show Masked Events***. If you select this checkbox, all events that have been grouped together with a device's ***Event Mask*** setting are displayed in the **Event Console** page. If you do not select this checkbox, these events are grouped together and rolled-up under the event with the highest severity, and you can click on the magnifying-glass icon (🔍) to view the masked events.
- ***Show Severity Badges***. If you select this checkbox:
  - The value in the ***Severity*** column is displayed as a color-coded badge on the **Event Console** page and the **Ticket Console** page.
  - The value in the ***Current State*** column is displayed as a color-coded badge on the **Device Manager** page.

  If you do not select the ***Show Severity Badges*** checkbox:
  - On the **Event Console** page, the value in the ***Event Message*** column and the value in the ***Severity*** column are painted with the severity color.
  - On the **Ticket Console** page, the value in the ***Description*** column and the ***Severity*** column are painted with the severity color.
  - On the **Device Manager** page, the value in the ***Device Name*** column and the value in the ***Current State*** column are painted with the severity color.
- ***Collapse All Organizations***. If you select this checkbox, all organizations with assigned events are displayed but contracted; the **Event Console** page displays only a list of contracted organizations, which you can expand by clicking the plus sign (+). The default behavior of Skylar One is to expand each organization and display the list of events for each organization.
- ***Event Console Columns***. In this list, select the columns that you want to display by default in the **Event Console** page.

NOTE: You can also edit the list of columns to display in the **Event Console** page from the **Account Preferences** page. When you edit the list of columns in the **Account Preferences** page, the selected list of columns automatically updates in the **Event Console Preferences**modal page, and vice versa.

5. Click **[Save]** to save your changes.

Hiding the Header Bar

You can also customize the display of the **Event Console** by hiding the header bar. To hide the header bar, click on the arrow in the top right of the **Event Console**.

Event Masks in the Event Console

In the **Device Properties** page for each device, you can define an **Event Mask**.

NOTE: For more information on the **Device Properties** page, see the section on *Device Administration.*

When a device uses the ***Event Mask*** setting, events that occur on a single device within a specified span of time are grouped together. This allows related events that occur in quick succession on a single device to be rolled up and posted together under one event description.

- By default, when events are masked, the **Event Console** displays all events that occur on the device within the specified timespan under a single event, the one with the highest severity. The magnifying-glass icon (🔍) appears to the left of the event. When you click on the magnifying-glass icon, the **Suppression Group** modal page appears. This page includes details about all events that are masked under the displayed event.
- If an event has ***Occurrence Count*** and ***Occurrence Time*** set in its **Event Policy Editor** page, Skylar One uses the very first logged occurrence of the event to calculate the ***Event Mask***, even if that first occurrence did not appear in the **Event Console** (due to the ***Occurrence Count*** and ***Occurrence Time*** fields).
    - For example, suppose an event, *event_x*, has an ***Occurrence Count*** of "3" and an ***Occurrence Time*** of "10 minutes." This means that the event must occur on the same device at least three times within 10 minutes before the event appears in the **Event Console**. Suppose the event, *event_x*, occurs on *device_A* at 15:51, 15:52, and 15:53. The event appears in the **Event Console** with a time stamp of "15:53," an age of "2 minutes," and a count of "3."
    - Suppose **device_A** includes an ***Event Mask*** of "Group in blocks every 5 minutes." To calculate how to group *event_x*, the ***Event Mask*** uses the time stamp of the first occurrence, 15:51, even though the event did not appear in the **Event Console** at that time. The ***Event Mask*** also uses the time of the first occurrence, 15:51, to calculate the "Age/Elapsed" value for the event in the **Suppression Group** modal page.

- If you want masked events to appear in the **Event Console** by default, go to the **Event Console Preferences** page (Events > Actions > Console Preferences), and enable the ***Show Masked Events*** field.

Chapter 3

Understanding Event Insights

Overview

This chapter describes how to view and interact with the **Event Insights** page (Events > Event Insights).

This chapter covers the following topics:

How Skylar One Provides Event Insights Data

The **Event Insights** page (Events > Event Insights) provides a global view of the alerts generated by Skylar One, the events created as the result of specific alert conditions, and the number of events that are currently active. You can use this page to track the source of your events and monitor the noise reduction that Skylar One is providing for you.

Noise reduction is the percentage of alerts that did not become events in Skylar One. A mature, tuned Skylar One system might have a high noise reduction percentage, as Skylar One is sharing only the events that matter to your environment.

Comparing alerts and events in Skylar One:

- An ***alert*** is defined by a formula that Skylar One evaluates each time data is collected. If the formula evaluates to "true" while Skylar One is collecting data on the devices in your environment, Skylar One generates an alert.

- ***Events*** are messages that are triggered when a specific condition is met. For example, an event can signal if a server has gone down, if a device is exceeding CPU or disk-space thresholds, or if communication with a device has failed. Alternately, an event can simply display the status of a managed element.
- Not every alert triggers an event. An alert must have an ***event policy*** in Skylar One that defines the conditions for the event, and when an alert meets the conditions in the event policy, Skylar One generates an event.

The **Event Insights** page lets administrator-level users see how Skylar OneSkylar One evaluates alerts ("alarms") and reduces data ***noise***. Skylar One identifies ***noise*** as any extraneous data collected by a large system that provides little insight to the administrator. The **Event Insights** page aims to sift and identify any of this extraneous data, thus resulting in a more valuable and refined event generation process. All of this fine-tuned data is viewable in the **[Overview]** tab of the **Event Insights** page.

You can edit the time range for the data displayed on this page. To apply a time range to your desired insights-data collection:

1. Click the time selector drop-down field at the top-right of the page. The time selector drawer expands.
2. You can manually enter the specific time range you want by typing in the ***From*** and ***To*** fields, or you can select one of the time ranges listed underneath the ***Absolute Time Ranges*** and ***Relative Time Ranges*** headers.
3. If your time range requires a specific time of day for collection, select the ***Specify Time*** checkbox.
4. If your time range requires collection from a specific date up until current time, select the ***Live Data*** checkbox. If working within a selected time range previous to current date, leave the checkbox unselected.
5. Click **[Apply]** to update the page to your selected time range's data.

You can also filter the page's displayed data by organizations. To apply a filter for desired organizations to your insights-data collection:

1. Click the filter icon ( ) located next to the time selector drop-down field at the top-right of the page.

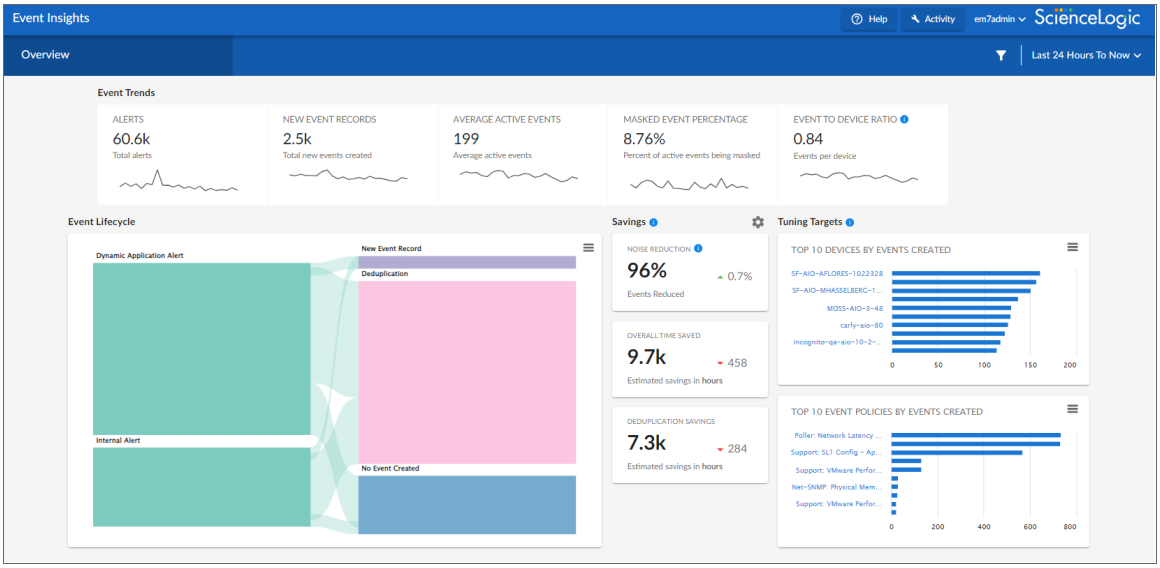
   The filter drawer expands.
2. Select your specific organization's fields to filter the page's data collection.

Elements of the Event Insights Page

The widgets displayed on the Event Insights page include:

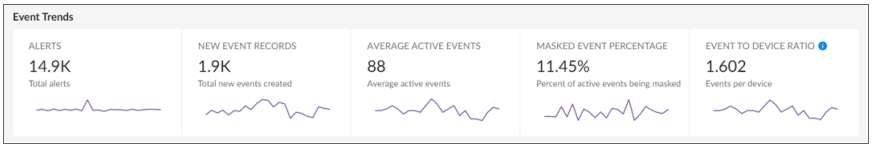
- ***Event Trends***. Displays a device's alert and event metrics in number and line-chart form.
- ***Event Lifecycle***. Provides a visual Sankey chart containing metrics for source alerts and their event life-cycle's results.
- ***Savings***. Highlights a system's "Noise Reduction" percentage, "Overall Time Saved" estimate, and "Deduplication Savings" estimate. These estimates are based on the defined-time estimate taken to triage a Skylar One event.

- ***Tuning Targets***. Displays two bar-charts: the top-10 most utilized Event Policies and top-10 noisiest devices by event volume. These two charts are based on the page's time context.



Event Trends

The ***Event Trends*** widget includes data metrics based on your organizational alignment.



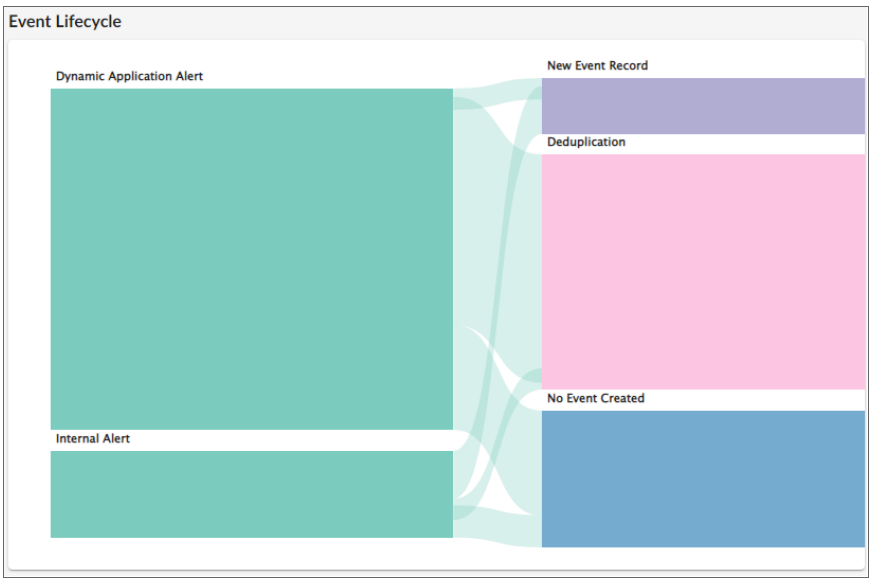
The data metrics include the following:

- ***Alerts***. Displays the total number of alerts generated from the formula in Skylar One.
- ***New Events Records***. Specifies the total number of actual new events created.
- ***Average Active Events***. Displays the average number of active events.
- ***Masked Event Percentage***. Shows the ratio of masked events to the total events created; this ratio is also displayed over a time series. The closer this value is to 1, the higher the number of masked events.
- ***Event to Device Ratio***. Displays the ratio of total events created to the number of active devices; it is also displayed over a time series. The closer this value is to 0, the fewer the events per device.

NOTE: Not every alert triggers an event, and some alerts could trigger more than one event record.

Event Lifecycle

The ***Event Lifecycle*** widget provides a visual Sankey chart for event lifecycle metrics.



The first column of this chart depicts the total number of alerts generated by your system; the blocks displayed are broken into the following source alerts:

- ***API***. Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the section on *snippet actions*. For more information on snippet Dynamic Applications, see the section on *developing snippet Dynamic Applications*. For more information on the ScienceLogic API, see the section on *generating events with the ScienceLogic API*.
- ***Dynamic Application***. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell Skylar One how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. Skylar One examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, Skylar One generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees Fahrenheit. If the chassis temperature exceeds 100 degrees at some point in the future, Skylar One inserts a message in the associated device's log files. Skylar One then matches that message with an existing event, and then triggers the event. For more information, see the section on *Dynamic Application Development*.
- ***Internal***. Internal Collections, such as Availability, Latency, Network Interface Collection, Monitors, and more. Skylar One manifests internal alerts that result in events aligned against devices.

- ***SNMP Trap***. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like managers of managers (MoMs). An SNMP trap is an unsolicited message from a device to Skylar One. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device. For more information on traps, see the section on *SNMP Traps*.
- ***Syslog***. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices such as managers of managers (MoM). A syslog is an unsolicited message from a device to Skylar One. Syslog is a standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools. For more information on syslogs, see the section on *syslog messages*.
- ***Email***. Message is generated by an email message sent to Skylar One. For more information on generating events with email messages, see the section on *events from email*.
- ***Skylar One agent***. Message is generated by log file messages collected by a Skylar One agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by an agent, see the section on *Monitoring Device Logs Using an Agent*.

The second column of this chart depicts data-blocks revealing the next step in the Event Lifecycle process:

- ***New Event Record***. Total number of actual new events created.
- ***Deduplication***. Total number of event occurrences, on the active event record, that appeared multiple times on the same device. Since Skylar One does not create new records for each occurrence (unless specified to do so), it updates the existing active event record, along with an incrementing count, to show an updated number of occurrences.
- ***No Event Created***. Total number of events that were not created from the alerts.

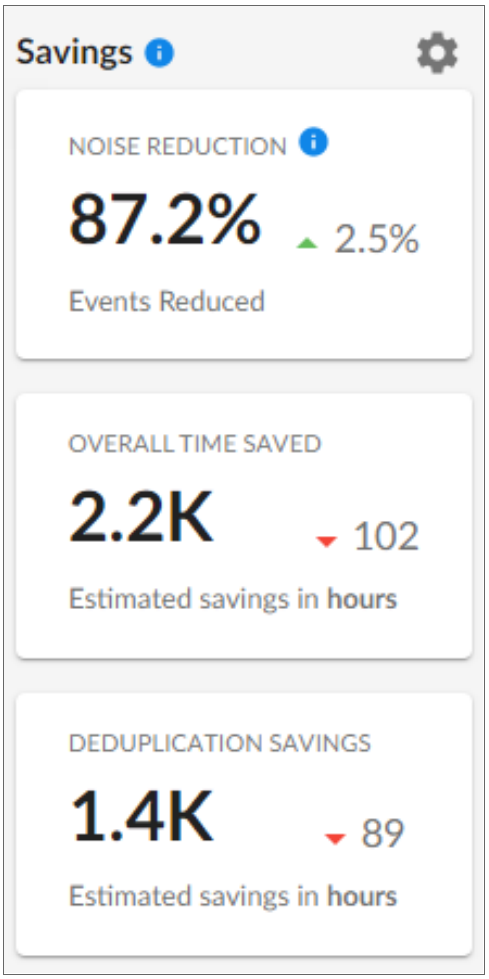
> **NOTE:** If a type of source alert does not show up in the ***Event Lifecycle*** widget, it means that specific source alert wasn't available to pull from the device.

Click the list icon (≡) to download either graph into a CSV report.

Savings

The ***Savings*** widget highlights an estimated amount of time saved in hours through Skylar One's built-in noise reduction mechanisms like deduplication. These calculations have been made using 10 minutes as the time taken to triage a single event record; they are also calculated based on the assertion that every alert resulted in a unique event record.

> **NOTE:** The ***Savings*** widget's calculations are based on a subset of events, not all events total.



These tiles include:

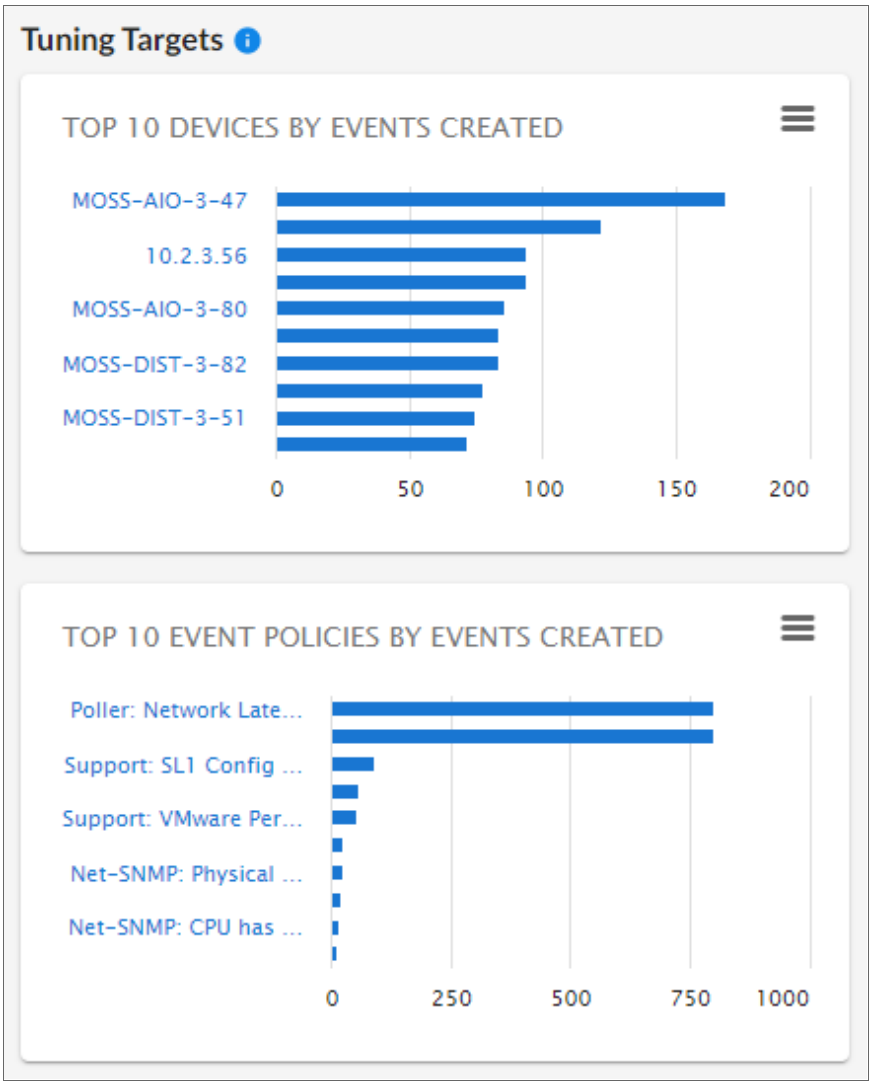
- ***Noise Reduction***. Noise Reduction is the percentage of alerts that did not become new event records. A mature, tuned system has a higher noise reduction percentage.
- ***Overall Time Saved***. Estimated time savings (in hours) from Skylar One's noise reduction mechanisms.
- ***Deduplication Savings***. Estimated deduplication savings (in hours) from Skylar One's noise reduction mechanisms.

This widget includes a modalwhere you can apply a set-time value to the ***Savings*** section's calculations. To view how to apply a set-time value, see the below section.

Tuning Targets

The ***Tuning Targets*** widget displays two graphs that depict the top-10 noisiest devices and top-10 event policies in your system. These two charts are based on the page's time context.

Click the list icon (≡) to download either graph into a CSV report.

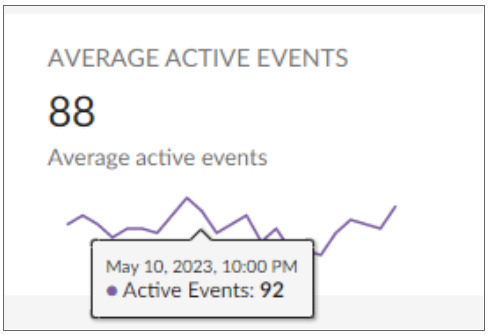


Interacting with the Event Insights Widgets

From the Event Insights page (Events > Event Insights), you can interact with the various data-metric widgets by selecting line-chart data points and hovering over Sankey chart information.

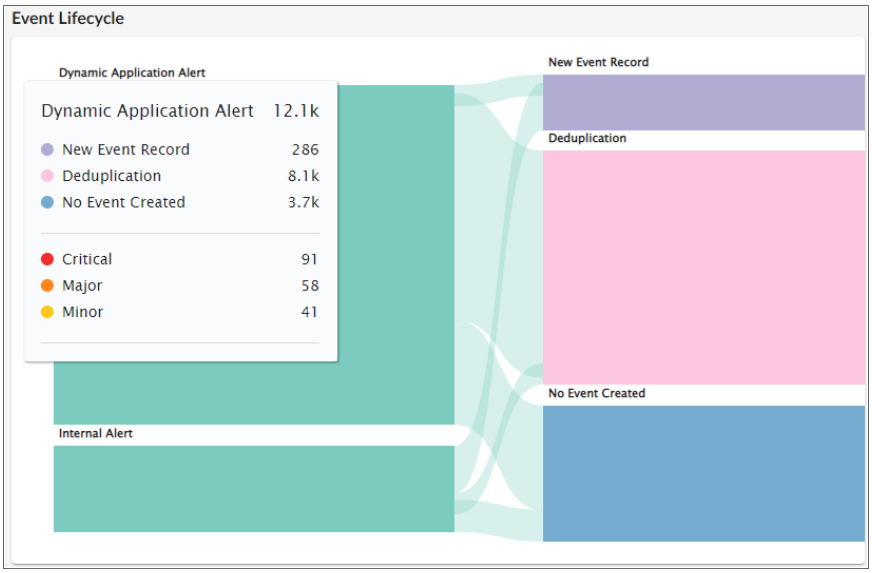
To view the ***Event Trends*** widget's line-chart data points:

1. Go to the **Event Insights** page (Events > Event Insights).
2. Select a data point along either of the line-charts associated with your desired ***Event Trends*** widget. The following data point's text-box appears and displays a specific time stamp and its number of alerts:



To view specific ***Event Lifecycle*** widget's bar-chart information:

1. Go to the **Event Insights** page (Events > Event Insights).
2. Hover your mouse over a desired Sankey chart metric in the widget.
   The following chart metric pop-up appears and displays a bar-chart text box containing relational values from alert links and reviewable severity numbers for new event-records created:



NOTE: The height of a chart's nodes reflects higher volumes of the metric. The thickness of the connectors shows you what is happening to the majority of the data, such as deduplication, event creation, and so on.

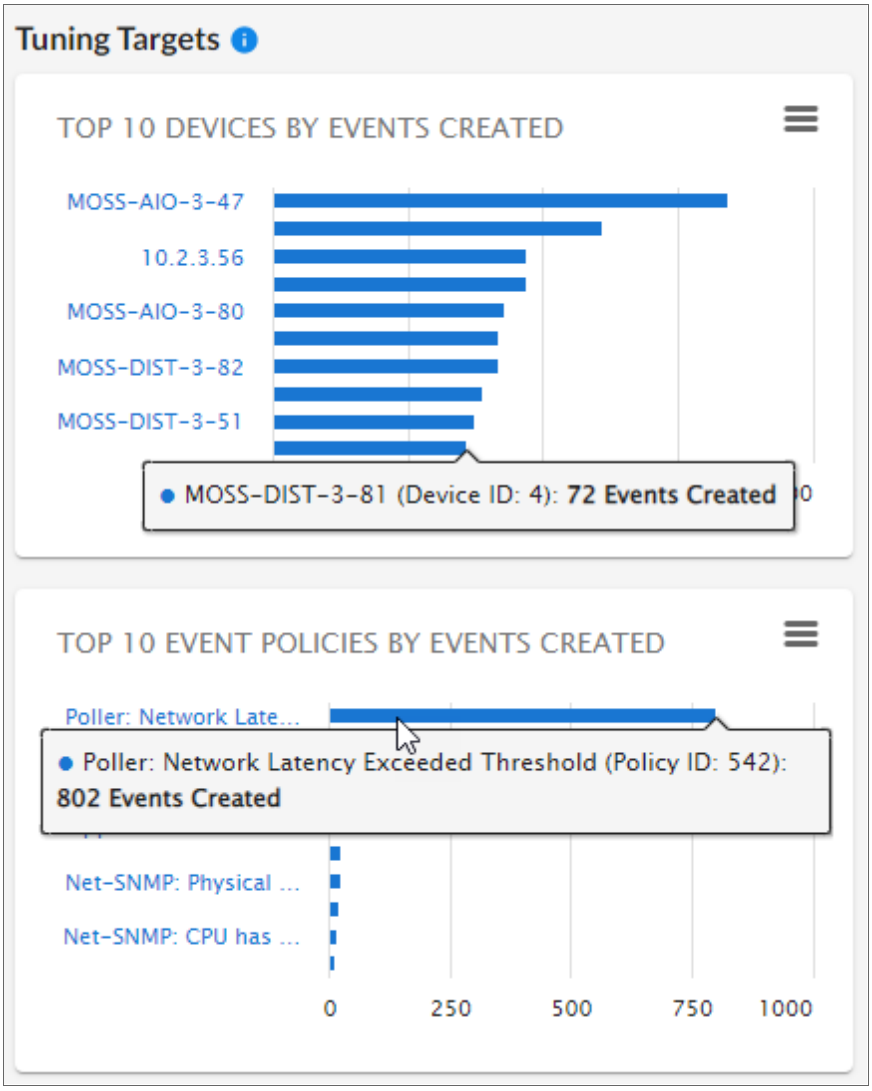
To edit ***Savings*** widget calculations and savings information:

1. Go to the **Event Insights** page (Events > Event Insights).
2. Click the **[Savings Settings]** gear icon ( ) located to the right of the widget.
   The **Savings Settings** modal appears.

3. Enter the amount of time that your organization takes to triage a single event. The default value shows 10 (in minutes).
4. Click **[Save]** to complete. You can click **[Reset To Default]** to reset the default values.

To view specific or further information within the ***Tuning Targets*** widget's charts:

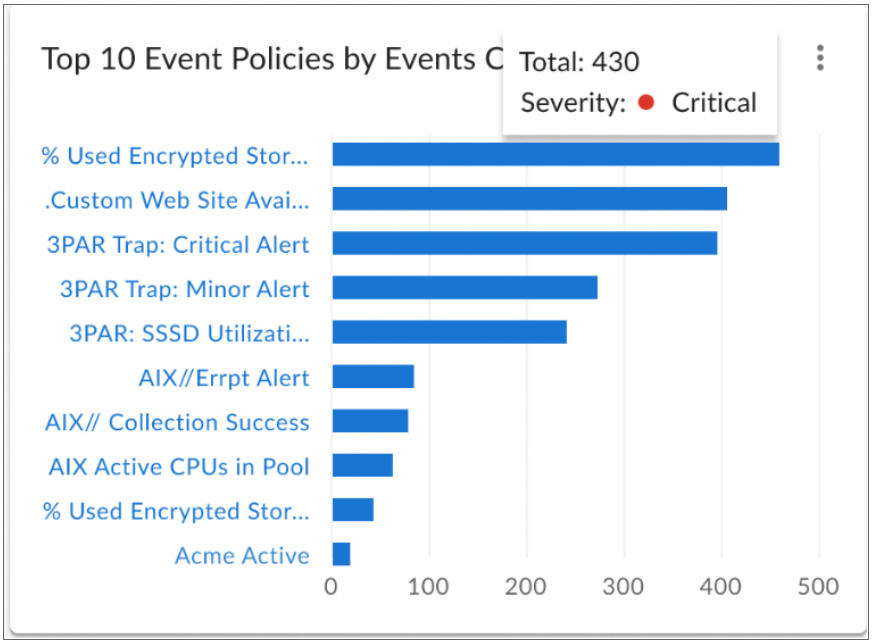
1. Go to the **Event Insights** page (Events > Event Insights).
2. Select a data point within the bar-chart(s) that is associated with your desired device and/or event policy. The following data point's text-box appears and displays a specific count for that device or event policy:

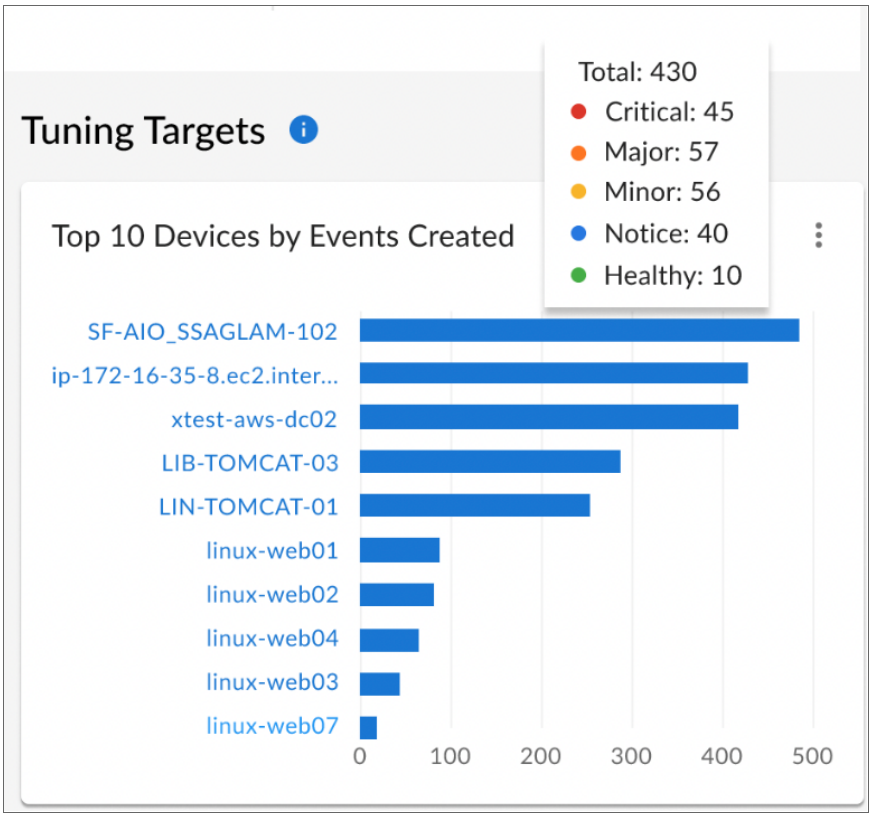


3. To view further Device or Event Policy information within the ***Tuning Targets*** widget, you can click the linked device or event policy. After your selection, Skylar One redirects you to the appropriate device or event policy page.

To access even more data that is included in the ***Tuning Targets*** widgets' bar graphs, hover your mouse over either the “Top 10 Devices by Events Created” or “Top 10 Event Policies by Events Created” bar-

graph widgets to view different points in the graph that display the count of events created for each severity, as well as the overall event total count for each device/event policy.





Chapter 4

Responding to Events

Overview

This chapter describes the different ways in which you can respond to events in Skylar One.

This chapter covers the following topics:

Responding to Events

When events occur, there are multiple ways you can respond to them:

- ***Acknowledge***. Lets other users know that you are aware of an event and are working on a response.
- ***Add a Note***. Adds additional text to an event. Notes can be displayed on the **Events** page and can be included in automation actions.
- ***Clear***. Removes an instance of an event from the **Events** page. The cleared instance is no longer displayed.
- ***Suppress***. Specifies that if the event occurs again on the same device, the event is not displayed on the **Events** page.
- ***Disable***. Specifies that if the event occurs on any device or is triggered by any application or policy, the event does not appear in the Event Console.

Selecting Multiple Events

On the **Events** page, you can use the checkboxes to the left of the event to select more than one event at a time. After you select the events, you can click the **[Acknowledge]** or **[Clear]** button at the bottom of the page to acknowledge or clear those events simultaneously.

If you do *not* want to acknowledge or clear the selected events, click the **[Deselect All]** button to deselect the checkboxes.

If you want to select *all* of the events that are currently showing on the tab, click the **[Select All Visible]** button.

Acknowledging and Clearing Events

When you ***acknowledge*** an event, you let other users know that you are aware of that event and that you are working on a response.

When you ***clear*** an event, you let other users know that this event has been addressed. Clearing an event removes a single instance of the event from the **Events** page. If the event occurs again on the same device, it reappears on the **Events** page and on the **[Events]** tab of the **Device Investigator** page, even if you previously cleared that event.

> **NOTE:** When you acknowledge a parent event, all masked events under that parent event are also acknowledged.

To acknowledge and clear events:

1. To acknowledge an event, find the event on the **Events** page and click the **[Acknowledge]** button for that event. Your user name replaces the **[Acknowledge]** button for that event.

   You can also click the **[Acknowledge]** button in a specific event's **Investigator** page.

2. To see when an event was acknowledged and who acknowledged it, hover your mouse over an acknowledged field.

3. If an event was acknowledged by another user and you have the relevant permissions, you can click the **[Reacknowledge]** button to acknowledge that event.
4. To clear an event, click the **[Clear]** button. The event is removed from the **Events** page.

> **TIP:** If you want to hide the **[Acknowledge]** or **[Clear]** buttons on the **Events** page, click the gear icon (⚙) and deselect those columns.

Viewing and Editing Event Notes

From the **Events** page, you can access ***event notes***, which contain event definitions, probable causes, and resolutions for the event, along with a text field where you can add more information about the event or the device you are monitoring. If event notes already exist for that event, the opening text of that note appears in the ***Event Note*** column of the **Events** page.

To view or edit an event note:

1. On the **Events** page, click the note icon ( ) for that event. The **Edit Event Note** modal appears.

> **TIP:** You can also edit an event note on the **Events** page by clicking the actions icon (⋮) for that event and selecting *Edit Event Note*. This is helpful if you have hidden the ***Event Note*** column on the **Events** page. To add or edit an event note for multiple events, check the box next to the events for which you want to edit the note, then click the **[Edit Note]** button at the top of the inventory table.

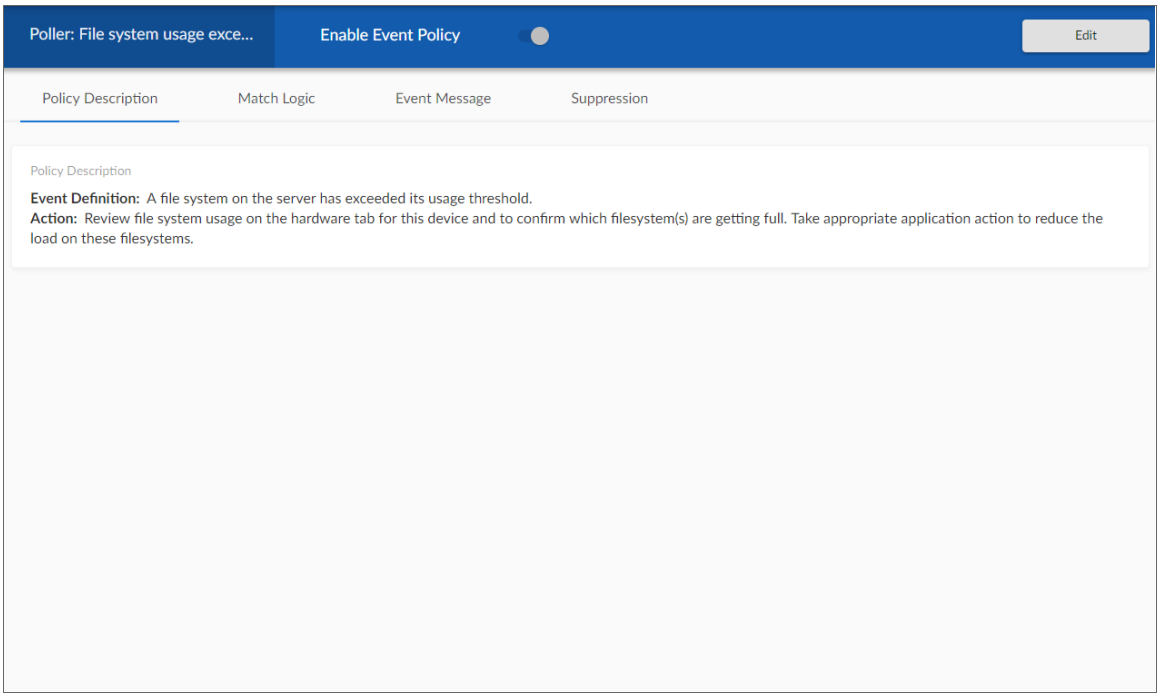
2. Type your additional text for the event note and then click **[Save]**. The event note is updated.

Viewing the Event Policy

From the **Events** page, you can view the event policy for an event, which allows you to view a description of the policy, enable or disable the policy, and edit policy details.

To view an event policy from the **Events** page:

1. On the **Events** page, click the actions icon (⋮) for that event and select *View Event Policy*. The **Event Policy Editor** page appears for that event:



2. Click the **[Edit]** button to edit the Event Policy. For more information, see *Defining and Editing Event Policies*.

Suppressing and Unsuppressing an Event for a Device

When you suppress an event, you are specifying that in the future, if this event occurs again on the same device, the event does not appear in the **Events** page or the **[Events]** tab for a device.

If a suppressed event occurs on a different device, it appears in the **Events** page and on the **[Events]** tab for that different device.

When you suppress an event, the current instance of the event still appears in the **Events**. To remove the current instance from the event console, clear the event. (For more information, see the section *Clearing One or More Events*.)

NOTE: To suppress an event, non-administrator users must be granted one or more access keys that include the following access hooks: Events/Event:View and Event:Clear. Non-administrator users can then view and suppress events that belong to the same organization(s) as the user. For more information on access hooks, see the section on *Access Permissions*.

Suppressing an Event for a Single Device

To suppress an event:

1. Go to the **Events** page.
2. Click the actions icon (⋮) for the event you want to suppress and select *Suppress Event for this Device.* In the future, if this event occurs again on the same device, the event does not appear in the **Events** page. Additionally, the suppressed event displays on the **Event Suppressions** page (Events > Event Suppressions).

> **NOTE:** Non-administrator user accounts can only view suppressed events that are aligned with the same organization(s) to which the user is aligned. Administrator users can view all suppressed events.

Suppressing an Event on Multiple Devices

When you suppress an event on multiple devices, you are specifying that, in the future, if this event occurs again on any of those devices, the event does not appear in the **Events** page or in the **Viewing Events** page for any of those devices.

To suppress an event on multiple devices:

1. Go to the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic user interface).
2. In the **Event Policies** page, click the actions icon (⋮) of the event policy you want to edit and select *Edit*.
3. The selected event policy is displayed in the **Event Policy Editor** page, where you can edit one or more properties of the event policy.
4. Click the **[Basic]** tab.
5. On the **[Basic]** tab, click the **[Configure Suppressions]** button. The **Select Suppressions** modal appears. From the **Select Suppressions** modal, you can select the devices or device groups on which to suppress the event. To do so:
    - Click **[Devices]** to select one or more devices on which to suppress the event. When you click **[Devices]**, the available devices appear below. Select the checkboxes of the devices you want to add to the suppression list.
    - Click **[Device Groups]** to select one or more device groups on which to suppress the event. When you click **[Device Groups]**, the available devices appear below. Select the checkboxes of the device groups you want to add to the suppression list.
6. Click **[Save]**.

Unsuppressing an Event for a Single Device

On the **Event Suppressions** page (Events > Event Suppressions), you can view a list of all suppressed events in Skylar One and choose to unsuppress one or more of those events. When you unsuppress an event, if this event occurs again on the same device, the event appears in the **Events** page.

> **NOTE:** To unsuppress an event, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Suppressions, and Event:Suppressions. Non-administrator user accounts can then view a list of suppressed events that belong to the same organization as the user. Non-administrator user accounts can also unsuppress one or more of these suppressed events. For more information on access hooks, see the section on *Access Permissions*.

To unsuppress an event:

1. Go to the **Event Suppressions** page (Events > Event Suppressions).
2. Select the checkbox for each event you want to unsuppress.
3. Click the **[Delete]** button that appears in the top left.

Unsuppressing All Instances of an Event

You can simultaneously unsuppress all instances of an event. That is, if a single event has been suppressed for multiple devices, you can unsuppress the event on all devices. In the future, if the unsuppressed event occurs again on any device, the event appears in the **Events** page.

> **NOTE:** To unsuppress an event on all devices, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Non-administrator user accounts can then access the **Event Policies** page and unsuppress one or more events on all devices. For more information on access hooks, see the section on *Access Permissions*.

To unsuppress an event on all devices:

1. Go to the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic user interface).
2. Select the checkbox for the event you want to unsuppress on all devices.
3. Click **[Clear Suppressions]**. In the future, if the unsuppressed event occurs again on any device, it appears in the **Events** page or in the **Viewing Events** page for the device.

Viewing Suppressed Events

From the **Event Suppressions** page (Events > Event Suppressions), you can view a list of all suppressed events in Skylar One.

The **Event Suppressions** page displays the following about each suppressed event:

- ***Device/Group Name***. The name of the device or device group associated with the suppressed event.
- ***IP Address***. The IP address of the device or device group associated with the suppressed event.
- ***Event Policy ID***. Unique numeric ID for the event policy associated with the suppressed event.
- ***Event Policy Name***. The name of the event policy associated with the suppressed event.
- ***Severity***. The severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Created Date***. Date and time when the event was suppressed.
- ***Created By***. The user ID of the user who suppressed the event.

TIP: You can sort the list by a column's values by clicking on its column heading. You can also filter the items on the page by typing or selecting filter options in one or more of the filters found above the columns. For more information, see the topic on *Filtering Inventory Pages*.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the topic on *Adjusting the Row Density*.

TIP: You can rearrange the columns in the list by clicking and dragging the column to a new location. You can adjust a column's width by clicking and dragging the right edge of the column. For more information about editing and adding columns, see the topic on *Editing the Settings for an Inventory Page*.

Enabling and Disabling Events

You can simultaneously disable one or more events on all devices. When an event is disabled, it no longer appears in the **Events** page for any devices. You can also enable an event that has been disabled.

NOTE: To disable or enable an event on all devices, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Non-administrator user accounts can then access the **Event Policies** page and enable one or more events on all devices. For more information on access hooks, see the section on *Access Permissions*.

Disabling Events

To disable one or more events:

1. Go to the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic user interface).
2. Select the checkboxes for the events you want to disable.
3. Click **[Disable]**. The selected events no longer appear in Skylar One for any device, application, or policy.

Enabling Events

To enable one or more events:

1. Go to the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic user interface).
2. Select the checkboxes for the events you want to enable.
3. Click **[Enable]**. The selected event(s) once again appear in Skylar One.

Creating a Ticket from an Event

On the **Events** page, you can create a ticket from an event by clicking the actions icon (⋮) for that event and selecting *Create Ticket*. The **Ticket Editor** appears. For more information about creating a ticket from the **Events** page, see the *Creating a Ticket from the List of Events* section.

Responding to Events in the Classic Event Console

On the **Event Console** page (Events > Classic Events, or the Events tab in the classic user interface), you can acknowledge new events as they are detected by the system. Acknowledging an event lets other users know that you are aware of the event and working to resolve it.

When an event has been acknowledged, the acknowledging user's name appears in the ***Acknowledged*** column. This lets other users know that someone is investigating or taking action on the event.

> **NOTE:** To acknowledge an event, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Events/Event:View and Event:Acknowledge. Non-administrator user accounts can then view and acknowledge events in the same organization(s) as the user. For more information on Access Keys, see the section on *Access Permissions*.

> **NOTE:** When you acknowledge a parent event, all masked events under that parent event are also acknowledged. For more information about parent/child events and masked events, see the section on *Event Correlation and Parent and Child Events*.

To acknowledge a single event:

1. Go to the **[Events]** tab in the classic user interface.
2. In the **Event Console** page, find the event you want to acknowledge and click on the checkbox in the ***Acknowledged*** column for that event.
3. A check mark and your username appear in the ***Acknowledged*** column for that event.
4. You can also acknowledge an event that has already been acknowledged by another user. To do this, click on the check mark icon. Your username now appears in the ***Acknowledged*** column for that event, replacing the username of the person who previously acknowledged the event.

To acknowledge multiple events:

1. In the **Event Console** page, select the checkbox in the far right column for each event that you want to acknowledge.
2. Acknowledge the event(s) by doing one of the following:
   - Click the **[Ack]** button.
   - From the ***Select Action*** drop-down list, select *Acknowledge*, then click the **[Go]** button.
3. For each acknowledged event, a check mark and your username appear in the ***Acknowledged*** column.

> **NOTE:** Users cannot unacknowledge an event. Another person can acknowledge the event to change the name associated with the acknowledged event, but you cannot remove an acknowledgment.

Adding a Note About an Event in the Classic Event Console

You can add brief notes to an event in the **Event Console** page. Each note appears in the ***Note*** column for an event. Skylar One does not keep a historical record of each note.

> **NOTE**: A note can be included in an action policy by using the %_user_note variable. For details on creating automation policies and action policies, see the sections on *automation policies* and *action policies*.

To create or edit a note for an event:

1. In the **Event Console** page, find the event to which you want to add a note.
2. In the ***Note*** column for that event, click on the wrench icon ( ).
3. In the **Add a Note** modal, enter the note text. Click **[Save]** to save the note.
4. The new or edited text appears in the ***Note*** column for the event.

Adding a Note to Multiple Events in the Classic Event Console

You can add a brief note to multiple events simultaneously and/or overwrite existing notes for multiple events. The note appears in the ***Note*** column for each event and in the ***Note*** field in the **Event Information** page for each event. Skylar One does not keep a historical record of each note.

> **NOTE:** A note can be included in an action policy by using the %_user_note variable. For details on creating automation policies and action policies, see the sections on *automation policies* and *action policies*.

To create or edit a note for multiple events:

1. In the **Event Console** page, find the events for which you want to add a note and/or overwrite the existing note.
2. For each event that you want to add and/or edit a note, select the checkbox in the last column.
3. In the ***Select Action*** drop-down field, select *Add/Update Event Note*, then click the **[Go]** button.
4. In the **Add a Note** modal, enter the text for the note. Click the **[Save]** button.
5. The new or edited text appears in the ***Note*** column for each selected event.

Clearing One or More Events in the Classic Event Console

When you clear an event, you remove only a single instance of the event from the current display in the **Event Console** page. If the event occurs again on the same entity, it reappears in the **Event Console** page.

> **NOTE:** To clear an event, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Events/Event:View and Event:Clear. Non-administrator user accounts can then view and clear events in the same organization(s) as the user. For more information on access hooks, see the section on *Access Permissions*.

To clear an event:

1. Go to the **[Events]** tab.
2. In the **Event Console** page, select the checkbox for each event you want to clear. To select all events in an organization, click the checkmark icon above each organization's group of events.
3. Clear the event(s) by doing one of the following:
   - Click the **[Del]** button.
   - In the ***Select Action*** drop-down list, select *Clear*, then click the **[Go]** button.
4. When you successfully clear an event, it no longer appears in the **Event Console** page.

NOTE: The ***Event Clearing Mode*** option in the **Behavior Settings** page (System > Settings > Behavior) affects how rolled-up events and suppressed events can be cleared. For details, see the section on *System Settings that Affect Events*.

Suppressing an Event on a Single Device in the Classic User Interface

When you suppress an event in the classic Skylar One user interface, you are specifying that in the future, if this event occurs again on the same device, the event does not appear in the **Event Console** page or the **Viewing Events** page for a device.

If a suppressed event occurs on a different device, it appears in the **Event Console** page and on the **Viewing Events** page for that different device.

When you suppress an event, the current instance of the event still appears in the **Event Console**. To remove the current instance from the event console, clear the event (see the section *Clearing One or More Events*).

NOTE: To suppress an event, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Events/Event:View and Event:Clear. Non-administrator user accounts can then view and suppress events that belong to the same organization(s) as the user. For more information on access hooks, see the section on *Access Permissions*.

To suppress an event in the classic Skylar One user interface:

1. Go to the **[Events]** tab.
2. In the **Event Console**, click the information icon (ℹ) for the event you want to suppress.
3. In the **Event Information** page, click the **[Actions]** menu and select *Suppress Event for this Device*.
4. In the future, if this event occurs again on the same device, the event does not appear in the **Event Console** page.

NOTE: Non-administrator user accounts can view only suppressed events that are aligned with the same organization(s) to which the user is aligned. Administrator users can view all suppressed events.

Suppressing an Event On Multiple Devices in the Classic User Interface

When you suppress an event on multiple devices, you are specifying that, in the future, if this event occurs again on any of those devices, the event does not appear in the **Event Console** page or in the **Viewing Events** page for any of those devices.

To suppress an event on multiple devices in the classic Skylar One user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, select the page icon ( ) of the event you want to suppress.
3. The **Event Policy Editor** page appears, with the **[Suppressions]** tab selected.
4. In the **Suppressions** tab, you can select the devices or device groups on which to suppress the event. To do so:
   - Select one or more device groups in the ***Available Device Groups*** field and then click the right arrow button (**[>>]**) so those groups appear in the ***Suppressed Device Groups*** field.
   - Select one or more devices in the ***Available Devices*** field and then click the right arrow button (**[>>]**) so those devices appear in the ***Suppressed Devices*** field.
5. Click **[Save]**. In the future, if the event occurs on one of the selected devices, the event does not appear in the **Event Console** page or in the **Viewing Events** page for the device. The suppressed event appears in the **Event Suppression List** page (Registry > Events > Suppressions).

Unsuppressing an Event in the Classic User Interface

You can view a list of all suppressed events in Skylar One and choose to unsuppress one or more of those events. When you unsuppress an event, if this event occurs again on the same device, the event appears in the **Events** page (or the **Event Console** page in the classic Skylar One user interface) .

> **NOTE:** To unsuppress an event, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Suppressions, and Event:Suppressions. Non-administrator user accounts can then view a list of suppressed events that belong to the same organization as the user. Non-administrator user accounts can also unsuppress one or more of these suppressed events. For more information on access hooks, see the section on *Access Permissions*.

To unsuppress an event:

1. Go to the **Event Suppression List** page (Registry > Events > Suppressions).
2. In the **Event Suppression List** page, select the checkbox for each event you want to unsuppress.
3. In the ***Select Action*** drop-down menu, in the lower right, select *DELETE Suppression*.
4. Click the **[Go]** button.

5. In the future, if the unsuppressed event occurs again on the same device, the event appears in the **Events** page (or the **Event Console** page in the classic Skylar One user interface) .

Unsuppressing All Instances of an Event in the Classic User Interface

You can simultaneously unsuppress all instances of an event. That is, if a single event has been suppressed for multiple devices, you can unsuppress the event on all devices. In the future, if the unsuppressed event occurs again on any device, the event appears in the **Event Console** page.

> **NOTE:** To unsuppress an event on all devices, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Non-administrator user accounts can then access the **Event Policy Manager** page and unsuppress one or more events on all devices. For more information on access hooks, see the section on *Access Permissions*.

To unsuppress an event on all devices in the classic Skylar One user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, select the checkbox for the event you want to unsuppress on all devices.
3. In the ***Select Action*** drop-down menu, select *CLEAR the Suppression List*.
4. Click the **[Go]** button. In the future, if the unsuppressed event occurs again on any device, it appears in the **Event Console** page or in the **Viewing Events** page for the device.

Disabling an Event in the Classic User Interface

You can simultaneously disable one or more events on all devices. When an event is disabled, it no longer appears in the **Event Console** for any devices.

> **NOTE:** To disable an event on all devices, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Non-administrator user accounts can then access the **Event Policy Manager** page and disable one or more events on all devices. For more information on access hooks, see the section on *Access Permissions*.

To disable one or more events in the classic Skylar One user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, select the checkbox for each event you want to disable.
3. In the ***Select Actions*** drop-down list, select *DISABLE these Event Policies*.
4. Click the **[Go]** button. The selected event(s) no longer appear in Skylar One for any device, application, or policy.

Enabling an Event in the Classic User Interface

You can simultaneously disable one or more events on all devices. When an event is disabled, it no longer appears in the **Event Console** for any devices. You can also enable an event that has been disabled.

> **NOTE:** To enable an event on all devices, non-administrator user accounts must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Non-administrator user accounts can then access the **Event Policy Manager** page and enable one or more events on all devices. For more information on access hooks, see the section on *Access Permissions*.

To enable one or more events in the classic Skylar One user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, select the checkbox for each event you want to enable.
3. In the ***Select Actions*** drop-down list, select *ENABLE these Event Policies*.
4. Click the **[Go]** button. The selected event(s) once again appear in Skylar One.

Chapter 5

Events and Tickets

Overview

This chapter describes how to create tickets from events in Skylar One.

This chapter covers the following topics:

Creating a Ticket from the List of Events

A ***ticket*** is a request for work that can be tracked in Skylar One. This request can be in response to a problem that needs to be fixed, for routine maintenance, or for any type of work required by your enterprise. A ticket can be created manually or created based on an event. For example, if an event occurs that says that a device is using 99 percent of disk space, you might want to create a ticket that tasks a co-worker with adding additional disk space to the device.

If a ticket is created from the **Events** page (or the **Event Console** page in the classic Skylar One user interface), based on a selected event, most of the ticket fields are populated automatically by Skylar One.

NOTE: To create a ticket from an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Events/Event:View, Ticketing/Ticket:View, and Ticket:Create. Accounts of type "user" can then create and save tickets from the **Events** page (or the **Event Console** page in the classic Skylar One user interface). For more information on access keys, see the manual ***Access Permissions***.

NOTE: Depending on the ***Event Console Ticket Life Ring Button Behavior*** setting in the **Behavior Settings** page (System > Settings > Behavior), clicking the life-ring icon ( ) in the **Event Console** either creates a ScienceLogic ticket or an external ticket. When viewing an event in the **Events** page (or the **Event Console** page in the classic Skylar One user interface), you can create a ticket based on the selected event. Some of the ticket fields are populated automatically with values from the event. To create a ticket based on an event:

1. On the **Events** page or the **Event Investigator** page for a specific event, click the actions icon ( ) for the event and select *Create Ticket*. (Or, if you are using the classic Skylar One user interface, on the **Event Console** page, click on the life-ring icon ( ) of the event for which you want to create a ticket.) The **Ticket Editor** page appears.
2. Depending on the ***Event Console Ticket life-ring Button Behavior*** setting in the **Behavior Settings** page (System > Settings > Behavior), Skylar One creates a Skylar One ticket or an external ticket. For more information, see the *Event Ticket Behavior Settings* section.
3. Most of the fields are already populated with values from the event. You can accept these values or edit them. The following fields display:
    - ***Description***. A brief description of the problem or ticket. If you create a ticket from an event on the **Events** page (or the **Event Console** page in the classic Skylar One user interface), this field is populated automatically by Skylar One.
    - ***Organization***. Select the organization to associate with the ticket in the drop-down menu. If you create a ticket from an event on the **Events** page (or the **Event Console** page in the classic Skylar One user interface), this field is populated automatically by Skylar One.
    - ***Element***. By default, this field includes the element associated with the event. Can be an organization, device, device group, asset record, IP network, interface, vendor, or user account. To change the element or find another element, click the magnifying glass icon ( ). The **Finder** page appears, where you can search for another element.
    - ***Aligned Event***. If applicable, the event that is associated with the ticket. Clicking on the icon displays read-only details about the event.
    - ***Ticket Description***. Description of the problem or ticket. By default, this field includes the Event Message from the event. You can edit this field to suit your business requirements.
    - ***Alternate Location***. This field appears only if the selected organization has one or more alternate locations. If the selected organization has one or more alternate locations, you can select one of those locations in this field.

- ***Ticket State***. Custom parameter, defined in the **Ticket States** page (Registry > Ticketing > Custom States). Allows you to add additional workflow restrictions to a ticket. For more information, see the chapter on "Custom Ticket States" in the ***Ticketing*** manual.
- ***Status***. Status of the ticket. The choices are:
    - *Open*. Ticket has been created.
    - *Pending*. Ticket has been acknowledged.
    - *Working*. Someone is working on the ticket.
    - *Resolved*. Issue has been resolved.
- ***Severity***. The severity of the problem. When a ticket is created from an event in the **Events** page (or the **Event Console** page in the classic Skylar One user interface), this field is populated automatically by Skylar One with the event's severity. For more information about severity values, see the section *Understanding Event Severity*.
- ***Category***. Descriptive category assigned to the ticket. You can use the **Select Objects Editor** page (System > Customize > Select Objects) to customize the list of possible categories.
- ***Source***. Original source for the ticket. You can use the **Select Objects Editor** page (System > Customize > Selected Objects) to customize the list of possible sources. The default choices are:
    - *Automated*. Ticket was created automatically when an event occurred. An administrator has configured Skylar One to behave this way.
    - *Email*. An email about an issue prompted this ticket.
    - *External*. An external source created this ticket.
    - *Internal*. This ticket was created in Skylar One.
    - *Phone*. A phone call about an issue prompted this ticket.
- ***Queue***. Ticket Queue to which the ticket is assigned. When you select a ***Ticket Queue***, Skylar One populates the ***Assigned User*** field with a list of members from the specified queue.
- ***Assigned User***. User who is responsible for resolving the ticket. This drop-down list contains entries for each user who is assigned to the specified Ticket Queue and who has a Login State of *Active*. When a ticket is assigned to a user, Skylar One automatically sends the user an email message as notification.
- ***Custom Fields***. If your Skylar One system includes embedded custom fields for tickets, you can supply a value in those fields. For more information on custom fields, see the chapter on *Form Fields* in the manual ***Customizing User Experience***.

4. To add a note to the ticket, click the **[New Note]** button. A new instance of the **Notepad Editor** appears in the **Notes & Attachments** pane. In the **Notepad Editor**, you can format the text and include links and images in a note.
5. Click **[Save]** to save the ticket.

For more information on creating tickets, see the chapter on *Creating and Editing Tickets* in the ***Ticketing*** manual.

Event Ticket Behavior Settings

The behavior of the *Create Ticket* option on the **Events** page (or the life-ring icon ( ) in the **Event Console** page in the classic Skylar One user interface) is determined on the **Behavior Settings** page (System > Settings > Behavior) in the classic Skylar One user interface. To change this behavior:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Select from the following options in the ***Event Console Ticket Life Ring Button Behavior*** field:
   - *Create/View EM7 Ticket*. When you select the *Create Ticket* option or click the life-ring icon ( ) for an event, Skylar One displays the **Ticket Editor** page, where you can define a Skylar One ticket and automatically associate it with the selected event. This is the default behavior.
   - *Create/View External Ticket*. If an external ticket is aligned with an event, when you select the *Create Ticket* option or click the life-ring icon ( ) for that event, Skylar One spawns a new window and displays the external ticket (as specified in the `force_ticket_uri` database field). If an external ticket is not yet aligned with an event, when you select the *Create Ticket* option or click the life-ring icon ( ) for that event, Skylar One sets a "request" flag for the ticket and displays an acknowledgment that a new ticket has been requested. You can then use the "request" in run book logic to create the ticket on the external system.
3. Click **[Save]** to save your changes.

NOTE: For more information on events and external tickets, see *integrating events and external tickets*.

Integrating Events with External Tickets

The ***External Ticket*** column on the **Events** page (or on the **Event Console** page of the classic user interface) lets you integrate events with an external ticketing system.

- If an external ticket is aligned with an event, then when you select the *Create Ticket* option (or click the life-ring icon ( )) for that event, Skylar One spawns a new window and displays the external ticket (as specified in the *force_ticket_uri* field).
- If an external ticket is not yet aligned with an event, when you select the *Create Ticket* option (or click the life-ring icon ( )) for that event, Skylar One sets a "request" flag for the ticket and displays an acknowledgment that a new ticket has been requested. You can then use the "request" in run book logic to create the ticket on the external system.

External Tickets on the Events Page or Event Console

The following two fields in the `master_events.events_active` database table in Skylar One populate the values for external tickets on the **Events** page (or the **Event Console** page in the classic Skylar One user interface):

- ***force_ticket_uri***. This field contains the URI that leads to the external ticket. Selecting the *Create Ticket* option on the **Events** page or clicking on the life-ring icon ( ) for an external ticket in the **Event Console** page opens a new window with the specified URI loaded.
- ***ext_ticket_ref***. Name or ID number associated with the external ticket. This value is displayed in the ***External Ticket*** column on the **Events** page (or the **Event Console** page of the classic user interface).

NOTE: Additional database fields (`force_ticket_uri_2`, `force_ticket_uri_3`, `ext_ticket_ref_2`, and `ext_ticket_ref_3`) populate values for up to three external tickets.

The value stored in the `ext_ticket_ref` field for an event (i.e., the ticket number for that event on the external ticketing system) is displayed in the ***External Ticket*** column on the **Events** page (or the **Event Console** page of the classic user interface) for that event.

For example, suppose the events in an off-site Skylar One system are being integrated with the ScienceLogic Customer Care ticketing system, em7.sciencelogic.com. On the off-site system, for each event that has an open ticket, the `force_ticket_uri` and `ext_ticket_ref` values would be set to those of a ticket on the em7.sciencelogic.com system.

Suppose we want to test using a single ticket. Suppose this ticket has the ***TID 10000*** on the system ***em7.sciencelogic.com***.

In the off-site Skylar One system, we would define the following:

- ***force_ticket_uri***. The URI that leads to the ticket in the off-site system. Selecting the *Create Ticket* option on the **Events** page (or clicking on the life-ring icon ( ) for an external ticket in the **Event Console** page of the classic user interface) opens a new window with the URI loaded.

  ```
  http://em7.sciencelogic.com/em7/index.em7?exec=ticket_management#tickets_search.tid=10000
  ```

- ***ext_ticket_ref***. Name or ID number that is displayed in the ***External Ticket*** column on the **Events** page (or the **Event Console** page of the classic user interface) in the off-site system. We would enter:

  ```
  10000
  ```

Using Run Book Automation to Populate the ScienceLogic Database with Values from External Tickets

To integrate events with an external ticketing system, you must create run book automation actions that perform requests to the external ticketing system and populate the `force_ticket_uri` and `ext_ticket_ref` fields in the `master_events.events_active` table.

NOTE: Additional database fields (`force_ticket_uri_2`, `force_ticket_uri_3`, `ext_ticket_ref_2`, and `ext_ticket_ref_3`) populate values for up to three external tickets.

The following run book automation policies and actions could be used to integrate events with an external ticketing system:

- An automation policy that runs when events are created. Depending on your business needs, this automation policy might run when an event is acknowledged or when a user selects the *Create Ticket* option on the **Events** page (or the life-ring icon ( ) in the **Event Console** in the classic Skylar One user interface). This automation policy would execute the following actions:
    - One or more snippet actions that create a ticket in the external ticketing system. The ticket can be created using one or more of the available variables; for example, %M contains the message text for the event that triggered the automation policy. One of the snippet actions could pass the ticket ID for the ticket to Skylar One.
    - An SQL query action that updates the `ext_ticket_ref` and `force_ticket_uri` fields for the event. The value of `ext_ticket_ref` should be set to the value passed by the previous snippet action (accessed using the %_EM7_RESULT_% variable). The SQL query should use the %e variable (the event ID for the event that triggered the automation policy) to ensure that the query updates the correct event.
- An automation policy that runs when events are cleared. This automation policy would execute a snippet action that:
    - Performs an SQL query to retrieve the `ext_ticket_ref` value for the event that triggered the automation policy.
    - Resolves the appropriate ticket in the external ticketing system.

For details on creating run book automation policies, see the manual ***Run Book Automation***.

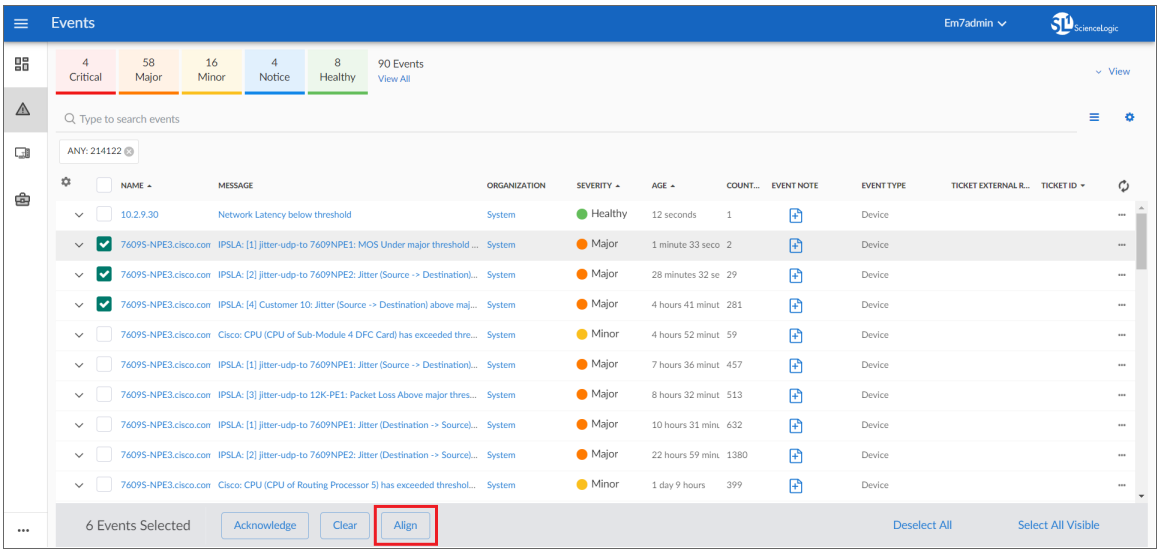
Aligning an External Ticket with Multiple Events

Initially, to link an external ticket to a ScienceLogic event, you must create a custom run book automation policy and a custom run book action or use the ScienceLogic APIs. For more information, see the *section on Integrating Events with External Tickets*. For help with these tasks, contact ScienceLogic Customer Care.

After linking an external ticket to a ScienceLogic event, you can copy that link to other related events. This section describes how to copy the link to an external ticket to multiple, related events.

To copy the link to an external ticket to multiple, related events:

1. Go to the **Events** page.
2. Select the checkboxes of the events to which you want to copy the link to an external ticket and then click **[Align]**:



3. The **Align External Tickets** modal appears. This page displays a list of external tickets that are currently aligned with active events. Select the external ticket that you want to align with the selected events. Click **[Align]**.
4. The selected events now display the external ticket ID in the ***External Ticket*** column.

Aligning an External Ticket with Multiple Events in the Classic User Interface

To copy the link to an external ticket to multiple, related events in the classic Skylar One user interface:

1. In the **Event Console** page, select the checkbox for each event that you want to align with a single external ticket.
2. In the ***Select Action*** drop-down list, select *Set External Ticket* and then click the **[Go]** button.
3. The **Set External Ticket** modal appears. This page displays a list of external tickets that are currently aligned with active events. Select the external ticket that you want to align with the selected events. Click **[Save]**.
4. The selected events now display the external ticket ID in the ***External Ticket*** column.

Chapter 6

Event Correlation and Parent and Child Events

Overview

This chapter describes ***Topology Events***, which are also called ***Event Correlation***.

This chapter covers the following topics:

Event Correlation

In Skylar One, there are four types of events that might not appear on the **Events** page (or the **Event Console** page in the classic Skylar One user interface):

- ***Rolled-up events***. Multiple occurrences of the same event on the same device. When the same event occurs multiple times on a single device, Skylar One does not display each occurrence on the **Events** page. Instead, Skylar One displays a single entry and notes the number of occurrences in the ***Count*** column.
- ***Suppressed Events***. Suppressed events do not appear on the **Events** page. For details on suppressing events for a single device, see the section on *Suppressing Events*.

- ***Topology Events***. In Skylar One, event correlation or topology suppression means the ability to build parent-child relationships between devices and between events. When events are correlated, only the parent event is displayed on the **Events** page. The magnifying-glass icon (🔍) appears to the left of the parent event. When you click on the magnifying-glass icon, the list of child events is displayed. The child events are rolled up under the parent event and are not displayed on the **Events** page. For the parent event, the count column increases to indicate the number of correlated child events. Optionally, you can define event categories that allow Skylar One to more efficiently align suppressing events with suppressible events. When you align an event category to a suppressing or suppressible event, that event is correlated with only events that are aligned with the same event category.
- ***Event Masks***. When a device uses the Event Mask setting, events that occur on a single device within a specified span of time are grouped together. On the **Events** page, masked events are displayed under a single event, the one with the highest severity. For details on event masks, see the section on *Event Masks*.

Skylar One performs two types of event correlation:

- ***Automatic Event Correlation***. During discovery, Skylar One automatically discovers and defines parent-child relationships between devices based on Layer-2, Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Layer-3, and legacy VMware topology or data collected from Dynamic Applications.
- ***Manual Event Correlation***. In Skylar One, you can configure devices and events so that events that are associated with child devices are rolled up under the parent device's events on the **Events** page (or the **Event Console** page in the classic Skylar One user interface). For example, suppose a switch fails. Instead of seeing an event for the failed switch and seeing events about failed communication for each device connected to the switch, only a single event would appear on the **Events** page (or the **Event Console** page in the classic Skylar One user interface). The single event would describe the switch failure. When you manually define a hierarchy between events, you can also include an event category. An event category allows Skylar One to more efficiently align suppressing events with suppressible events.

To manually define event correlation, you must perform two tasks:

- Define parent and child devices.
- Define a hierarchy between events–that is, define parent events (called suppressing events) and child events (called suppressible events).

IMPORTANT: Enabling a discovered device configured with CDP or LLDP topology in Skylar One causes the device to provide information on its neighbor. This information only identifies that there is a neighbor device, not which is the parent or the child. This might cause the parent-child relationship to switch, which requires you to manually reverse the issue within the Skylar One user interface. In Skylar One, you can manually build parent-child relationships between specific device categories. For more information, see *Defining Parent and Child Devices*.

Event Correlation Precedence

In some instances you might have multiple parent-child links between two devices. Skylar One displays only one of the relationships. Skylar One gives precedence to showing these relationships in the following order:

- Manually defined event correlation links
- Layer-3 links
- Link Layer Discovery Protocol (LLDP) links
- Cisco Discovery Protocol (CDP) links
- Layer-2 links
- Legacy VMware links
- Component relationship links

Additionally, any manually created, edited, or deleted links take precedence over the information discovered by Skylar One. The changes are propagated to discovery and event correlation.

Defining Parent and Child Devices

In Skylar One, you can create parent-and-child relationships and define event correlations. Skylar One creates parent and child devices automatically when:

- Skylar One discovers Layer-2, Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Layer-3, and legacy VMware topology.
- Skylar One performs collection for Dynamic Applications that create component devices or device relationships.

You can also manually define parent and child relationships between devices.

On the **Device Children** modal, you can select one or more devices to become children of the currently selected device.

To add children to a device:

1. Go to the **Device Manager** page (Devices > Classic Devices).
2. In the **Device Manager** page, select the wrench icon ( ) for the device for which you want to add child devices. The **Device Properties** page appears.

> **NOTE:** You cannot create parent-child relationships for devices with a device category of *Virtual*.

3. In the **Device Properties** page, in the **[Actions]** drop-down list, select *Device Children*. The **Device Children** modal appears.

4. In the **Device Children** modal, select one or more devices to be children of the current device.
5. Click **[Save]**.

Device Categories That Do Not Support Child Devices

A device category is a logical categorization of a device by primary function. Skylar One uses device categories to group related devices in reports and views.

Device categories are paired with device classes to organize and describe discovered devices. The device class usually describes the manufacturer and model of a device. The device category describes the function of the hardware.

Devices that are members of the following device categories cannot be assigned child devices:

- Office Printers, Device Category #4
- Workstations, Device Category #6
- Environmental.Utility, Device Category #8
- Environmental.HVAC, Device Category #9
- Environmental.Security, Device Category #10
- System.Tape, Device Category #17
- Office.Copiers, Device Category #22
- Office.Facsimiles, Device Category #23
- Telephony.Phone, Device Category #36
- Office.Plotter, Device Category #40
- Pingable, Device Category #98
- Virtual, Device Category #97

To determine a device's device category, look at the ***Category*** field on the ***Info*** drawer of the **Device Investigator** page.

Defining Event Topology Masking and Suppression

Topology masking, also referred to as ***topology suppression***, is a setting that defines the rules that Skylar One uses to determine event correlation and suppression when events occur on devices that have a parent/child relationship.

In Skylar One, you can create parent-and-child relationships and define event correlations. Skylar One creates parent and child devices automatically when:

- Skylar One discovers Layer-2, Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Layer-3, ARP, and legacy VMware topology.
- Skylar One performs collection for Dynamic Applications that create component devices or device relationships.

You can also manually *define parent and child relationships* between devices.

For event correlation to occur, two types of event policies must be defined: masking events and maskable events.

- ***Masking events***. If this type of event occurs on a parent device, Skylar One searches all related child devices for ***maskable*** events. On the child devices, all maskable events are masked. Only the masking event appears on the **Events** page; the maskable events are nested under the parent event.
- ***Maskable events***. This type of event is masked on a child device *only* when a masking event occurs on the parent device.

The following options are available:

- *Disabled*: Events from this policy do not mask, or get masked, by topology.
- *Mask events on child devices*: If an event occurs from this policy on a parent device, Skylar One searches for all related child devices for maskable events. If a Category has been aligned to this policy, Skylar One refines the search to all child devices and masks all events that have been defined as maskable and assigned the same Category. If you have not assigned a Category to this policy, Skylar One refines the search to all child devices and masks all events that have been defined as maskable and are not assigned a Category.
- *Maskable under a parent device's event*: If an event occurs from this policy on a child device, Skylar One masks this event by topology only when a masking event occurs on the parent device. If a Category has been aligned to this policy, Skylar One masks this event when it occurs on a child device and an event that has been defined as masking occurs on its parent device. The masking event must have the same Category as the maskable event. If a Category has not been aligned to this policy, when a masking event that is not assigned to a Category occurs on the parent device Skylar One searches all child devices and masks all events that have been defined as maskable and are not assigned to a Category.
- *Both*: If an event occurs from this policy on a parent device, it behaves as a masking event. If this event occurs on a child device, it behaves as a maskable event.

For more information about how to define an event as masking or maskable, see the section on *The Event Message Tab*.

Defining Event Topology Suppression in the Classic Skylar One User Interface

To manually configure event correlation in the classic Skylar One user interface, you must define two types of events:

- ***Suppressing events***. If this event occurs on a parent device, Skylar One searches all related child devices for ***suppressible*** events. On the child devices, all suppressible events are suppressed. Only the suppressing event appears in the **Events** page (or the **Event Console** page in the classic Skylar One user interface). The suppressible events do not appear in the **Events** page (or the **Event Console** page in the classic Skylar One user interface).
- ***Suppressible events***. This type of event is suppressed on a child device only when a suppressing event occurs on the parent device.

NOTE: If you configure event categories, the suppressing and suppressible events must be associated with the same category for correlation to occur. If you do not configure event categories, each and every suppressing event that occurs on a parent device causes Skylar One to suppress **all suppressible** events on the associated child devices.

To define an event as a suppressing event on the **Event Policy Manager** page in the classic Skylar One user interface):

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager.
2. On the **Event Policy Manager** page, click the wrench icon (🔧) of the event that you want to define as the ***suppressing*** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]** tab.
4. In the ***Topology Suppression*** field, select *Suppressing*.
5. Click **[Save]**. In the future, when this event occurs on a device, Skylar One checks if the device is a parent device. If the device is a parent device, specified events (suppressible events) with the same category are suppressed on the child devices.

To define an event as a suppressible event on the **Event Policy Manager** page in the classic Skylar One user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. On the **Event Policy Manager** page, click the wrench icon (🔧) of the event that you want to define as the ***Suppressible*** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]** tab.
4. In the ***Topology Suppression*** field, select *Suppressible*.
5. Click **[Save]**. In the future, when this event occurs on a device, Skylar One checks if the device is a child device. If the device is a child device, Skylar One checks to see if a suppressing event with the same category has occurred on the parent device. If a suppressing event has occurred on the parent device, the specified event is suppressed on the child device.

Example: Child Event Suppression

For example, suppose you have the following devices and event policies defined:

- A parent device, a Cisco Catalyst switch named *Boise-DMZ*.
- A child device to *Boise-DMZ*, a server named *HQ-W2K3-VC01*.
- An event policy, "Poller: Interface operationally down", defined as a suppressing event.
- A second event policy, "Poller: Device not responding", defined as a suppressible event.
- Both events are associated with the same event category.

In this scenario, if an interface goes down on the switch *Boise-DMZ*, Skylar One cannot communicate with the server, *HQ-W2K3-VC01*, attached to the switch.

With the above defined event topology suppression:

- The event "Poller: Interface operationally down" occurs on *Boise-DMZ*.
- The event "Poller: Device not responding" is suppressed on the server *HQ-W2K3-VC01*.
- On the **Events** page (or the **Event Console** page in the classic Skylar One user interface), the only event that appears in this scenario is the event "Poller: Interface operationally down" on the device *Boise-DMZ*.

Event Categories

Event categories allow Skylar One to match masking events with the right maskable events. When you assign a category to a masking or maskable event, that event only correlates with events that share the same category. An event can belong to multiple categories, but for correlation to occur, the masking and maskable events must share at least one category in common.

> **NOTE:** This section uses the terms "masking" and "maskable," but these are interchangeable with "suppressing" and "suppressible" from the classic Skylar One interface.

Without event categories, any masking event on a parent device causes Skylar One to mask every maskable event across all child devices, regardless of whether those events are related. For example, a collection failure on a chassis could end up masking an unrelated temperature warning on a blade.

With event categories, Skylar One only correlates events that share the same category. Using the same example, a collection-related masking event would only mask events that were maskable and tagged with the same collection category, leaving unrelated events (like temperature warnings) visible.

The table below illustrates how event categories control which events are correlated:

Event Name	Type	Event Category
Dynamic App Collection Problem	masking	Dynamic Applications.Collection
Dynamic Application taking too long to collect	maskable	Dynamic Applications.Collection
Availability check failed	maskable	Dynamic Applications.Collection
Fan critical	masking	Environment.Temperature
Temperature critical	maskable	Environment.Temperature

In this example, if "Dynamic App Collection Problem" occurs on a parent chassis, Skylar One masks "Dynamic Application taking too long to collect" on the child blade (which is in the same category), but leaves "Temperature critical" visible (because it is in a different category).

Viewing the List of Event Categories

The **Event Categories** page (Events > Event Categories) displays the following about each event category:

- ***Name***. Name of the event category. You can click the name to edit the category.
- ***Event Policy Count***. Number of event policies that are aligned with the event category.

- ***ID***. Unique numeric ID for the event category, generated by Skylar One.
- ***Correlation Time***. Number of minutes that must pass before custom run book actions with an ***Action Type*** of *Run a Snippet* can correlate the event category. For more information about snippet-based run book actions, see the section on *Run Book Actions.*
- ***Event Occurrence***. Indicates whether the correlation time is measured from the first occurrence of the event (*First*) or the most recent occurrence (*Last*).
- ***Last Edited By***. Name of the user who created or last edited the event category.
- ***Last Edited Date***. Date and time the event category was created, imported into Skylar One, or last edited.

TIP: You can sort the list by a column's values by clicking on its column heading. You can also filter the items on the page by typing or selecting filter options in one or more of the filters found above the columns. For more information, see the topic on *Filtering Inventory Pages*.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the topic on *Adjusting the Row Density*.

TIP: You can rearrange the columns in the list by clicking and dragging the column to a new location. You can adjust a column's width by clicking and dragging the right edge of the column. For more information about editing and adding columns, see the topic on *Editing the Settings for an Inventory Page*.

Creating an Event Category

From the **Event Categories** page, you can define a new event category to organize and classify events according to your business requirements.

To create an event category:

1. Go to the **Event Categories** page (Events > Event Categories).
2. Click **[Create Event Category]**. The **Create an Event Category** modal appears.
3. Complete the following fields:
    - ***Category Name***. The name of the event category. Accepts up to 64 single-byte alphanumeric characters.
    - ***Correlation Time***. An integer value between 1 and 4,294,967,295 that indicates the number of minutes that must pass before custom run book actions with an ***Action Type*** of *Run a Snippet* can correlate the event category. For details, see the section on *Run Book Actions*.
    - ***Event Occurrence***. Select whether the correlation time is measured from the first occurrence of the event (*First*) or the most recent occurrence (*Last*).
4. Click **[Save]** to create the event category, or **[Cancel]** to discard your changes.

Assigning an Event Category to an Event

For information about how to assign an event category to an event policy, see the section on *The Advanced Tab*.

Assigning an Event Category to an Event in the Classic Skylar One User Interface

For information about how to assign an event category to an event policy in the classic Skylar One user interface, see the section on *Defining Pattern Matching and Advanced Behavior in the Advanced Tab*.

Editing an Event Category

You can edit an existing event category from the **Event Categories** page.

To edit an event category:

1. Go to the **Event Categories** page (Events > Event Categories).
2. Locate the event category you want to edit and click its ***Name***. (Alternatively, click the actions icon (⋮) and select *Edit*.) The **Edit Event Category** modal appears.
3. Complete the fields on the modal. For more information about these fields, see the section on *Creating an Event Category*.
4. Click **[Save]** to save the edited event category, or **[Cancel]** to discard your changes.

Deleting One or More Event Categories

You can delete one or more event categories from the **Event Categories** page. When you remove an event category, the category is also removed from any event policy with which it is aligned.

To delete event categories:

1. Go to the **Event Categories** page (Events > Event Categories).
2. Do one of the following:
   - To delete a single event category, click the actions icon (⋮) for that category and select *Delete*.
   - To delete multiple event categories, select their checkboxes and then click **[Delete]**.
3. In the modal that appears, click **[Delete]** to confirm the event category deletion.

Chapter 7

Defining and Editing Event Policies

Overview

This chapter describes how to edit and define an event policy.

This chapter covers the following topics:

How Skylar One Generates Events

Skylar One includes pre-defined events for the most commonly encountered conditions on the most common platforms. Skylar One allows you to customize these events. If the pre-defined events do not meet the needs of your organization, you can define new events. You can edit existing event policies and create new event policies in the **Event Policies** page (or the **Event Policy Manager** page in the classic Skylar One user interface).

Skylar One monitors devices (and their applications and components). Skylar One then generates log messages based on incoming trap and syslog data, incoming email messages, and user-defined policies. Each message is associated with a specific monitored device, organization, asset record, IP network,

interface, IT service, vendor, user account, or virtual interface. Skylar One then uses these log messages to generate events. Skylar One examines each incoming log message and compares it to each event policy. If a log message matches an event policy, Skylar One generates an instance of the event and displays the instance in the **Events** page (or the **Event Console** page in the classic Skylar One user interface). The event instance is associated with the entity that triggered the original log message.

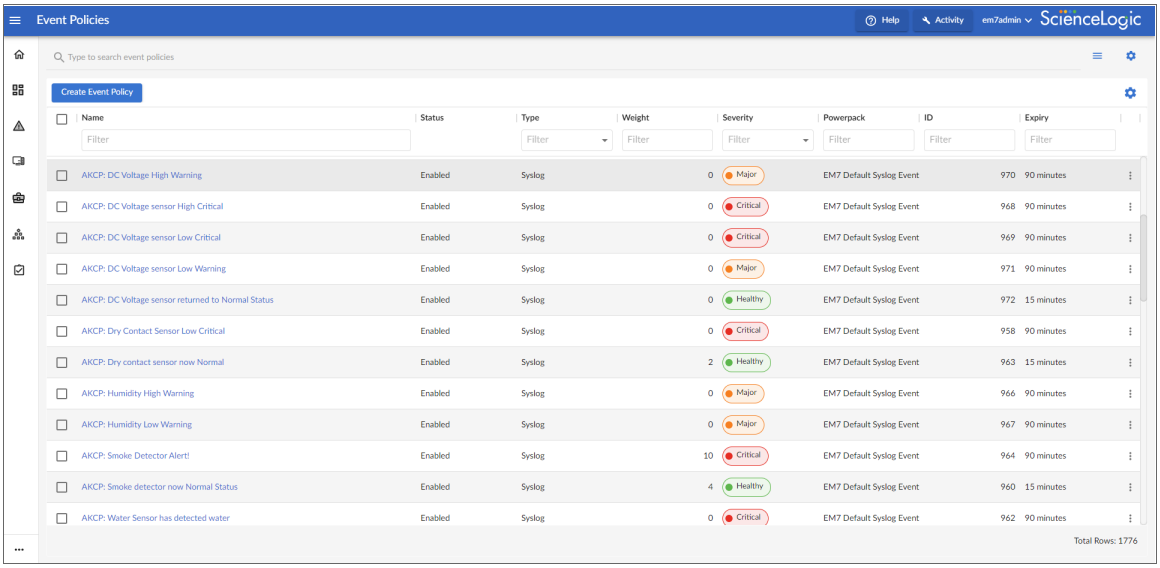
Skylar One generates events by collecting logs and messages from the following:

- ***Syslog***. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices such as managers of managers (MoM). A syslog is an unsolicited message from a device to Skylar One. Syslog is a standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools. For more information on syslogs, see the section on *syslog messages*.
- ***Internal***. Message is generated by a ScienceLogic process. The message is about the Skylar One system itself, instead of the devices that the Skylar One system monitors.
- ***Trap***. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like managers of managers (MoMs). An SNMP trap is an unsolicited message from a device to Skylar One. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device. For more information on traps, see the section on *SNMP Traps*.
- ***Dynamic***. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell Skylar One how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. Skylar One examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, Skylar One generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees Fahrenheit. If the chassis temperature exceeds 100 degrees at some point in the future, Skylar One inserts a message in the associated device's log files. Skylar One then matches that message with an existing event, and then triggers the event. For more information, see the section on *Dynamic Application Development*.
- ***Email***. Message is generated by an email message sent to Skylar One. For more information on generating events with email messages, see the section on *events from email*.
- ***API***. Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the section on *snippet actions*. For more information on snippet Dynamic Applications, see the section on *developing snippet Dynamic Applications*. For more information on the ScienceLogic API, see the section on *generating events with the ScienceLogic API*.
- ***ScienceLogic Agent***. Message is generated by log file messages collected by a Skylar One agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by an agent, see the section on *Monitoring Device Logs Using an Agent*.
- ***Rules Engine***. Message is generated through internal policy evaluations, complex correlation rules, or rule-based logic. Users cannot create or edit event policies with a ***Source*** of *Rules Engine*.
- ***Skylar Automated RCA***. Message is generated by Skylar Automated RCA alerts. Skylar One receives an alert from Skylar Automated RCA and creates an event from it. For more information, see the *Skylar AI documentation*.

- ***Skylar AI***. Message is generated by Skylar AI alerts. Skylar One receives an alert from Skylar AI and creates an event from it. For more information, see the *Skylar AI documentation*.

Viewing the List of Event Policies

The **Event Policies** page (Events > Event Policies) displays a list of all event policies in Skylar One. This page also allows you to define new event definitions and edit existing event definitions.



The **Event Policies** page displays the following about each event policy:

- ***Name***. The name of the event policy.
- ***Status***. Specifies whether the event policy is to be operational or not. Possible values are "Enabled" or "Disabled".
- ***Type***. Specifies the source for the event policy. For more information, see the section on *Event Sources*.
- ***Weight***. If two event definitions are very similar, the weight field specifies the order in which Skylar One should match messages against each event definition. This field is most useful for event policies that use expression matching. The event definition with the lowest weight is matched first.
- ***Severity***. The severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Edited By***. Name of the user who created or last edited the event.
- ***Expiry***. If enabled, the time in which an active event is cleared automatically if there is no reoccurrence of the event.
- ***Ext. Category***. The category for the event. This is an optional field. If Skylar One sends this event to an external system, this field defines the event category for use by the external system.

- ***External ID***. The external event ID for the event. The external event ID is an optional field that can be used to correlate an event policy with an event ID on another network-monitoring system or on another Skylar One system where the event has a different event ID.
- ***Last Edited***. Date and time the event was created, imported into Skylar One, or last edited.
- ***ID***. Unique numeric ID for the event policy, generated by Skylar One.
- ***PowerPack***. Specifies whether the event is included in a PowerPack.
- ***Alignment***. Displays the organization alignment of an event policy.
- ***Threshold***. If enabled, the number of instances of an identical event from the identical source that must occur before creating a new event message in the **Events** page.
- ***Time***. If enabled, the maximum amount of time to wait between multiple identical messages from the same source before creating a new event message in the *Event Monitor*. This allows related events to be rolled-up and posted together, under one event description.

TIP: You can sort the list by a column's values by clicking on its column heading. You can also filter the items on the page by typing or selecting filter options in one or more of the filters found above the columns. For more information, see the topic on *Filtering Inventory Pages*.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the topic on *Adjusting the Row Density*.

TIP: You can rearrange the columns in the list by clicking and dragging the column to a new location. You can adjust a column's width by clicking and dragging the right edge of the column. For more information about editing and adding columns, see the topic on *Editing the Settings for an Inventory Page*.

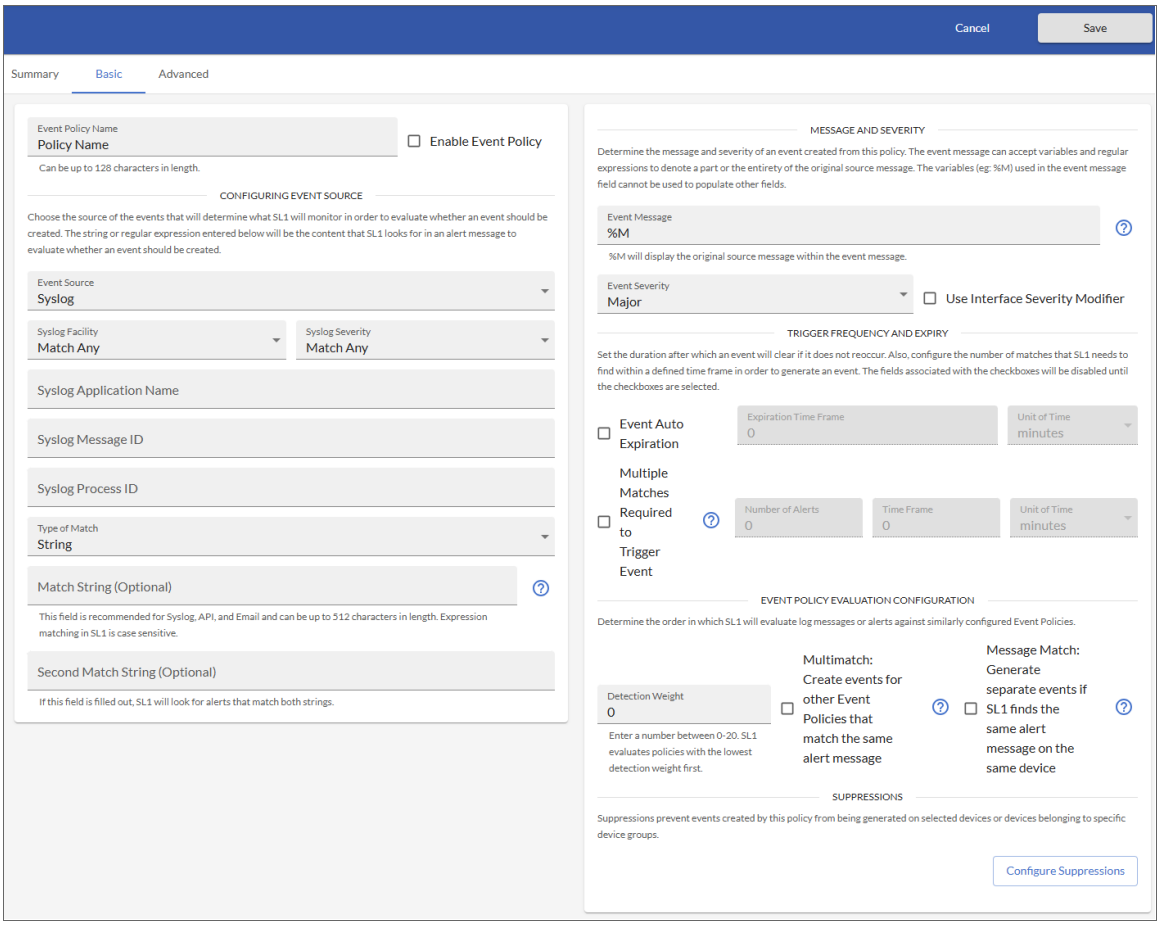
Defining an Event Policy

Skylar One includes pre-defined events for the most commonly encountered conditions on the most common platforms. However, if the pre-defined events do not meet the needs of your organization, you can define new events that better suit your needs.

From the **Event Policies** page (or the **Event Policy Manager** page in the classic Skylar One user interface), you can define a new event. You can define custom events to meet your business requirements. You can also define events to be triggered by any custom Dynamic Application alerts you have created.

To create an event definition:

1. Go to **Event Policies** page (Events > Event Policies).
2. In the **Event Policies** page, click the **[Create Event Policy]** button. The **Event Policy Editor** page appears, displaying the **[Basic]** tab.

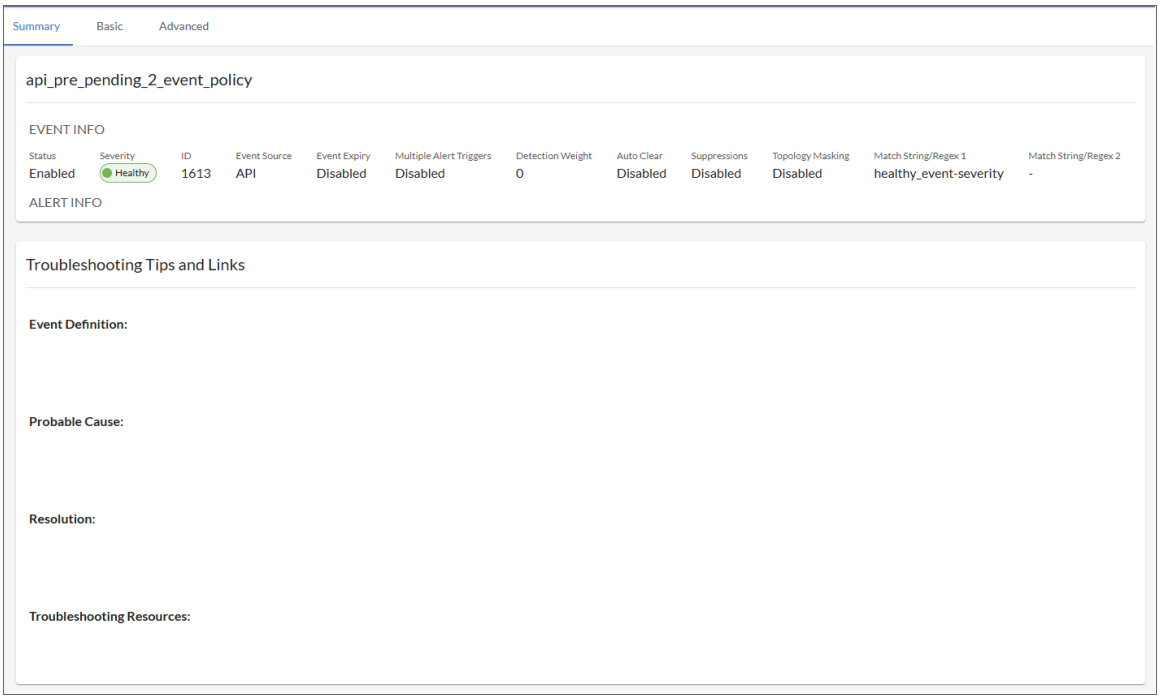


3. On the **Event Policy Editor** page and its tabs, you can define a new event. The **Event Policy Editor** page contains the following tabs:
    - **[Summary]**. The landing page when viewing or editing an existing event policy. This tab provides an at-a-glance view of the event policy properties.
    - **[Basic]**. The starting point when creating a new event policy, and the tab where you define the fundamental configuration options for the event policy.
    - **[Advanced]**. Contains more advanced configuration options, such as topology masking, device sub-entity settings, external system integration fields, and event auto-clear mapping.
4. New event policies are global by default and apply to all devices unless specified in the Suppressions field for an event policy, but you can also align the event policy to a specific organization or organizations to apply the event policy to only devices in the chosen organizations. To select a specific organization:
    - Click **[Global Policy]** at the top of the event policy. The **Policy Alignment** modal appears.
    - Select the ***Specific Organizations*** radio button.
    - If needed, use the box under ***Choose Organizations*** to filter the list of organizations.
    - Select the organizations to which the event policy should belong, and then click the **[Apply]** button to return to your event policy.

The Summary Tab

On the **[Summary]** tab, you can view an at-a-glance summary of the event policy that highlights key information or edit the following field:

- ***Troubleshooting Tips and Links***. You can use the rich text editor to add useful information about the event policy, such as an event definition, probable cause, potential resolution, or any troubleshooting resources.



The Basic Tab

On the **[Basic]** tab, you can define or edit the following fields:

- ***Event Policy Name***. Enter a name for the event policy.
- ***Enable Event Policy***. Select this checkbox to enable, or clear the checkbox to disable the event policy.

Configuring Event Source

- ***Event Source***. Specifies the source for the event. The fields below this field change based on your selection. Your options are:

- *Syslog*. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices such as managers of managers (MoM). A syslog is an unsolicited message from a device to Skylar One. Syslog is a standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools. For more information on syslogs, see the section on *syslog messages*. The following fields appear:
    - ***Syslog Facility***. Select the facility information used by syslog to match an event message.
    - ***Syslog Severity***. Select the severity information used by syslog to match an event message.
    - ***Syslog Application Name***. Type the application name used by syslog to match an event message.
    - ***Syslog Message ID***. Type the message ID used by syslog to match an event message.
    - ***Syslog Process ID***. Type the process ID used by syslog to match an event message.

    NOTE: For more information on the syslog fields for events, see https://datatracker.ietf.org/doc/html/rfc5424.

- *Internal*. Message is generated by a ScienceLogic process. The message is about the Skylar One system itself, instead of the devices that the Skylar One system monitors. The following option appears:
    - ***Link-Message***. Click the **[Select Link-Message]** button to specify the message generated by Skylar One. The **Link-Message** modal appears with a list of messages to select from. Once you have selected a message, click the **[Select]** button.

    NOTE: You can use the field at the top of the ***Link-Message*** field to filter the list of ScienceLogic messages. If you enter an alpha-numeric string in the field, the ***Link-Message*** field includes only ScienceLogic messages that match the string.

- *Trap*. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like managers of managers (MoMs). An SNMP trap is an unsolicited message from a device to Skylar One. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device. For more information on traps, see the section on *SNMP Traps*. The following options appear:

- ***Link-Trap***. Manually enter a custom trap OID as an alternative to selecting a Link-Trap using the **[Select Existing Link-Trap]** button. You can use an asterisk (*) as a wildcard character at the end of the trap OID. If you add the wildcard character to the end of the trap OID, the event policy matches all trap OIDs that start with the specified OID string. This is useful for creating "catch-all" event policies.

- ***Select Existing Link-Trap*[Select Existing Link-Trap]**. Click this button to display a list of trap OIDs that are included in the MIB files that have been compiled in Skylar One. Select one of the listed trap OIDs to associate with the event. The **Link-Trap** modal appears with a list of traps to select from. After you have selected a trap, click the **[Select]** button.

> **NOTE:** You can use the field at the top of the ***Link-Trap*** field to filter the list of SNMP traps. If you type an alpha-numeric string in the field, the ***Link-Trap*** field includes only traps that match the string.

> **NOTE:** Before selecting a trap OID, check the **SNMP Trap Filters** page (Evnts > SNMP Trap Filters, or Registry > Events > SNMP Trap Filters in the classic user interface) to be sure that the trap is not being filtered out. For more information on the **SNMP Trap Filters** page, see the *Filtering Traps* section.

- ***Source Host Varbind***. For events with a source of "trap", specifies an OID that is included in the trap. This OID contains either the IP address or hostname to align with the event. Use this field to align an event with a device other than the trap's sender. For more information about traps in Skylar One, see the section on *SNMP Traps*.

- If a value is specified in this field, Skylar One examines the OID specified in this field. If the value stored in the OID matches the primary IP address or hostname of a device in Skylar One, the resulting event is aligned with that device.
- If a value is specified in this field, Skylar One examines the OID specified in this field. If the value stored in the OID does not match a primary IP address or hostname of a device in Skylar One, the resulting event is aligned with the device that sent the trap.
- If no value is specified in this field, but the trap includes the default snmpTrapAddress OID, Skylar One examines the value stored in the snmpTrapAddress OID. If the value stored in the default snmpTrapAddress OID matches the primary IP address or hostname of a device in Skylar One, the resulting event is aligned with that device.
- If no value is specified in this field and the trap does not include the snmpTrapAddress OID, Skylar One aligns the resulting event with the device that sent the trap.

- *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell Skylar One how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. Skylar One examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, Skylar One generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees Fahrenheit. If the chassis temperature exceeds 100 degrees at some point in the future, Skylar One inserts a message in the associated device's log files. Skylar One then matches that message with an existing event, and then triggers the event. For more information, see the section on *Dynamic Application Development*. The following option appears:

    - ***Link-Alert***. Click the **[Select Dynamic Application Alert]** button to display a list of alerts defined in Dynamic Applications. A **Link-Alert** modal displays a list of alerts. After you search for and select an alert, click **[Select]**. The alert is added to the ***Link-Alert*** field.

- *API*. Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the section on *snippet actions*. For more information on snippet Dynamic Applications, see the section on *developing snippet Dynamic Applications*. For more information on the ScienceLogic API, see the section on *generating events with the ScienceLogic API*.

- *Email*. Message is generated by an email message sent to Skylar One. For more information on generating events with email messages, see the section on *events from email*.

- *ScienceLogic Agent*. Message is generated by log file messages collected by a Skylar One agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by an agent, see the section on *Monitoring Device Logs Using an Agent*. The following option appears:

    - ***Log Policy***. Select the Log File Monitoring Policy the agent uses to collect the log message.

- *Skylar Automated RCA*. Message is generated by Skylar Automated RCA alerts. Skylar One receives an alert from Skylar Automated RCA and creates an event from it. For more information, see the *Skylar AI documentation*. The following options appear:

    - ***Skylar Automated RCA Alert Type***. Select the alert type used by Skylar Automated RCA to match an event message.

    - ***Skylar Automated RCA Severity***. Select the severity used by Skylar Automated RCA to match the severity in the event message. The default value for this field is *P1*.

- *Skylar AI*. Message is generated by Skylar AI alerts. Skylar One receives an alert from Skylar AI and creates an event from it. For more information, see the *Skylar AI documentation*.

    - ***Skylar AI Severity***. Select the severity used by Skylar AI to match the severity in the event message. The default value for this field is *Disregard Severity*.

After selecting and defining your ***Event Source***, enter values in the following fields :

- ***Type of Match***. Use this field to select *String* or *Regular Expression*.
- ***Match String (Optional)***. A string used to correlate the event with a log message. Can be up to 512 characters in length. To match this event policy, the text of a log message or alert must match the value you enter in this field. Can be any combination of alpha-numeric and multi-byte characters. Skylar One's expression matching is case-sensitive. This field is recommended for events generated with a source of Syslog, API, and Email.
- ***Second Match String (Optional)***. A secondary string used to match against the originating log message. Can be up to 512 characters in length. Can be any combination of alpha-numeric and multi-byte characters. To match this event policy, the text of a log message or alert must match the value you enter in this field and the value you entered in the ***Match String*** field. This field is optional.

Message and Severity

- ***Event Message***. The message that appears on the **Events** page or the **Event Console** page when this event occurs. This field defaults to "%M" for new event policies upon creation. The message can be any combination of alphanumeric and multi-byte characters. Variables include the characters "%" (percent) and "|" (bar). You can also use regular expressions and variables that represent text from the original log message to create the ***Event Message***:

    - To include regular expressions in the event message, surround the regular expression with %R and %/R. For example:

      %RFilename: .*? %/R

      This example would search for the first instance of the string "Filename: " (Filename-colon-space) followed by any number of any characters up to the line break. The %R indicates the beginning of a regular expression. The %/R indicates the end of a regular expression.

      Skylar One uses the regular expression to search the log message and uses the matching text in the event message.

      For details on regular expression syntax, see the documentation at http://www.python.org.

      NOTE: If an event policy with a source of "Email" or "Trap" includes a poorly formed regular expression in the event message, Skylar One stops evaluating the event after 10 seconds and generates a system event with a severity of Minor, alerting you to the issue.

- You can also use the following variables in this field:
  - *%I* (capital "eye"). Depending on the context, this variable contains one of the following:
    - For events with a source of "dynamic", this variable contains the index value from SNMP; this index value displays in the Event Message. For Dynamic Applications, %I maps to the raw index that comes back from SNMP. For example, a walk of the MIB at .1.3.6.1.4.1.999.3.2.1 might return the following OIDs, in which case *%I* would return .1.1, .2.1, and .3.1, respectively:

      ```
      1.3.6.1.4.1.999.3.2.1.1.1

      1.3.6.1.4.1.999.3.2.1.2.1,

      1.3.6.1.4.1.999.3.2.1.3.1.
      ```

    - For events with a source of "syslog" or "trap", this variable contains the value that matches the ***Identifier Pattern*** field in the **[Advanced]** tab.
    - For events with a source of "internal", this variable contains the "yName" (sub-entity name) value that matches the ***Identifier Pattern*** field in the **[Advanced]** tab.
  - *%M*. The full text of the log message that triggered the event is displayed in ***Event Message*** field.
  - *%V*. Data Value from log file is displayed in the ***Event Message*** field.
  - *%T*. Threshold value from the log file is displayed in ***Event Message*** field.

> **NOTE:** Events with a ***Source*** of *Rules Engine* contain the variable ***%_event_detail_uri***. This variable resolves to the URL of the incident and provides ScienceLogic users with more details about the event.

- ***Event Severity***. Defines the severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Use Interface Severity Modifier***. If selected, when the event is triggered, Skylar One checks to see if the interface associated with this event has a custom severity modifier. If so, the event appears in the **Event Console** with that custom severity modifier applied to the severity in the ***Event Severity*** field. For example, if an interface with an ***Event Severity Adjust*** setting of *Sev -1* triggers an event with an ***Event Severity*** of *Major* and that event has the ***Use Interface Severity Modifier*** checkbox selected, the event appears in the **Event Console** with a severity of *Minor*.

Trigger Frequency and Expiry

- ***Event Auto Expiration***. If selected, enter the time in which an active event is cleared automatically if there is no reoccurrence of the event, in the fields that appear:
    - ***Expiration Time Frame***. Enter the amount of time before an active event is cleared automatically if there is no reoccurrence.
    - ***Unit of Time***. Select *minutes* or *hours*.
- ***Multiple Matches Required to Trigger Event***. If selected, enter the number of alerts and the time in which an event requires multiple triggers to occur in the fields that appear:
    - ***Number of Alerts***. Enter the number of alerts required to trigger an event within the time frame.
    - ***Time Frame***. Enter the time frame within which multiple alerts trigger an event.
    - ***Unit of Time***. Select *minutes* or *hours*.

Event Policy Evaluation Configuration

- ***Detection Weight***. If two event definitions are very similar, this field specifies the order in which Skylar One should match messages against the similar event definitions. The event definition with the lowest weight is matched first. This field is most useful for events that use expression matching. Options range from 0 (first) – 20 (last).
- ***Multimatch***. By default, Skylar One matches a log message or alert to only one event policy. If a log message or alert matches multiple event policies, Skylar One uses the ***Detection Weight*** setting to determine which event policy the log message or alert matches. If you select the ***Multimatch*** checkbox in all event policies that can match the same log message or alert, Skylar One generates an event for every event policy that matches that single log message or alert.
- ***Message Match***. If Skylar One has generated an event and then a second log message or alert matches the same event policy for the same entity, Skylar One does not generate a second event, but increases the ***count*** value for the original event on the **Events** page and in the **Viewing Events** page. By default, this behavior occurs regardless of whether the two log messages or alerts contain the same message. If you select the ***Message Match*** checkbox, this behavior occurs only if the log messages or alerts contain the same message.

Suppressions

You can suppress the event on selected devices or all devices in selected device groups. When you suppress an event, you are specifying that, in the future, if this event occurs again on a specific device, the event does not appear on the **[Events]** tab for the device.

A manually suppressed event is suppressed only for the selected devices and devices in the selected device groups. If the event occurs on another device on which it is not suppressed, the event appears on the **Events** page and on the **[Events]** tab for that device.

> **NOTE:** If you want to disable an event for all devices, see the section on *disabling an event*.

- **[Configure Suppressions]**. Click this button to specify the devices or device groups for which to suppress the event. The **Select Suppressions** modal appears on the **[Devices]** tab. Once you have selected the devices or device groups you want to suppress, click the **[Save]** button. The **Select Suppressions** modal includes the following tabs:

- **[Devices]**. To suppress the current event on one or more devices, select those devices from the list.

> **NOTE:** You can use the box at the top of the **Select Suppressions** modal to filter the list of devices. You can enter an alpha-numeric string in the box, and the list includes only devices that match the string.

- **[Device Groups]**. To suppress the current event on all devices in one or more device groups, select those device groups from the list. For information on device groups, see the section on *Device Groups*.

> **NOTE:** You can use the box at the top of the **Select Suppressions** modal to filter the list of device groups. You can enter an alpha-numeric string in the box, and the list includes only device groups that match the string.

> **NOTE:** Device groups that have *Event/View Suppression* enabled appear in this window. For information on creating device groups, see the section on *creating device groups*.

IMPORTANT: After entering information in each tab, click the **[Save]** button to save your new event.

The Advanced Tab

In the **[Advanced]** tab, you can define or edit the following fields:

Configurations for External System

- ***Correlate events with an external system***. Select this checkbox if you want to correlate the event with an external system. Enter the ***External ID*** in the field that appears when this is selected.
- ***Categorize events with an external system***. Select this checkbox if you want to categorize this event for an external system. Enter the ***External Category*** in the field that appears when this is selected.

Topology Masking

- ***Masking***. Use this option to nest events under parent devices' events if there are parent-child relationships between devices.

  IMPORTANT: Enabling a discovered device configured with CDP or LLDP topology in Skylar One causes the device to provide information on its neighbor. This information identifies only that there is a neighbor device, not which device is the parent or the child. This might cause the parent-child relationship to switch, which requires you to manually reverse the issue within Skylar One. Skylar One allows you to manually build parent-child relationships between specific device categories. For more information, see *Defining Parent and Child Devices.*

  Select one of the following options:

  - *Disabled*. Topology masking is disabled for this event.
  - *Mask events on child devices*. If this event occurs on a parent device, Skylar One searches all related children devices for masked events.
    - If you have assigned a ***Category*** to this event, Skylar One searches all the children devices and masks all events that have been defined as masked and are assigned to the same ***Category***.
    - If you have not assigned a ***Category*** to this event, Skylar One searches all children devices and masks all events that have been defined as masked and are not assigned to a ***Category***.
    - The masked events do not appear on the **Events** page. They are nested under the parent event.
  - *Maskable under a parent device's event*. This type of event is masked on a child device only when a maskable event occurs on the parent device.
    - If you have assigned a ***Category*** to this event, Skylar One masks this event when it occurs on a child device and an event that has been defined as masked occurs on its parent device. The masked event must have the same ***Category*** as the maskable event.
    - If you have not assigned a ***Category*** to this event, when a masked event that is not assigned to a ***Category*** occurs on the parent device, Skylar One searches all children devices and masks all events that have been defined as maskable and are not assigned to a ***Category***.
    - The maskable events do not appear on the **Events** page. They are nested under the parent event.
  - *Both*. If selected, then if this event occurs on a parent device, it behaves as a masked event. If this event occurs on a child device, it behaves as a maskable event.

- ***Choose Category***. When you define a hierarchy between events, you can include a ***Category***. A ***Category*** allows Skylar One to more efficiently align masked events with maskable events. When you align an event category to a masked or maskable event, that event is correlated with only events that are aligned with the same category. An event can be aligned to multiple categories; for event correlation to occur, the masked event and the maskable event must both be aligned with a common category.

  Click the **[Choose Category]** button to open the **Available Categories** modal and select the categories you want to add.

> **NOTE:** For more details on event categories, see the section on *event correlation*.

> **NOTE:** If you assign a topology category to an event that is neither suppressing nor suppressible, Skylar One does not use the ***Category***. The ***Category*** has no effect.

  - If you have assigned a ***Category*** to a masked event, Skylar One searches all the children devices and suppresses all events that have been defined as maskable and are assigned to the same ***Category***.

  - If you have not assigned a ***Category*** to a masked event, when the event occurs on the parent device Skylar One searches all children devices and suppresses all events that have been defined as maskable and are not assigned to a ***Category***.

Settings for Device Sub-Entities

- ***Extract sub-entity using a regular expression***. Select this checkbox if you want to extract a sub-entity using a regular expression. Enter values in the following fields that appear when this is turned on:
    - ***Identifier pattern***. A regular expression used to extract the name of a sub-entity (like the name of a network interface) from within the log entry. By identifying the sub-entity, Skylar One can create a unique event for each sub-entity, instead of a single event for the entire device. For an event to auto-clear another event, both events must have the same sub-entity name. The regular expression can be up to 512 characters in length and can include multi-byte characters.
    - ***Result order for multiple entities***. If the ***Identifier Pattern*** field returns multiple results, users can specify which results to use and in which order. Each result is represented by a variable. For example, users could specify "%2:%1" for "Interface %2: Peer %1", where %1 is the first match with identifier pattern and %2 is the second match with identifier pattern. This field is optional.
    - ***Sub-entity type (y-type)***. Specifies a sub-entity type (yType). A sub-entity is a hardware component (CPU, disk, interface, etc). The "yType" value is stored as an integer in a database table; each sub-entity type is associated with a unique integer value (for example, Interfaces = 7). If Skylar One knows an interface's "yName" (specified in the ***Identifier Pattern*** field) and the "yType" (specified in this field), Skylar One can determine the unique "yID" for the interface. The "yID" is stored in the table in which all instances of a specific sub-entity are stored. For example, for "yType" of "interface," the "yID" is a unique numeric ID for a specific interface on a specific device. This "yID" is stored in the table of all discovered interfaces (if_id in master_dev.device_interfaces) and is unique within this table.

> **NOTE:** If you used the previous three fields to associate an event with an interface, then on the **Events** page, the link icon for this event is for an interface and leads to a performance report for the specific interface.

> **NOTE:** The %Y variable (yName) and %y variable (yID) can be used in policies associated with events that use the previous three fields. That is, run book action policies and related ticket templates that are triggered by the event can use the %Y variable and the %y variable. For details on run book action policies and using ticket templates, see the section on *Creating an Action Policy that Creates a New Ticket*.

> **NOTE:** For events generated by Dynamic Application alerts, the %Y variable value is pre-populated with a unique index value that is used to ensure that events roll up correctly. If an event policy does not specifically override the %Y variable, this variable is populated with the "yName" (sub-entity name) value, which is taken from an index value that might not be human-readable.

> **NOTE:** Skylar One populates the "yName" (sub-entity name) value in varying ways based on the event source.
>
> For example, for events generated by Dynamic Application alerts, the yName is typically pulled from the event message using the ***Identifier Pattern*** and ***Result order for multiple entities*** that are defined in the event policy.
>
> Meanwhile, for internal events, the yName is determined by the process that creates the alert, based on which element reported the condition. So, for instance, if a filesystem exceeds a particular threshold, the yName is the filesystem identifier.

Auto-Clear

- ***Auto-Clear***. If enabled, this field specifies that the current event clears each selected event. Select ***Auto-Clear***, then click the **[Choose Event Policies]** button to select one or more events from the list. The **Available Event Policies** page appears. Select the event policies you want to auto-clear and then click the **[Select]** button.

  When the current event occurs, Skylar One automatically removes each selected event from the **Events** page. For example, suppose you have a "Device not responding to ping" event. If the next polling session produces the "Device now responding normally to ping " event, the auto-clear feature could automatically clear the original event from the **Events** page.

> IMPORTANT: After entering information in each tab, click the **[Save]** button to save your new event.

Editing an Event Policy

Skylar One includes pre-defined events for the most commonly encountered conditions on the most common platforms. However, you can customize these events to meet the needs of your organization. You can edit existing event policies in the **Event Policies** page.

> CAUTION: If you edit an event policy that was imported into your Skylar One system in a PowerPack, you should remove the event policy from the PowerPack. If you do not remove the event policy from the PowerPack and the same PowerPack is updated and re-imported into your system, any changes you have made in the **[Basic]** and **[Advanced]** tabs for the event policy are over-written. For more information on PowerPacks, see the sections on *PowerPacks.*

To edit an existing event policy:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Click the actions icon (⋮) for the event policy you want to edit and select *Edit*.

3. The selected event policy is displayed in the **Event Policy Editor** page, where you can edit one or more properties of the event policy. The **Event Policy Editor** page contains the following fields and tabs:
    - **[Summary]**. The landing page when viewing or editing an existing event policy. This tab provides an at-a-glance view of the properties of the event policy. This tab is described in the *Summary Tab* section.
    - **[Basic]**. The starting point when creating a new event policy, and the tab where you define the fundamental configuration options for the event policy. This tab is described in the *Basic Tab* section.
    - **[Advanced]**. Contains more advanced configuration options, such as topology masking, device sub-entity settings, external system integration fields, and event auto-clear mapping. This tab is described in the *Advanced Tab* section.
4. Click **[Save]** to save your changes to the event policy.

Duplicating an Event Policy

If you are creating a new Event Policy that is similar to an existing Event Policy, you can duplicate the existing Event Policy. You can then edit the duplicated Event Policy as needed to create your new Event Policy.

To duplicate an Event Policy:

1. Go to the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic user interface).
2. Click the actions icon (⋮) for the event policy you want to duplicate and select *Duplicate*. A new Event Policy appears in the list. It has the same name as the Event Policy you duplicated, with the addition of "-Copy" at the end. For example, if you duplicated an Event Policy with the name "Temperature Critical", then the new Event Policy would be named "Temperature Critical-Copy".
3. Follow the instructions in the *Editing an Event Policy* section to edit the new Event Policy.

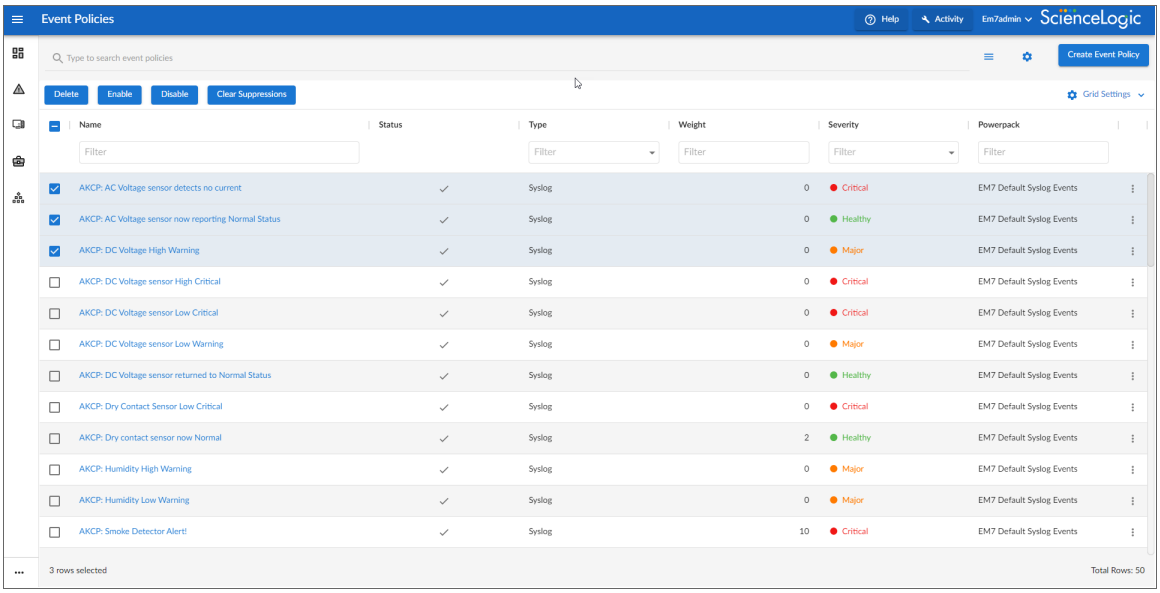
Deleting an Event Policy

To delete an Event Policy:

1. Go to the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic user interface).
2. Click the actions icon (⋮) for the event policy you want to duplicate and select *Delete*.

Selecting Multiple Event Policies

On the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic user interface), you can use the checkboxes to the left of the Event Policies to select more than one Event Policy at a time.



After you select the Event Policies, you can click one of the following buttons at the bottom of the page:

- ***Delete*[Delete]**. Deletes all of the selected Event Policies. When you click **[Delete]**, a confirmation dialog appears. To confirm that you want to delete the selected Event Policies, click **[Delete]** in the confirmation dialog.
- ***Enable*[Enable]**. Enables all of the selected Event Policies. When an Event Policy is enabled, it appears on the **Events** page for any device that meets the Event Policy's *match logic* criteria.
- ***Disable*[Disable]**. Disables all of the selected Event Policies. When an Event Policy is disabled, it no longer appears on the **Events** page for any device, even if a device meets the Event Policy's *match logic* criteria.
- ***Clear Suppressions*[Clear Suppressions]**. Clears all *suppressions* for all of the selected Event Policies. In the future, if the Event Policy is triggered on a device on which it was previously suppressed, the event appears on the **Events** page for that device.

If you want to select *all* of the Event Policies that are currently showing on the page, click the **[Select All Visible]** button.

If you do *not* want to take action on the selected Event Policies, click the **[Deselect All]** button to deselect the checkboxes.

NOTE: To use these features on the **Event Policies** page, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. For more information on access hooks, see the section on *Access Permissions*.

Using Event Policies in the Classic Skylar One User Interface

This section describes how to view, define, and edit event policies using the **Event Policy Manager** in the classic Skylar One user interface.

Viewing the List of Event Policies in the Classic Skylar One User Interface

From the **Event Policy Manager** page of the classic user interface, you can view a list of all event policies in Skylar One.

To access the **Event Policy Manager** page:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager). The **Event Policy Manager** page appears.
2. The **Event Policy Manager** page displays the following about each event policy:

TIP: To sort the list, click on a column heading. The list will be sorted by the column value, in ascending order. To sort the list by descending order, click the column heading again. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering the Items on a Classic Page* in the ***Introduction to Skylar One*** manual.

- ***Event Policy Name***. The name of the event.
- ***Type***. Specifies the source for the event. For more information, see the section on *Event Sources*.
- ***State***. Specifies whether the event is to be operational or not. Possible values are "enabled" or "disabled".
- ***P-Pack***. Specifies whether the event is included in a PowerPack.
- ***Severity***. The severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Weight***. If two event definitions are very similar, the weight field specifies the order in which Skylar One should match messages against each event definition. This field is most useful for events that use expression matching. The event definition with the lowest weight is matched first.
- ***ID***. Unique numeric ID for the event, generated by Skylar One.
- ***Expiry***. If enabled, the time in which an active event is cleared automatically if there is no reoccurrence of the event. Choices are:

    - Disabled
    - 1 minute – 24 hours
- ***Time***. If enabled, the maximum amount of time to wait between multiple identical messages from the same source before creating a new event message in the *Event Monitor*. This allows related events to be rolled-up and posted together, under one event description. Choices are:
    - Disabled
    - 1 minute – 24 hours
- ***Thresh***. If enabled, the number of instances of an identical event from the identical source that must occur before creating a new event message in the **Event Console** page. Choices are:
    - Disabled
    - 1 – 100
- ***Edited By***. Name of the user who created or last edited the event.
- ***Last Edited***. Date and time the event was created, imported into Skylar One, or last edited.
- ***External ID***. The external event ID for the event. The external event ID is an optional field that can be used to correlate an event policy with an event ID on another network-monitoring system or on another Skylar One system where the event has a different event ID.
- ***Category***. The category for the event. This is an optional field. If Skylar One sends this event to an external system, this field defines the event category for use by the external system.

Defining an Event Policy in the Classic Skylar One User Interface

Skylar One includes pre-defined events for the most commonly encountered conditions on the most common platforms. However, if the pre-defined events do not meet the needs of your organization, you can define new events that better suit your needs.

From the **Event Policy Manager** page in the classic Skylar One user interface, you can define a new event. You can define custom events to meet your business requirements. You can also define events to be triggered by any custom Dynamic Application alerts you have created.

To create an event definition in the classic Skylar One user interface:

1. Go to **Event Policy Manager** page (Registry > Events > Event Manager).
2. On the **Event Policy Manager** page, click the **[Create]** button. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page and set of tabs, you can define a new event. The **Event Policy Editor** page contains three tabs:
    - ***Policy***. Allows you to define basic parameters for the event. This tab is described in the following section.
    - ***Advanced***. Allows you to define pattern-matching for the event and also define event roll-ups and suppressions.

- ***Suppressions***. Allows you to suppress the event on selected devices. When you suppress an event, you are specifying that, in the future, if this event occurs again on a specific device, the event does not appear on the **Event Console** page or the **Viewing Events** page for the device.

Defining Basic Event Parameters in the Policy Tab

On the **Event Policy Editor**, the **[Policy]** tab allows you to define or edit the basic parameters for an event. In the **[Policy]** tab, you can define or edit the following fields:

- ***Event Source***. Specifies the source for the event. For more information, see the section on *Event Sources*.
- ***Policy Name***. The name of the event. Can be any combination of alphanumeric characters, up to 48 characters in length.
- ***Operational State***. Specifies whether the event is to be operational or not. Choices are *Enabled* or *Disabled*.

- ***Event Message***. The message that appears on the **Events** page or the **Event Console** page when this event occurs. This field defaults to "%M" for new event policies upon creation. The message can be any combination of alphanumeric and multi-byte characters. Variables include the characters "%" (percent) and "|" (bar). You can also use regular expressions and variables that represent text from the original log message to create the ***Event Message***:

    - To include regular expressions in the event message, surround the regular expression with %R and %/R. For example:

      %RFilename: .*? %/R

      This example would search for the first instance of the string "Filename: " (Filename-colon-space) followed by any number of any characters up to the line break. The %R indicates the beginning of a regular expression. The %/R indicates the end of a regular expression.

      Skylar One uses the regular expression to search the log message and uses the matching text in the event message.

      For details on regular expression syntax, see the documentation at http://www.python.org.

      NOTE: If an event policy with a source of "Email" or "Trap" includes a poorly formed regular expression in the event message, Skylar One stops evaluating the event after 10 seconds and generates a system event with a severity of Minor, alerting you to the issue.

- You can also use the following variables in this field:
  - *%I* (capital "eye"). Depending on the context, this variable contains one of the following:
    - For events with a source of "dynamic", this variable contains the index value from SNMP; this index value displays in the Event Message. For Dynamic Applications, %I maps to the raw index that comes back from SNMP. For example, a walk of the MIB at .1.3.6.1.4.1.999.3.2.1 might return the following OIDs, in which case *%I* would return .1.1, .2.1, and .3.1, respectively:

      ```
      1.3.6.1.4.1.999.3.2.1.1.1

      1.3.6.1.4.1.999.3.2.1.2.1,

      1.3.6.1.4.1.999.3.2.1.3.1.
      ```

    - For events with a source of "syslog" or "trap", this variable contains the value that matches the ***Identifier Pattern*** field in the **[Advanced]** tab.
    - For events with a source of "internal", this variable contains the "yName" (sub-entity name) value that matches the ***Identifier Pattern*** field in the **[Advanced]** tab.
  - *%M*. The full text of the log message that triggered the event is displayed in ***Event Message*** field.
  - *%V*. Data Value from log file is displayed in the ***Event Message*** field.
  - *%T*. Threshold value from the log file is displayed in ***Event Message*** field.

> **NOTE:** Events with a ***Source*** of *Rules Engine* contain the variable ***%_event_detail_uri***. This variable resolves to the URL of the incident and provides ScienceLogic users with more details about the event.

- ***Event Severity***. Defines the severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Use Modifier***. If selected, when the event is triggered, Skylar One checks to see if the interface associated with this event has a custom severity modifier. If so, the event appears in the **Event Console** with that custom severity modifier applied to the severity in the ***Event Severity*** field. For example, if an interface with an ***Event Severity Adjust*** setting of *Sev -1* triggers an event with an ***Event Severity*** of *Major* and that event has the ***Use Modifier*** checkbox selected, the event appears in the **Event Console** with a severity of *Minor*.
- ***Policy Description***. Text that explains what the event means and what possible causes are. You can use the editor to format the description text, insert content from a saved template, and add an attachment, link, or image to the description. This text is displayed in the **Event Console** page and the **Ticket Console** page.

After defining the basic properties, click **[Save]** to save your new event.

Defining Pattern Matching and Advanced Behavior in the Advanced Tab

You can use the **[Advanced]** tab on the **Event Policy Editor** page to define or edit pattern-matching for the event and also define event roll-ups and suppressions. In the **[Advanced]** tab, you can define or edit the following fields:

- ***Occurrence Count***. If enabled, the number of instances of an identical event from the identical source (that is, on the same device) that must occur before creating a new event message on the **Events** page. Options include:
    - Disabled
    - 1 – 1,000 times
- ***Occurrence Time***. The time span during which the instances of an identical event (specified in the ***Occurrence Count*** field) from the identical source must occur before Skylar One creates a new event message on the **Events** page. For example, if the ***Occurrence Count*** field contains the value "2" and the ***Occurrence Time*** field contains the value "5 minutes", the event instance must occur twice in five minutes on the same device before Skylar One generates an event message. Options include:
    - Disabled
    - Time periods from 1 minute – 2 days

  When an event has met the ***Occurrence Count*** and ***Occurrence Time*** thresholds, Skylar One creates a new event message on the **Events** page. On the **Events** page, the ***Age/Elapsed*** column specifies the time since the very first occurrence of the event, even though that occurrence did not appear on the **Events** page. The ***Count*** column specifies the number of times the event has occurred, even though the event does not appear on the **Events** page multiple times.
- ***Expiry Delay***. If enabled, the time in which an active event is cleared automatically if there is no reoccurrence of the event. Options include:
    - Disabled
    - 1 minute – 24 hours
- ***Detection Weight***. If two event definitions are very similar, the weight field specifies the order in which Skylar One should match messages against the similar event definitions. The event definition with the lowest weight is matched first. This field is most useful for events that use expression matching. Options range from 0 (first) – 20 (last).

  The weight field allows users to define detailed event definitions to be used for specific log messages, while having catch-all event definitions with less-specific matches.

  For example, suppose Skylar One receives the following log message:

  2011/04/23 12:34:22 KTLD [ERROR] Message task exception 347 while handling return

  Now suppose two events have been defined:

- Event 1:

  Matches the expression:

  KTLD [ERROR]

  Has a weight of "10"

- Event 2:

  Matches the two expressions:

  KTLD [ERROR]

  and

  exception 347

  Has a weight of "5"

Both event definitions match the log message. However, Skylar One uses only the event definition with the lowest weight. So Skylar One would first validate the incoming message against Event 2.

- ***Log Policy***. Select the Log File Monitoring Policy the agent uses to collect the log message.

> **NOTE:** The ***Log Policy*** field appears only when you select Skylar One agent in the ***Event Source*** field of the **Policy** tab. See *Defining Basic Event Parameters in the Policy Tab* for more information.

- ***Link-Message***. For events with a source of "internal", specifies the message generated by Skylar One.

> **NOTE:** You can use the field at the top of the ***Link-Message*** field to filter the list of ScienceLogic messages. If you enter an alpha-numeric string in the field, the ***Link-Message*** field includes only ScienceLogic messages that match the string.

- ***Link-Alert***. For events with a source of "dynamic", displays a list of alerts defined in Dynamic Applications. Select an alert to associate with the event.

> **NOTE:** You can use the field at the top of the ***Link-Alert*** field to filter the list of alerts from Dynamic Applications. If you enter an alpha-numeric string in the field, the ***Link-Alert*** field includes only alerts that match the string.

- ***Link-Trap***. For events with a source of "trap", displays a list of trap OIDs that are included in the MIB files that have been compiled in Skylar One. You can either select one of the listed trap OIDs to associate with the event or manually enter a custom trap OID. You can use an asterisk (*) as a wildcard character at the end of the trap OID. If you add the wildcard character to the end of the trap OID, the event policy matches all trap OIDs that start with the specified OID string. This is useful for creating "catch-all" event policies.

> **NOTE:** You can use the field at the top of the ***Link-Trap*** field to filter the list of SNMP traps. If you enter an alpha-numeric string in the field, the ***Link-Trap*** field includes only traps that match the string.

> **NOTE:** Before selecting a trap OID, check the **SNMP Trap Filters** page (Evnts > SNMP Trap Filters, or Registry > Events > SNMP Trap Filters in the classic user interface) to be sure that the trap is not being filtered out. For more information on the **SNMP Trap Filters** page, see the *Filtering Traps* section.

- ***Source Host Varbind***. For events with a source of "trap", specifies an OID that is included in the trap. This OID contains the IP address to align with the event. This field allows you to align an event with a device other than the trap's sender. For more information about traps in Skylar One, see the section on *SNMP traps*.
    - If a value is specified in this field, Skylar One examines the OID specified in this field. If the value stored in the OID matches the primary IP address of a device in Skylar One, the resulting event is aligned with that device.
    - If a value is specified in this field, Skylar One examines the OID specified in this field. If the value stored in the OID does not match a primary IP address of a device in Skylar One, the resulting event is aligned with the device that sent the trap.
    - If no value is specified in this field, but the trap includes the default snmpTrapAddress OID, Skylar One examines the value stored in the snmpTrapAddress OID. If the value stored in the default snmpTrapAddress OID matches the primary IP address of a device in Skylar One, the resulting event is aligned with that device.
    - If no value is specified in this field and the trap does not include the snmpTrapAddress OID, Skylar One aligns the resulting event with the device that sent the trap.
- ***Syslog Facility***. Facility information used by syslog to match an event message.
- ***Syslog Severity***. Severity information used by syslog to match an event message.
- ***Syslog Application Name***. Application name used by syslog to match an event message.
- ***Syslog Process ID***. Process ID used by syslog to match an event message.
- ***Syslog Message ID***. Message ID used by syslog to match an event message.

NOTE: For more information on the syslog fields for events, see https://datatracker.ietf.org/doc/html/rfc5424.

- ***Component Type***. Appears for events from all sources. Optional field. If applicable, specifies the hardware component associated with the event. Options include:
  - N/A
  - CPU
  - Disk
  - File system
  - Memory
  - Swap
  - Interface
- ***External Event Id***. Optional. If Skylar One sends an event trap to an external system, this field helps identify the event for the external system. If you need to correlate this event with an event ID on another network-monitoring system or on another Skylar One system where the event has a different event ID, you can reference that external event ID in this field. For details on sending traps to external systems, see the section on *action policies that send SNMP traps*.
- ***External Category***. Optional. If Skylar One sends an event trap to an external system, this field helps categorize the event for the external system. For details on sending traps to external systems, see the section on *action policies that send SNMP traps*.
- ***Match Logic***. Specifies whether Skylar One should process the ***First Match String*** field and ***Second Match String*** as regular expressions or as simple text matches.

NOTE: If you selected *Regex Match* in the ***Match Logic*** field, you cannot define a "match all" expression by leaving the ***First Match String*** and ***Second Match String*** fields empty.

- ***Use Multi-match***. By default, Skylar One matches a log message or alert to only one event policy. If a log message or alert matches multiple event policies, Skylar One uses the ***Detection Weight*** setting to determine which event policy the log message or alert matches. If you select the ***Use Multi-match*** checkbox in all events that can match the same log message or alert, Skylar One generates an event for every event policy that matches that single log message or alert.
- ***Use Message-match***. If Skylar One has generated an event and then a second log message or alert matches the same event policy for the same entity, Skylar One does not generate a second event, but increases the ***count*** value for the original event on the **Events** page and in the **Viewing Events** page. By default, this behavior occurs regardless of whether the two log messages or alerts contain the same message. If you select the ***Use Message-match*** checkbox, this behavior occurs only if the log messages or alerts contain the same message.

- ***First Match String***. A string used to correlate the event with a log message. Can be up to 512 characters in length. To match this event policy, the text of a log message or alert must match the value you enter in this field. Can be any combination of alpha-numeric and multi-byte characters. Skylar One's expression matching is case-sensitive. This field is required for events generated with a source of Syslog, API, and Email.
- ***Second Match String***. A secondary string used to match against the originating log message. Can be up to 512 characters in length. Can be any combination of alpha-numeric and multi-byte characters. To match this event policy, the text of a log message or alert must match the value you enter in this field and the value you entered in the ***First Match String*** field. This field is optional.

NOTE: The ***Match Logic*** field specifies whether Skylar One should process ***First Match String*** and ***Second Match String*** as simple text matches or as regular expressions.

NOTE: You can define an event so that it is triggered only when it occurs on a specific interface. You can then include the interface name and Skylar One's unique interface ID for the interface in the event message. When defining an event, you can use the following three fields below to associate an event with an interface.

- ***Identifier Pattern***. A regular expression used to extract the name of a sub-entity (like the name of a network interface) from within the log entry. By identifying the sub-entity, Skylar One can create a unique event for each sub-entity, instead of a single event for the entire device. For an event to auto-clear another event, both events must have the same sub-entity name. The regular expression can be up to 512 characters in length and can include multi-byte characters.

  For example, a log message indicating a link has gone down may include the network interface name. So the ***Identifier Pattern*** field could extract the network interface name from the log message. Skylar One assigns this value as the "yName" (sub-entity name) of the interface in the database table for interfaces. This name tends to be more descriptive of the interface (for example eth01, eth02, s01, s02) and is unique on the device, but is not unique in Skylar One.

NOTE: Skylar One's expression matching is case-sensitive.

  For details on the regular-expression syntax allowed by Skylar One, see http://www.python.org/doc/howto/.

- ***Override YType***. Specifies a sub-entity type (yType). A sub-entity is a hardware component (CPU, disk, interface, etc). The "yType" value is stored as an integer in a database table; each sub-entity type is associated with a unique integer value (for example, Interfaces = 7). If Skylar One knows an interface's "yName" (specified in the ***Identifier Pattern*** field) and the "yType" (specified in this field), Skylar One can determine the unique "yID" for the interface. The "yID" is stored in the table in which all instances of a specific sub-entity are stored. For example, for "yType" of "interface," the "yID" is a unique numeric ID for a specific interface on a specific device. This "yID" is stored in the table of all discovered interfaces (if_id in master_dev.device_interfaces) and is unique within this table.

- ***Identifier Format***. (Optional.) If the ***Identifier Pattern*** field returns multiple results, you can use variables to specify which results to use and in which order. Additional text strings can also be added with the variables to provide descriptions and make event messages more readable. When an ***Event Message*** definition contains the variable *%I* (capital "eye"), the *%I* variable is replaced with the output specified in the ***Identifier Format*** field. You can use the following variables in this field, in addition to text strings:
    - %1. The first match with the identifier pattern. This is the default behavior if no value is supplied in the ***Identifier Format*** field.
    - %2. The second match with identifier pattern.
    - %3. The third match with the identifier pattern. And so forth.

NOTE: If you used the previous three fields to associate an event with an interface, then on the **Events** page, the link icon for this event is for an interface and leads to a performance report for the specific interface.

NOTE: The %Y variable (yName) and %y variable (yID) can be used in policies associated with events that use the previous three fields. That is, run book action policies and related ticket templates that are triggered by the event can use the %Y variable and the %y variable. For details on run book action policies and using ticket templates, see the section on *Creating an Action Policy that Creates a New Ticket*.

NOTE: For events generated by Dynamic Application alerts, the %Y variable value is pre-populated with a unique index value that is used to ensure that events roll up correctly. If an event policy does not specifically override the %Y variable, this variable is populated with the "yName" (sub-entity name) value, which is taken from an index value that might not be human-readable.

NOTE: Skylar One populates the "yName" (sub-entity name) value in varying ways based on the event source.

For example, for events generated by Dynamic Application alerts, the yName is typically pulled from the event message using the ***Identifier Pattern*** and ***Identifier Format*** that are defined in the event policy.

Meanwhile, for internal events, the yName is determined by the process that creates the alert, based on which element reported the condition. So, for instance, if a filesystem exceeds a particular threshold, the yName is the filesystem identifier.

For example, given the following incoming message:

```
component: Primordial Pool; details: Pool not found; nodeID: 003;
There is extra data here we do not care about until the messageCode:
867-5309; state: Unknown
```

And given this ***Identifier Pattern***:

```
component: ([^;]+); details: ([^;]+); nodeID: ([^;]+);.*messageCode:
([^;]+); state: ([^;]+);
```

An ***Identifier Format*** could be specified as such:

```
3PAR message code: %4 - Node and component: %3-%1 - Current State: %5
```

Which would cause variable %I (capital "eye") used in an ***Event Message*** to return the following string:

```
3PAR message code: 867-5309 - Node and component: 003-Primordial Pool
- Current State: Unknown
```

- ***Auto-Clear***. If enabled, this field specifies that the current event clears each selected event. Click the **[Add Event Policy]** button to select one or more events from the list. When the current event occurs, Skylar One automatically removes each selected event from the **Event Console** page.

  For example, suppose you have a "Device not responding to ping" event. If the next polling session produces the "Device now responding normally to ping " event, the auto-clear feature could automatically clear the original event from the **Event Console** page.

> **NOTE:** You can use the field at the top of the ***Auto-Clear*** field to filter the list of events. If you enter an alpha-numeric string in the field, the ***Auto-Clear*** field includes only events that match the string.

- ***Topology Suppression***. Defines event correlation. This setting is used when events occur on devices that have a parent/child relationship. Skylar One automatically defines parent/child relationships when it discovers layer-2, CDP, LLDP, layer-3, and VMware topology. You can also manually define parent/child relationships between devices. For event correlation to occur, two types of events must be defined: *Suppressing* Events and *Suppressible* Events. For more details on topology suppression, see the section on *event correlation*.

  The ***Topology Suppression*** field contains the following options:

  - *Disabled*. This event is neither a parent event nor a child event.
  - *Suppressing*. If this event occurs on a parent device, Skylar One searches all related children devices for suppressible events.

- If you have assigned a ***Category*** to this event, Skylar One searches all the children devices and suppresses all events that have been defined as *Suppressible* and are assigned to the same ***Category***. For more details on event categories, see the section on *event correlation*.
- If you have not assigned a ***Category*** to this event, Skylar One searches all children devices and suppresses all events that have been defined as *Suppressible* and are not assigned to a ***Category***. For more details on event categories, see the section on *event correlation*.
- The suppressible events do not appear on the **Event Console** page. They are nested under the parent event.

◦ *Suppressible*. This type of event is suppressed on a child device only when a suppressing event occurs on the parent device.

- If you have assigned a ***Category*** to this event, Skylar One suppresses this event when it occurs on a child device and an event that has been defined as *Suppressing* occurs on its parent device. The suppressing event must have the same ***Category*** as the suppressible event. For more details on event categories, see the section on *event correlation*.
- If you have not assigned a ***Category*** to this event, when a *Suppressing* event that is not assigned to a ***Category*** occurs on the parent device Skylar One searches all children devices and suppresses all events that have been defined as *Suppressible* and are not assigned to a ***Category***. For more details on event categories, see the section on *event correlation*.
- The suppressible events do not appear on the **Event Console** page. They are nested under the parent event.

◦ *Both*. If this event occurs on a parent device, it behaves as a suppressing event. If this event occurs on a child device, it behaves as a suppressible event. See the descriptions of *Suppressing* and *Suppressible* for details on each type of event.

- ***Category***. When you define a hierarchy between events, you can include a ***Category***. A ***Category*** allows Skylar One to more efficiently align suppressing events with suppressible events. When you align an event category to a suppressing or suppressible event, that event is correlated with only events that are aligned with the same category. An event can be aligned to multiple categories; for event correlation to occur, the suppressing event and the suppressible event must both be aligned with a common category. For more details on event categories, see the section on *event correlation*.

> **NOTE:** You can use the field at the top of the ***Category*** field to filter the list of events. If you enter an alpha-numeric string in the field, the ***Category*** field includes only events that match the string.

> **NOTE:** If you assign a topology category to an event that is neither suppressing nor suppressible, Skylar One does not use the ***Category***. The ***Category*** has no effect.

  - If you have assigned a ***Category*** to a Suppressing event, Skylar One searches all the children devices and suppresses all events that have been defined as *Suppressible* and are assigned to the same ***Category***.
  - If you have not assigned a ***Category*** to a Suppressing event, when the event occurs on the parent device Skylar One searches all children devices and suppresses all events that have been defined as *Suppressible* and are not assigned to a ***Category***.

Defining Event Suppressions in the Suppressions Tab

The **[Suppressions]** tab in the **Event Policy Editor** page allows you to suppress the event on selected devices or all devices in selected device groups. When you suppress an event, you are specifying that, in the future, if this event occurs again on a specific device, the event does not appear on the **Events** page.

A manually suppressed event is suppressed only for the selected devices and devices in the selected device groups. If the event occurs on another device, the event appears on the **Events** page.

> **NOTE:** If you want to disable an event for all devices, see the section on *disabling an event*.

In the **[Suppressions]** tab, you can define or edit the following:

- ***Available Device Groups***. Device groups on which you can suppress the current event. To suppress the current event on all devices in a device group, highlight the device group and click the **[>>]** button. The device group should now appear in the ***Suppressed Device Groups*** field. To select multiple device groups, hold down the **<Shift>** key and select device groups. For information on device groups, see the section on *device groups*.

> **NOTE:** You can use the box at the top of the ***Available Device Groups*** field to filter the list of device groups. You can enter an alpha-numeric string in the box, and the ***Available Device Groups*** field includes only device groups that match the string.

> **NOTE:** Device groups that have *Event/View Suppression* enabled appear in this field. For information on creating device groups, see the section on *creating device groups*.

- ***Suppressed Device Groups***. Device groups on which the event is already suppressed. For information on device groups, see the section on *device groups*.
- ***Available Devices***. Devices on which you can suppress the current event. To suppress the current event on a device, highlight the device and click the **[>>]** button. The device should now appear in the ***Suppressed Devices*** field. To select multiple devices, hold down the **<Shift>** key and select devices.

> **NOTE:** You can use the box at the top of the ***Available Devices*** field to filter the list of devices. You can enter an alpha-numeric string in the box, and the ***Available Devices*** field includes only devices that match the string.

- ***Suppressed Devices***. Devices on which the event is already suppressed.

You can use the arrow buttons (**[<<]** and **[>>]**) to move device groups and devices from the ***Available*** and ***Suppressed*** lists.

Defining an Event Policy for a Specific Interface

You can define an event so that it is triggered only when it occurs on a specific interface.

You can also include the interface name and Skylar One's unique interface ID in automation policies associated with the event.

This section describes how to define an event policy for an interface.

There are three database fields that Skylar One uses to associate an event with an interface:

- ***yType***. The type of sub-entity (CPU, disk, interface, etc.). This value is stored as an integer; each sub-entity type is associated with a unique integer value (for example, Interfaces = 7).
- ***yID***. The unique ID of the instance of a sub-entity. This value is stored in the table in which all instances of a specific sub-entity are stored. For example, for yType of *interface*, the yID is a unique numeric ID for a specific interface on a specific device. This yID is stored in the table of all discovered interfaces (if_id in master_dev.device_interfaces) and is unique within this table.
- ***yName***. The name of the sub-entity. This name tends to be more descriptive of the interface (for example *eth01*, *eth02*, *s01*, *s02*) and is unique on the device, but is not unique in Skylar One.

When defining an event, you can use the following three fields to associate an event with an interface:

- ***Identifier Pattern***. A regular expression used to extract the specific sub-entity (like the name of a network interface) within the log entry. Skylar One uses this value as the yName of the interface. By identifying the sub-entity, Skylar One can create a unique event for each sub-entity, instead of a single event for the entire device. For example, a log message indicating a link has gone down may include the network interface name. So this field could extract the network interface name from the log message. Skylar One's expression matching is case-sensitive.

  For details on regular expression syntax, see the documentation at http://www.python.org.

- ***Identifier Format***. (Optional.) If the ***Identifier Pattern*** field returns multiple results, users can use variables to specify which results to use and in which order. Additional text strings can also be added with the variables to provide descriptions and make event messages more readable. When an ***Event Message*** definition contains the variable *%I* (capital "eye"), the *%I* variable is replaced with the output specified in the ***Identifier Format*** field. You can use the following variables in this field, in addition to text strings:

  - %1. The first match with the identifier pattern. This is the default behavior if no value is supplied in the ***Identifier Format*** field.
  - %2. The second match with identifier pattern.
  - %3. The third match with the identifier pattern. And so forth.

TIP: For an example of how to use the ***Identifier Pattern*** and ***Identifier Format*** fields to customize event messages, see the section on *Defining Pattern Matching and Advanced Behavior in the Advanced Tab*.

- ***Override YType***. Specifies a yType for the interface (yType for interfaces is *7*). If Skylar One knows the device name, the interface's yName (specified in the ***Identifier Pattern*** field), and the yType (specified in the ***Override YType*** field), Skylar One can determine the unique yID for the interface.

NOTE: For events generated by Dynamic Application alerts, the %Y variable value is pre-populated with a unique index value that is used to ensure that events roll up correctly. If an event policy does not specifically override the %Y variable, this variable is populated with the "yName" (sub-entity name) value, which is taken from an index value that might not be human-readable.

If these fields are used in an event:

- On the **Events** page, the link icon for this event is for an interface and leads to a performance report for the specific interface.
- The %Y variable (yName) and %y variable (yID) can be used in policies associated with this event. That is, run book action policies and related ticket templates that are triggered by the event can include the %Y variable and the %y variable. For details on run book action policies and using ticket templates, see the section on *Creating an Action Policy that Creates a New Ticket*.

Defining Custom Severity for an Interface

In the **Interface Properties** page, you can define a custom severity for an interface. You can then configure an event to use this custom severity when the event occurs for that interface. For details on the **Interface Properties** page, see section on *network interfaces*.

For example, suppose interface Gi1/0/1 on a Cisco switch named cisco_switch_network1 is part of a mission-critical service. By default, event policies for interface events have a severity of "notice" or "major". You could define a custom severity modifier that increases the severity of those events to "critical" when they are generated for the Gi1/0/1 interface.

You could then edit the following events and tell them to use the custom severity for each interface that includes a custom severity:

- Poller: Interface Admin down (usually has a default severity of "Notice").
- Poller: Interface operationally down (usually has a default severity of "Minor").
- Poller: Interface reporting discards (usually has a default severity of "Minor").
- Poller: Interface reporting packet errors (usually has a default severity of "Minor").

Now when any of those events occur on interface Gi1/0/1 on the switch cisco_switch_network1, the event has an increased severity.

To define a custom severity for an interface:

1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).
2. Click the wrench icon (🔧) for the interface for which you want to view the **Interface Properties** page.
3. Supply a value in the ***Event Severity Adjust*** field. Click **[Save]**.

To edit an event policy to use custom severities for interfaces:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Click the wrench icon (🔧) for the event policy you want to edit.
3. Click the **[Policy]** tab.
4. In the **Event Policy Editor** page, select the ***Use Modifier*** checkbox .
5. Click **[Save]**.

Editing an Event Policy in the Classic Skylar One User Interface

Skylar One includes pre-defined events for the most commonly encountered conditions on the most common platforms. You can customize these events to meet the needs of your organization. You can edit existing event policies in the **Event Policy Manager** page of the classic user interface.

CAUTION: If you edit an event policy that was imported into your Skylar One system in a PowerPack, you should remove the event policy from the PowerPack. If you do not remove the event policy from the PowerPack and the same PowerPack is updated and re-imported into your system, any changes you have made in the **[Policy]** and **[Advanced]** tabs for the event policy are over-written. For more information on PowerPacks, see the section on *PowerPacks.*

To edit an existing event policy:

1. Go to the **Event Policy Manager** page (Events > Event Policies).
2. In the **Event Policy Manager** page, click the wrench icon (🔧) of the event policy you want to edit.
3. The selected event policy is displayed in the **Event Policy Editor** page, where you can edit one or more properties of the event policy.
4. The **Event Policy Editor** page contains three tabs:
    - ***Policy***. Allows you to define basic parameters for the event. The fields in this tab are described in the section *Defining Basic Event Parameters in the Policy tab.*
    - ***Advanced***. Allows you to define pattern-matching for the event and also define event roll-ups and suppressions. The fields in this tab are described in the section *Defining Pattern Matching and Advanced Behavior in the Advanced Tab*.
    - ***Suppressions***. Allows you to suppress the event on selected devices. When you suppress an event, you are specifying that, in the future, if this event occurs again on a specific device, the event does not appear on the **Events** page. This tab is described in the section *Defining Event Suppressions in the Suppressions tab*.
6. Click **[Save]** to save your changes to the event policy.

Best Practices for Event Definitions

The **Event Policy Editor** page was designed to be an intuitive tool that allows technical users to quickly create customized events from standard collection methodologies. The following best practices help make event definitions efficient and effective:

- For quicker setup and consistency across platforms, you can export and import event definitions using PowerPacks (System > Manage > PowerPacks), which allows for easy sharing and backing-up. A PowerPack is an exportable and importable package of one or more Dynamic Applications, event policies, device categories, device classes, device templates, device groups, reports, dashboard widgets, dashboards, run book automations, run book actions, ticket templates, credentials, XSL transformations, UI themes, and/or IT Service policies. You can use PowerPacks to share customized content among Skylar One systems and to download customized content from ScienceLogic. For details on creating and using PowerPacks, see the section on *PowerPacks.*
- When creating new *event definitions*, make sure to set the ***Event Source*** field to the type of message you are working with.
- *Regular-expression matching* in Skylar One is case-sensitive.
- Use care when creating regular expressions. For example, remember that variables within messages (such as date, device name, and IP address) might differ from device to device.
- Using *the "weight" function* can help better qualify events and allow for greater definition of environment-specific events. For example, suppose you created three slightly different event definitions:
    - Event 1:
        - First Match String = Server Down
        - Second Match String = left blank
        - Detection Weight = 10
        - Severity = Minor
    - Event 2:
        - First Match String = Server Down
        - Second Match String = dev
        - Detection Weight = 5
        - Severity = Major
    - Event 3:
        - First Match String = Server Down
        - Second Match String = dev-mssql-001
        - Detection Weight = 0
        - Severity = Critical

  Because it has the lowest weight, Event 3, the critical event, would always be checked first. Event 2, the major event, would be checked second. The least specific event, Event 1, would be checked third.

Chapter 8

Event Notification and Event Automation

Overview

Skylar One includes automation features that allow you to define specific event conditions and the actions you want Skylar One to execute when those event conditions are met.

This chapter covers the following topics:

Automation Policies

An automation policy allows you to define automatic actions that should be executed in response to events. An ***automation policy*** defines the event conditions that can trigger an automatic action.

When the event criteria in an automation policy are met, an action is executed. This action is defined in an action policy. To view a list of action policies, go to the **Action Policy Manager** page (Registry > Run Book > Actions).

For example, an automation policy might specify: if the event "illicit process" occurs on device "mailserver01", and the event is not cleared within five minutes, execute the action policy "Email NOC". The action policy "Email NOC" could notify all NOC staff about the "illicit process" event.

Automation policies can describe the following criteria. One or more of these criteria must be met before an action is executed:

- One or more specified events must have occurred.
- Events must have occurred on one of the specified devices.
- Events must have the specified severity (critical, major, minor, notice, or healthy).
- Events must have the specified status (event is not cleared, event is not acknowledged, ticket is not created for event).
- A specific amount of time must elapse while the status does not change.

When the criteria are met, the automation policy triggers the execution of one or more specified action policies.

To create an automation policy, go to the **Automation Policy Manager** page (Registry > Run Book > Automation).

Action Policies

An ***action policy*** is an action that can be automatically triggered in Skylar One when certain criteria are met. The triggers are defined in an automation policy, on the **Automation Policy Manager** page (Registry > Run Book > Automation).

An action policy can perform one of the following tasks:

- Send an email message to a pre-defined list of users.
- Send an SNMP trap from Skylar One to an external device.
- Create a new ticket using ticket templates defined on the **Ticket Templates** page (Registry > Ticketing > Templates).
- Update an existing ticket.
- Write an SNMP value to an existing SNMP object on an external device.
- Execute a custom snippet (Python program).
- Query a database.

To create an action policy, go to the **Action Policy Manager** page (Registry > Run Book > Actions).

Chapter 9

Events from Email

Overview

Skylar One can generate events based on emails the system receives from external devices.

When an ***Event from Email*** policy matches an incoming email with a device in Skylar One, the Event from Email policy creates a log entry in the device log. The log entry includes the contents of the email subject line and message body. You can then configure Skylar One to trigger events from those log entries.

This chapter covers the following topics:

Configuring Events from Email

To configure Skylar One to generate an event from an incoming email, you must perform the following tasks:

- Define settings in the **Email Settings** page (System > Settings > Email) that allow Skylar One to receive incoming email messages.
- Ensure that the DNS server that handles name-service for the ScienceLogic network is configured correctly to direct email messages to Skylar One.
- In the **Emailer Redirection** page (Events > Inbound Email, or Registry > Events > Inbound Email in the classic user interface), define an email originator policy.
- Configure the third-party system to send event messages to Skylar One via email.
- Define events based on incoming email messages. In the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit), in the ***Event Source*** field, select *Email*.

For more information, see the chapter on "Events from Email" in the manual ***Inbound Email***.

Chapter 10

Using Webhooks to Generate Events

Overview

Webhooks enable one system to notify another system about events using a defined message format. You can configure Skylar One to receive webhook messages from third-party systems and then generate events from those messages.

This chapter covers the following topics:

What Are Webhooks?

Webhooks are system integration patterns where one system notifies other systems about events using a defined message format over HTTP.

In this scenario, the system sending the message is called the ***provider***, and the system ingesting and processing the message is called the ***receiver***.

You can configure your Skylar One system to ingest webhooks using one or more webhook receivers. You can then create event policies that generate events based on the received webhook messages.

Workflow for Configuring Skylar One to Ingest Webhooks

To configure Skylar One to ingest webhooks to generate events, you must do the following:

1. Upgrade to Skylar One version 11.2.0 or later.
2. *Enable the webhook collector process*.
3. *Configure your Message Collectors or All-In-One Appliance to process webhooks*.
4. *Add a ScienceLogic Library that contains your webhook handlers*, and include that library in an execution environment.
5. *Create a collector group (CUG)* and align one or more Message Collectors and devices to that collector group.
6. *Create a webhook receiver*.
7. *Define an event policy to create events from webhook payloads*.

Enabling the Webhook Collector Process

The "Data Collection: Webhook Collector" system process is disabled by default. Before you can use webhooks to generate events, you must enable this process.

To enable the webhook collector process:

1. In Skylar One, go to the **Process Manager** page (System > Settings > Admin Processes).
2. Locate the process named "Data Collection: Webhook Collector" and click its wrench icon (🔧). The **Process Editor** modal appears.
3. In the **Process Editor** modal, complete the following fields:
    - In the ***Operating State*** field, select *Enabled*.
    - In the ***Appliance Types*** field, select the *All-In-One Server* and *Message Collection Unit* checkboxes.

4. Click **[Save]**.

Configuring Message Collectors or an All-In-One Appliance for Webhooks

After you have enabled the webhook collector process, you must then configure nginx and firewalld on the Message Collectors or All-In-One Appliance on which you want to receive webhooks, so they know which port to listen to for webhook messages.

To configure Message Collectors or All-In-One Appliance for webhooks:

1. Use SSH to access the Message Collector or All-In-One Appliance on which you want to receive webhooks.
2. Run one of the following commands, depending on the version of Skylar One you are running:

   For Skylar One 11.2.0:

   ```
   sudo /opt/em7/share/scripts/webhook_collector_status.sh -e <port>
   ```

   where `<port>` is the desired port number. The default port for webhooks is 8443. For more information, see the chapter on "Required Ports" in the ***Installation and Initial Configuration*** manual to view a list of ports that are already reserved for use in Skylar One.

   For Skylar One 11.3.0 and later:

   ```
   sudo /opt/em7/share/scripts/configure_webhook.py activate
   ```

3. After running the script, check the output to ensure the **webhook_collector.service** is running. In the output, under "systemd", the **webhook_collector.service** should show that it is "active (running)".
4. If you want to view the webhook collector logs on the Message Collector or All-In-One Appliance, run one of the following commands, depending on the version of Skylar One you are running:

   For Skylar One 11.2.0:

   ```
   cat /var/log/em7/webhook_collector.log
   ```

   For Skylar One 11.3.0 and later:

   ```
   cat /var/log/sl1/webhook_collector.log
   ```

Adding a ScienceLogic Library with Webhook Handlers

Before you can create a webhook receiver in Skylar One, you must add a ScienceLogic library that contains your webhook handlers, which are Python functions that handle incoming requests. You must then add that library to an execution environment, which enables the Database Server to propagate the

library to the Message Collectors or All-In-One Appliance using the "Enterprise Database: Collector Config Push" process (**config_push.py**).

> **TIP:** It might be helpful to include a logger in your webhook handler functions so you can view log output.

To add a ScienceLogic library with webhook handlers:

1. Go to the **ScienceLogic Library Manager** page (System > Customize > ScienceLogic Libraries).
2. Click the **[Actions]** menu, then select *Import ScienceLogic Library*. The **Import ScienceLogic Library** modal appears.
3. Click the **[Browse]** button.
4. Select the library file that contains your webhook handlers, and then click **[Upload]**. ScienceLogic libraries support **py_directory** and **py_package** format types.
5. When you are finished, click **[Import]** and then click **[OK]** to confirm.
6. After your new library is imported, you must align it to an execution environment. To do so, click the **[Actions]** menu and then select *Execution Environments*. The **Execution Environments** modal appears.
7. Click **[New]** to create a new execution environment, or select an existing execution environment from the list and click its wrench icon ( ). The **Environment Editor** modal appears.
8. On the **Environment Editor** modal:
   - If you are creating a new execution environment, enter a name for your new environment in the ***Environment Name*** field, and then click the save icon ( ).
   - In the **ScienceLogic Library** pane, find the Library that you imported and then click its lightning bolt icon ( ) to align the library to the execution environment.
9. When you are finished, close the **Environment Editor** modal.

Aligning a Collector Group and Devices for Webhooks

The next steps to configuring Skylar One to ingest webhooks are to create a collector group (CUG), align the Message Collectors on which you want to receive webhooks to that collector group, and assign at least one device to that collector group.

To align a collector group for webhooks:

1. Create or edit a collector group (CUG) for use with webhooks. For more information, see the chapter on "Collector Groups" in the ***System Administration*** manual.
2. When creating the collector group, make sure to do the following:
   - In the ***Collector Group Name*** field, enter a unique name for the collector group if you are creating a new collector group.
   - In the ***Message Collector*** field, select the Message Collectors on which you want to receive webhooks. For an All-In-One Appliance, use the default collector group.

3. Discover a physical device, create a virtual device, or edit an existing physical or virtual device, and assign that device to the collector group you created in step 1.
    - If discovering a physical device in the default Skylar One user interface ("AP2") using guided discovery, select a collector group in the ***Collector Group Name*** field on the final page of the guided discovery wizard. For more information, see the section on "Adding Devices Using Guided Discovery" in the ***Discovery & Credentials*** manual.
    - If discovering a physical device in the default Skylar One user interface ("AP2") using unguided discovery, select a collector group in the ***Which collector will discover these devices?*** field on the final page of the unguided discovery wizard. For more information, see the section on "Adding Devices Using Unguided Discovery" in the ***Discovery & Credentials*** manual.
    - If discovering a physical device in the classic Skylar One user interface, select a Data Collector or All-In-One Appliance in the ***Collection Server PID*** field on the **Discovery Session Editor** modal. After initial discovery, each device uses the collector group that contains this Data Collector or All-In-One Appliance for collection and rediscovery. For more information, see the section on "Running a Classic Discovery Session" in the ***Discovery & Credentials*** manual.
    - If creating a virtual device, select a collector group in the ***Collector*** field of the **Create Virtual Device** modal. For more information, see the section on "Defining a Virtual Device" in the ***Device Management*** manual.
    - If editing an existing physical or virtual device in the default Skylar One user interface ("AP2"), go to the **[Settings]** tab of the **Device Investigator** for the device you want to update, click **[Edit]**, select a different collector group in the ***Collection Poller*** field, and then click **[Save]**. For more information, see the section on "The Settings Tab" in the ***Device Management*** manual.
    - If editing an existing physical or virtual device in the classic Skylar One user interface, go to the **Device Administration** panel for the device you want to update, click its wrench icon (), select a different collector group in the ***Collection Poller*** field, and then click **[Save]**. For more information, see the section on "Editing Device Settings" in the ***Device Management*** manual.

Managing Webhook Receivers

This section describes how to view, create, edit, and delete webhook receivers in Skylar One.

Viewing the List of Webhook Receivers

You can view a list of webhook receivers on the **Webhooks** page (Registry > Monitors > Webhooks). For each webhook receiver, the **Webhooks** page displays the following information:

- ***Webhook Name***. The unique name for each webhook receiver.
- ***Webhook URL Suffix***. The unique URL suffix for each webhook receiver.
- ***Webhook ID***. The unique ID for each webhook receiver.
- ***Import Module***. The Python handler module that is imported from the ScienceLogic Library associated with each webhook receiver.

- ***Import Handler***. The Python handler function that is imported from the ScienceLogic Library associated with each webhook receiver.
- ***Status***. The status of each webhook receiver.
- ***Device ID***. The unique ID of the device aligned to each webhook receiver.
- ***Device Name***. The name of the device aligned to each webhook receiver.
- ***IP Address***. The IP address of the device aligned to each webhook receiver.
- ***Device Category***. The category assigned to the device aligned to each webhook receiver.
- ***Organization***. The organization assigned to the device aligned to each webhook receiver.

Creating a Webhook Receiver

You can create webhook receivers from the **Webhooks** page or from the **Monitoring Policies** page for a device. Both methods are described in the sections below.

Creating a Webhook Receiver from the Webhooks Page

1. Go to the **Webhooks** page (Registry > Monitors > Webhooks).
2. Click the **[Create]** button. The **Create New Webhook** modal appears.
3. Select *the device that you want to align to the new webhook receiver* by clicking its device icon ( ).
4. Select *the ScienceLogic Library that contains the webhook handler function* by clicking its library icon ( ).
5. On the **Create New Webhook** modal, complete the following fields:
    - ***Device***. Displays the device that you selected to align to the webhook receiver. Click **[Change Selected Device]** to select a different device.
    - ***Webhook Name***. Type a unique name for the webhook receiver.
    - ***Webhook URL Suffix***. Type a unique URL suffix for the webhook receiver.

- ***Available Webhook URL***. Displays the auto-generated full URL of the webhook receiver. The webhook URL consists of the IP address and port number of the Message Collector or All-In-One Appliance that is associated with the selected device's collector group, the static URL fragment "/api/v1/webhook", and the webhook URL suffix, in the following format:

  ```
  https://<IP address>:<port number>/api/v1/webhook/<webhook URL suffix>
  ```

  For example: `https://10.2.20.56:8888/api/v1/webhook/test_webhook_url`

  NOTE: For Skylar One to auto-generate the full webhook URL, you must have already set up and enabled the webhook collector service on the associated Message Collector or All-In-One Appliance.

  NOTE: If the selected device is aligned to a collector group that includes multiple Message Collectors, then multiple URLs appear in this field, as Skylar One will auto-generate a URL for each Message Collector.

- ***Library***. Displays the ScienceLogic Library that you selected to align to the webhook receiver. Click **[Change Selected Library]** to select a different ScienceLogic Library.
- ***Import Module***. Type the Python handler module that you want to import from the selected ScienceLogic Library. The Python handler module consists of the name of the selected ScienceLogic Library as it appears in the ***Library*** field above, followed by the handler module name, separated by a period, in the following format:

  ```
  <Library name>.<handler module name>
  ```

  For example: `webhook_handler_library.example_handlers`
- ***Import Handler***. Type the name of the Python handler function that you want to import from the selected ScienceLogic Library.

6. Click **[Save]**.

TIP: To test that the webhook receiver is working, you can send an example test request by running the following command through the terminal, and then checking the **webhook_collector.log** file to view the results:

```
curl -XPOST -k <webhook_url> -d {} -H 'Content-Type: application/json' -vvv
```

Creating a Webhook Receiver from the Monitoring Policies Page

1. On the **Devices** page, select *the device that you want to align to the new webhook receiver* and click its **[Monitors]** tab.
2. Click the **[Create]** button and select *Create Webhook Receiver*. The **Create New Webhook** modal appears.
3. Select *the ScienceLogic Library that contains the webhook handler function* by clicking its library icon (). The **Create New Webhook** modal appears.
4. Complete the following fields:
   - ***Webhook Name***. Type a unique name for the webhook receiver.
   - ***Webhook URL Suffix***. Type a unique URL suffix for the webhook receiver.
   - ***Available Webhook URL***. Displays the auto-generated full URL of the webhook receiver. The webhook URL consists of the IP address and port number of the Message Collector or All-In-One Appliance that is associated with the selected device's collector group, the static URL fragment "/api/v1/webhook", and the webhook URL suffix, in the following format:

     ```
     https://<IP address>:<port number>/api/v1/webhook/<webhook URL suffix>
     ```

     For example: `https://10.2.20.56:8888/api/v1/webhook/test_webhook_url`

     NOTE: For Skylar One to auto-generate the full webhook URL, you must have already set up and enabled the webhook collector service on the associated Message Collector or All-In-One Appliance.

     NOTE: If the selected device is aligned to a collector group that includes multiple Message Collectors, then multiple URLs appear in this field, as Skylar One will auto-generate a URL for each Message Collector.

   - ***Library***. Displays the ScienceLogic Library that you selected to align to the webhook receiver. Click **[Change Selected Library]** to select a different ScienceLogic Library.
   - ***Import Module***. Type the Python handler module that you want to import from the selected ScienceLogic Library. The Python handler module consists of the name of the selected ScienceLogic Library as it appears in the ***Library*** field above, followed by the handler module name, separated by a period, in the following format:

     ```
     <Library name>.<handler module name>
     ```

     For example: `webhook_handler_library.example_handlers`
   - ***Import Handler***. Type the name of the Python handler function that you want to import from the selected ScienceLogic Library.

5. Click **[Save]**.

Editing and Deleting Webhook Receivers

You can edit and delete existing webhook receivers from the **Webhooks** page (Registry > Monitors > Webhooks).

To edit a webhook receiver:

1. Go to the **Webhooks** page (Registry > Monitors > Webhooks).
2. Locate the webhook receiver that you want to edit and click its wrench icon (🔧). The **Editing Webhook** modal appears.
3. In the **Editing Webhook** modal, change the values in one or more fields.
4. Click **[Save]** to save your changes.

To delete a webhook receiver:

1. Go to the **Webhooks** page (Registry > Monitors > Webhooks).
2. Locate the webhook receiver that you want to delete and then click its checkbox to select it.
3. Select *Delete Webhooks* from the ***Select Action*** drop-down menu.
4. Click the **[Go]** button.

Generating Events from Webhooks

For Skylar One to generate events from ingested webhook messages, you must create an event policy that looks for API messages that match strings from the webhook message.

To create an event policy for webhooks, follow the steps in the section *Defining an Event Policy*. When creating the policy, make sure to do the following:

- In the ***Event Source*** field, select *API*.
- In the ***Match String*** fields, type the string(s) you want to match from the webhook payload.

If configured correctly, events from webhook messages appear on the **Events** page, as well as in device logs.

Chapter 11

RSS Feeds and Events

Overview

Skylar One includes two types of RSS feeds that can be used with events:

- ***Custom RSS*** feeds that monitor events. You can define these in the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds).
- ***RSS feeds from external web sites***. You can view these feeds within Skylar One and configure Skylar One to create an event each time the external RSS feed is updated.

This chapter covers the following topics:

Viewing Events with an RSS Feed

With custom RSS feeds, you can view information about tickets and events without logging in to Skylar One. Custom RSS feeds from Skylar One can be viewed through a browser or through most free and commercially available feed viewers.

Defining a Custom RSS Feed

You can create a custom feed that filters tickets and events, and includes only tickets and events that you are interested in monitoring.

To define the RSS feed and specify the ticket and event criteria:

1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds).
2. Click the **[Refresh]** button to clear any values from the fields in the editor pane.
3. In the **Global Settings** pane, supply values in the following fields:
    - ***Feed Name***. Name of the feed. Can be any combination of alphanumeric characters, up to 64 characters in length.
4. In the **Custom RSS Feeds** page, under the **Ticket Settings** pane, you can specify the criteria that a ticket must meet to be included in the RSS feed. Supply values in the following fields:
    - ***Ticket Queues***. The RSS feed will include tickets only from the selected queues. You can select from a drop-down list of all ticket queues that you are allowed to view. By default, no queues are selected. To enable the RSS feed, you must select at least one queue. For more information on ticket queues, see *ticket queues*.
    - ***Assigned Only***. If you select this checkbox, the RSS feed will include only tickets that have been assigned.
    - ***Status***. The RSS feed will include only tickets with the status you select. The choices are:
        - *All*. Tickets of all statuses will be included in the RSS feed.
        - *Open*. Only tickets with a status of Open will be included in the RSS feed.
        - *Working*. Only tickets with a status of Working will be included in the RSS feed.
        - *Pending*. Only tickets with a status of Pending will be included in the RSS feed.
        - *Resolved*. Only tickets with a status of Resolved will be included in the RSS feed.
        - *O/W/P*. All tickets with a status of Open, Working, or Pending will be included in the RSS feed.
    - ***Minimum Severity***. The RSS feed will include only tickets with a severity equal to or greater than the severity you select. Choices are:
        - *Severity 5/Healthy*. All tickets will be included in the RSS feed.
        - *Severity 4/Notice*. Healthy tickets will **not** be included in the RSS feed.
        - *Severity 3/Minor*. Healthy and Notice tickets will **not** be included in the RSS feed.
        - *Severity 2/Major*. Healthy, Notice, and Minor tickets will **not** be included in the RSS feed.
        - *Severity 1/Critical*. Healthy, Notice, Minor, and Major tickets will **not** be included in the RSS feed.

5. In the **Custom RSS Feeds** page, under the **Event Settings** pane, you specify the criteria that an event must meet to be included in the RSS feed. Supply values in the following fields:
    - ***For Organization***. This box will contain a list of all organizations about which you are allowed to view information. Select one or more organizations for which you want to view event information. (To select multiple organizations, hold down the **<Ctrl>** key while clicking.) The RSS feed will include only events assigned to the selected organization(s). Users must select at least one organization from this list.
    - ***Unacknowledged Only***. Select this checkbox to include only unacknowledged events in the RSS feed.
    - ***Age Less Than***. The RSS feed will include only events with an age equal to or less than the selected age.
    - ***Minimum Severity***. The RSS feed will include only events with a severity equal to or greater than the severity you select. Choices are:
        - *Healthy*. All events will be included in the RSS feed.
        - *Notice*. Healthy events will **not** be included in the RSS feed.
        - *Minor*. Healthy and Notice events will **not** be included in the RSS feed.
        - *Major*. Healthy, Notice, and Minor events will **not** be included in the RSS feed.
        - *Critical*. Healthy, Notice, Minor, and Major events will **not** be included in the RSS feed.
    - ***Device Group Filter***. The RSS feed will include only events associated with devices in the selected device group. In this field, you can select a device group from a list of all device groups you are allowed to view. For more information on Device Groups, see the manual on ***Device Groups and Templates***.
6. Click **[Save]** to save the new Custom RSS Feed.

Editing a Custom RSS Feed

You can edit an existing custom RSS feed and make changes to the criteria for tickets and events. You can also delete an existing RSS feed.

To edit an existing RSS feed:

1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds)
2. In the **Custom RSS Feeds** page, go to the RSS Feeds registry pane, at the bottom of the page.
3. Click the wrench icon (🔧) of the RSS feed you want to edit.
4. The top pane is populated with values from the selected RSS feed. You can edit one or more values.
5. Click **[Save]** to save your changes.

To delete an existing custom RSS feed:

1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds).
2. In the **Custom RSS Feeds** page, go to the RSS Feeds registry pane, at the bottom of the page.
3. Click the delete icon (🗑) of the RSS feed you want to delete. Skylar One deletes the RSS feed.

Viewing a Custom RSS Feed

You can view a custom RSS feed in a browser window or in a third-party viewer.

To view an RSS feed from the **Custom RSS Feeds** page:

1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds).
2. In the **Custom RSS Feeds** page, go to the RSS Feeds registry pane, at the bottom of the page.
3. Click the RSS icon ( ) of the RSS feed you want to view.
4. The RSS feed displays in a browser window.
    - The window displays a list of all entries in the feed, and details on each entry (event or ticket).
    - Clicking on the ticket heading displays a new window containing the Ticket Report for that ticket.
    - In the Ticket Report, clicking on the "click here to login" link takes you to the Skylar One appliance where the ticket resides. Depending upon key privileges, you can then edit the ticket. Any changes to the ticket are dynamically updated in the RSS feed.

To view the RSS feed in a third-party viewer:

1. Perform the steps above to view the RSS feed in the **Custom RSS Feeds** page.
2. Copy the URL from the URL field in the browser window.
3. Launch the RSS viewer.
4. Paste the URL into the RSS viewer. The URL includes a key for authentication, so the viewer can retrieve the feed from Skylar One.

Defining an External RSS Feed to Trigger Events

You can view and monitor external RSS feeds from Skylar One. In Skylar One, you define one or more RSS feeds to monitor. You can then view the feeds directly from Skylar One. When new items are added to the feed, Skylar One can generate an event to notify users. With Skylar One, you can:

- Monitor RSS feeds for new updates
- View RSS feeds
- Trigger events based on RSS feeds

You can monitor the following types of RSS feeds with Skylar One:

- RSS 1.0+
- RSS 2.0+
- ATOM

The following sections describe how to define and/or edit an external RSS feed to monitor, and how to view the feed from within Skylar One.

Viewing the List of Monitored RSS Feeds

The **RSS News Feed Manager** page displays a list of existing policies for monitoring RSS feeds. For each policy, the page displays:

> **TIP:** You can sort the list by a column's values by clicking on its column heading. You can also filter the items on the page by typing or selecting filter options in one or more of the filters found above the columns. For more information, see the topic on *Filtering Inventory Pages*.

- ***Channel Name***. Name of the RSS feed that is monitored by the policy.
- ***Feed URI***. URL of the RSS feed.
- ***Organization***. Organization to associate with this monitoring policy.
- ***Feed Count***. Specifies the number of articles in the feed.
- ***State***. Specifies whether Skylar One is currently retrieving data for the policy. Choices are *Enabled* or *Disabled*.
- ***Collector***. Name of the Data Collector that collects data for the policy.
- ***Edit User***. The user who created or last edited the policy.
- ***Edit Date***. Date the policy was created or last edited.

Defining an RSS Feed to Monitor

In the **RSS News Feed Manager** page (Events > RSS Feeds), you can define RSS feeds that you want to monitor with Skylar One. To monitor an RSS feed:

1. Go to the **RSS News Feed Manager** page (Events > RSS Feeds).
2. In the **RSS News Feed Manager** page, click the **[Create]** button.
3. The **RSS Feed Editor** modal appears.
4. In the **RSS Feed Editor** modal, supply a value in each of the following fields:
    - ***Channel Name***. Name of the RSS feed. If you choose to trigger events based on updates to the RSS feed, this value appears in the ***Entity*** field of the event.
    - ***RSS URL***. URL of the RSS feed.
    - ***Organization***. Organization to associate with this monitoring policy.
    - ***Collection***. Specifies whether Skylar One should retrieve data from the RSS feed. Choices are *Enabled* or *Disabled*.
    - ***Eventing***. Specifies whether Skylar One creates an event when a new article is detected in the RSS feed. Select from the drop-down list:

- *None*. No event appears when new articles are detected.
- *Event Console*. A description of the new article appears as an event in the **Event Console** page.

- ***Severity***. If new articles trigger an event in the **Event Console** page, specifies the severity of the event. Select from the drop-down list of all event severities.
- ***Collector***. Specifies the Data Collector that monitors the RSS feed. Select from the available choices in the drop-down list. For All-In-One Appliances, this field does not apply.

5. Click **[Save]** to save the policy and monitor the RSS feed.

Editing a Monitored RSS Feed

From the **RSS News Feed Manager** page (Events > RSS Feeds), you can edit an existing monitoring policy for an RSS feed. To do this:

1. In the **RSS News Feed Manager** page, click the wrench icon ( ) of the monitored RSS feed you want to edit.
2. The **RSS Feed Editor** page appears, populated with values from the monitored RSS feed you selected.
3. In the **RSS Feed Editor** page, you can edit the values in one or more fields. For more information, see the section on *Defining an RSS Feed to Monitor*.
4. Click **[Save]** to save your changes to the policy.

Viewing Articles from an RSS Feed

From the **RSS News Feed Manager** page (Events > RSS Feeds), you can view a list of articles retrieved from a monitored RSS feed. To do this:

1. In the **RSS News Feed Manager** page, click the page icon ( ) of the monitored RSS feed you want to view.
2. The **Article Catalog** page appears.
3. In the **Article Catalog** page, you can select and view articles from a monitored RSS feed. To view an article, click its globe icon.

Chapter 12

Reports for Events

Overview

Skylar One provides the following types of reports on events:

- ***Event Statistics report from the Event Console page in the classic Skylar One user interface***. This report displays information about all active events on all devices in Skylar One.
- ***Event Statistics report from the Device Reports panel, in Viewing Events page***. This report displays information about all events, both active and cleared, that have occurred on the selected device.
- ***Reports in Reports > Quick Reports***. These reports are customizable and display detailed information about events.
- ***Event Overview from the System tab***. This report provides a graphical overview of all events in Skylar One.
- ***Event Statistics from the System tab***. This report displays a graph of the number of events processed by a selected All-In-One Appliance, Database Server, Data Collector, or Message Collector.

This chapter covers the following topics:

Event Statistics in the Event Console Page

The **Event Statistics** modal in the classic Skylar One user interface displays a report on all events you are allowed to view. Administrator users can view all events. Non-administrator users can view events that are aligned with the same organizations as their user account. For example, a user who is a member of the "Network" organization and the "NOC" organization can view events associated with those two organizations.

You can drill down to get more information about a specific event or about events on a specific element.

To access and view the Event Statistics report:

1. Go to the **Event Console** page (Events > Classic Events, or the Events tab in the classic user interface).
2. In the **[Actions]** drop-down list, select ***Event Statistics***. The Event Statistics report appears.
3. Initially, the **Event Statistics** page displays the bar graph "All Event Types for All Elements" for the past day.
4. The "All Event Types for All Elements" graph displays:
    - All events that have occurred on all elements (that you are allowed to view) for the past day. You can select the **[7 Days]** button or the **[30 Days]** button to change the time period.
    - Each event, represented by a colored bar. Mousing over a bar displays the name of the event and the number of occurrences.
    - The event name on the x-axis.
    - The number of occurrences on the y-axis.
    - A table, listing each event and the number of occurrences.
5. Clicking on a bar displays the "Single Event Type on All Elements" bar graph.
6. The "Single Event Type on All Elements" graph displays:
    - Each occurrence of the selected event on all elements (that you are allowed to view) during the selected time period.
    - Each element is represented by a colored bar. Mousing over a bar displays the name of the element and the number of occurrences.
    - The element name on the x-axis.
    - The number of occurrences on the y-axis.
    - The graph also includes a table of each element where the event occurred and the number of occurrences.
7. Clicking on a bar displays the "Single Event Type For Selected Device" bar graph.
8. The "Single Event Type For Selected Device" graph displays:
    - The number of times the selected event occurred on the selected device during the selected time period.

- Each occurrence of the selected event on the selected element during the selected time period.
- Mousing over a bar displays the name of the element and the number of occurrences.
- The date on the x-axis.
- The number of occurrences on the y-axis.
- The graph also includes a table, listing the device, the events, and the number of occurrences.

9. Clicking on the bar displays the *Events page for the device*.

Event Statistics for a Single Device

You can view an Event Statistics report for a single device. This report displays information about all events, both active and cleared, that have occurred on the selected device.

To view and access the Event Statistics report for a single device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. On the **Device Manager** page, select the bar graph icon ( ) for the device for which you want to view Event Statistics.
3. Skylar One displays the **Device Reports** panel for the device. In the **Device Reports** panel for the device, click the **[Events]** tab.
4. On the **Viewing Events** page, click the **[Stats]** button. The **Event Statistics** modal appears.
5. By default, the **Event Statistics** page displays the graph "All Event Types for the Last Month." This graph displays all events that have occurred on the device this month. This graph displays:
    - All events that have occurred on the device in the last month. You can select the **[7 Days]** button to change the time period.
    - Each event, represented by a colored bar. Mousing over a bar displays the name of the event and the number of occurrences.
    - The event name on the x-axis.
    - The number of occurrences on the y-axis.
    - A table, listing each event and the number of occurrences.
    - Additionally, clicking on a button displays all events that have occurred on the device during the selected time period.
6. Clicking on a bar displays the "Event Type" graph. This graph displays:
    - Each occurrence of the selected event on the element during the time period.
    - The name of the event, total number of occurrences, and date of the selected occurrence (when mousing over a bar).
    - The element name on the x-axis.
    - The number of occurrences on the y-axis.

- A table, listing each occurrence of the event on the device, the date of the occurrence, and number of total occurrences.

Event Reports in the Reports Tab

On the **Reports** page (Reports > Reports), you can create custom reports as well as view predefined reports. Skylar One includes many predefined reports under ***Run Report > Events*** on the NavBar that are ready to be generated and viewed. Three such reports are the Event Clear Map report, the Event Detections report, and the Unique Event Detections report.

- The ***Event Clear Map*** report displays a list of events that are defined to auto-clear. For each event defined to auto-clear, the report displays the correlating event that will cause the auto-clear. Auto-clear means that when a specific event occurs, Skylar One automatically removes the current event from the **Events** page. For example, suppose you have an event "Device not responding to ping". You could define the event as auto-clear when the event "Device now responding normally to ping" occurs. During the next polling session, if the event "Device now responding normally to ping" occurs, the auto-clear feature could automatically clear the original event "Device not responding to ping" from the **Events** page.
- The ***Event Detections*** report displays the number of occurrences of one or more events during the selected time period. The report can display either the total number of occurrences for each selected event or the occurrences per device. Users can choose to group events by organization and device.
- The ***Unique Event Detections*** report displays the number of unique occurrences of one or more events during the selected time period. The report contains two "sheets": Data and Control. The Data sheet contains information for each event detection such as the date and number of events, device, and event type. The Control sheet displays information such as a description, report version, date of report generation, organizations, devices, and duration.

NOTE: For details on these event reports and event-related reports in the **Reports** page (Reports > Reports), see the section on *default reports for events*.

NOTE: You can open the root cause report for all Skylar Automated RCA events by clicking the **[View Full Root Cause Report]** in Skylar Automated RCA button at the top of the **Reports** page.

Input and Output for Quick Reports comply with multi-tenancy. That is, only users of type ***Administrator*** can view options, devices, and policies for all devices. Users of type ***User*** can view options, devices, and policies for their own organization(s) only, both when selecting options and in the generated report.

Event Clear Map Report

To generate and view the Event Clear Map report:

1. Go to the **Run Quick Report** page for the Event Clear Map report (Reports > Run Report > Events > Event Clear Map).
2. Supply values in the following fields:

- ***Sort By***. Specifies how the report is organized. Choices are:
    - *Severity*. Events are grouped by severity.
    - *Event Name*. Events are listed alphabetically by event name. The secondary sort is by severity.
    - *Event ID*. Events are listed by event policy ID. Event ID is a unique numerical ID assigned by Skylar One to each event policy.
- ***Show At or Above***. Filter the events to include in the report. Only events of the selected severity or of a greater severity are included in the report. Choices are:
    - *Critical*. Only events with "Critical" severity are included in the report.
    - *Major*. Events with "Major" and "Critical" severities are included in the report.
    - *Minor*. Events with "Minor," "Major," and "Critical" severities are included in the report.
    - *Notice*. Events with "Notice," "Minor," "Major," and "Critical" severities are included in the report.
    - *Healthy*. All events are included in the report, regardless of severity.
- ***Show Events***. Specifies whether to include only events that are defined as auto-clear or to include both events that are defined as auto-clear and events that are not defined as auto-clear. Choices are:
    - *That are cleared*. The generated report includes only events that are defined as auto-clear.
    - *Including non-cleared*. The generated report includes both events that are defined as auto-clear and events that are not defined as auto-clear.
- ***Optional Columns***. Specifies optional columns of event information to include in the report. If you do not select any additional columns in this field, the report includes the following default columns: ***Cleared Event***, ***Severity***, ***Direction***, and ***Clearing Event***.
- ***Output Format***. Select the format in which Skylar One saves the generated report. Choices are:
    - *ODF Spreadsheet*. Displays the output in the OpenOffice spreadsheet application.
    - *Microsoft Excel*. Displays the output in an .xlsx file.
    - *Web page*. Displays the output in an .html file.
    - *Adobe Acrobat*. Displays the output in a .pdf file.
- **[Generate]**. This button generates the report, using the parameters you specified in this page.

For each event that has been defined to auto-clear and that meets the selection criteria, the report can include the following columns:

NOTE: If you do not select any Optional Columns in the ***Optional Columns*** field, the report contains only the default columns: ***Cleared Event***, ***Severity***, ***Direction***, and ***Clearing Event***.

- ***Cleared Event***. The name of the event.
- ***Severity***. The severity of the event. For more information about severity values, see the section *Understanding Event Severity*.
- ***Source***. Specifies the source for the event. For more information, see the section on *Event Sources*.
- ***Dynamic Application Name***. If applicable, the Dynamic Application that contains the alert that triggered the original event.
- ***Cleared Source Text***. Event messages from the event that was cleared.
- ***Expires***. The time in which the active event is cleared automatically if there is no reoccurrence of the event.
- ***Direction***. Specifies whether the two events clear each other (<==0==>) or whether the event to the right clears the event to the left (0==>).
- ***Clearing Event*** . Name of the event defined to auto-clear the event in ***Cleared Event***.

Event Detections Report

To generate and view the Event Detections report:

1. Go to the **Run Quick Report** page for the Event Detections report (Reports > Run Report > Events > Event Detections).
2. Supply a value in each of the following fields:
    - ***All Organizations***. All events associated with all organizations are included in the report.
    - ***Organizations***. This list contains an entry for each organization in Skylar One. Events associated with each selected organization are included in the report.
        - To select all organizations, select the *All Organizations* checkbox.
        - To select individual organizations, unselect the *All Organizations* checkbox, then expand the organization and select each organization's checkbox.
    - ***All Events***. All events are included in this report.
    - ***Events***. This list contains an entry for each event in Skylar One.
        - To select all events, select the *All Events* checkbox.
        - To select an event, unselect the *All Events* checkbox, then highlight an entry in the list.
        - To select multiple events, unselect the *All Events* checkbox, then hold down the **CTRL** key while clicking on each event that you want to select.
    - ***Report Options***. Specifies the amount of information to include in the report.

    - *Show Details*. Displays both the summary report and a detailed report, grouped by event name or by organization and device.
- ***Separated By***. If you selected *Show Details* in the ***Report Options*** field, specifies how the report is organized. Choices are:
    - *Event Name*. Events are listed alphabetically by event name.
    - *Org/Device*. Events are grouped first by organization and secondly by device.
- ***Optional Columns***. Specifies optional columns of event information to include in the report. If you do not select any additional columns in this field, the report includes the following default columns: ***Event Name***, ***Detection Count***.
- ***Report Span***. Specifies the time interval to use to select data for this report. The ***Duration*** field uses this interval. The choices are:
    - *Daily*
    - *Weekly*
    - *Monthly*
- ***Starting***. Specifies the relative start date for the report. Data from that relative start date through the date determined by the ***Duration*** field are included in the report.
- ***From Date***. Specifies the absolute start date for the report. Data from that absolute start date through the date determined by the ***Duration*** field are included in the report.
- ***Duration***. Specifies the number of days, weeks, or months to include in the report. The increment displayed in this field depends upon the value selected in the ***Report Span*** field.
- ***Output Format***. Select the format in which Skylar One saves the generated report. Choices are:
    - *ODF Spreadsheet*. Displays the output in the OpenOffice spreadsheet application.
    - *Microsoft Excel*. Displays the output in an .xlsx file.
    - *Web page*. Displays the output in an .html file.
    - *Adobe Acrobat*. Displays the output in a .pdf file.
- **[Generate]**. This button generates the report, using the parameters you specified in this page.

For each event that has been selected to include in the report, the following is displayed:

- ***Event Name***. Name of the event.
- ***Detection Count***. Number of times the event occurred.
- ***Device ID.*** The Device ID where the event occurred.
- ***Organization***. Organization associated with the event.
- ***Device Name.*** The Device Name where the event occurred.
- ***IP Address.*** The IP address of the device where the event occurred.
- ***Severity.*** The severity (Healthy, Notice, Minor, Major, or Critical) of the event.
- ***Detection Count.*** The total number of occurrences of the event during the selected time span.

- ***First Occurrence.*** The date on which the event first occurred during the selected time span.
- ***Last Detected.*** The date on which the event last occurred during the selected time span.

Unique Event Detections Report

This report contains two "sheets": Data and Control. The Data sheet contains information for each event detection such as the date and number of events, device, and event type. The Control sheet displays information such as a description, report version, date of report generation, organizations, devices, and duration.

To generate and view the Unique Event Detections report:

1. Go to the **Run Quick Report** page for the Unique Event Detections report (Reports > Run Report > Events > Unique Event Detections).
2. Supply a value in each of the following fields:

- ***Device Selection***: Select the devices that you want to appear in the report. The choices are:
    - *All devices*. Select this checkbox if you want all devices in the system to be included in this report.
    - *Organizations*. If the ***All devices*** checkbox is not selected, select one or more organizations. The report contains only the devices in the organizations you select. You can further filter the list of devices to include in the report by selecting devices in the ***Devices by Organization*** field.
    - *Select individual devices*. If the ***All devices*** checkbox is not selected, the ***Select individual devices*** checkbox is available. Select this checkbox if you would like to use the ***Devices by Organization*** field to select the individual devices to include in the report.
    - *Devices by Organization*. This field displays a list of all devices in the organizations selected in the ***Organizations field***. If the ***Select individual devices*** checkbox is selected, you can select one or more devices to include in the report.
- ***Device Group Selector***: Select the device groups that you want to appear in the report. The choices are:
    - *All Device Groups*. Select this checkbox if you want to include all device groups in the report.
    - *Device Groups*. If the ***All Device Groups*** checkbox is not selected, select one or more device groups. The report contains only the devices in the device groups you select.
- ***Separated By***. Group devices by ***Organization***, ***Device Group***, or ***Device***.
- ***Sort by***. Select the checkboxes to sort the report by ***Organization*** or ***Device***.
- ***Event Types***. Select the types of events that you want to appear in the report. The choices are:
    - *All events*. Select this checkbox to include all event types.
    - *Events*. If the ***All events*** checkbox is not selected, select one or more event types. The report contains only the event types that you select.
- ***Report Span***. Specifies the time interval to use to select data for this report. The ***Duration*** field uses this interval. The choices are:

    - *Daily*
    - *Weekly*
    - *Monthly*
- ***Starting***. Specifies the relative start date for the report. Data from that relative start date through the date determined by the ***Duration*** field are included in the report.
- ***From Date***. Specifies the absolute start date for the report. Data from that absolute start date through the date determined by the ***Duration*** field are included in the report.
- ***Duration***. Specifies the number of days, weeks, or months to include in the report. The increment displayed in this field depends upon the value selected in the ***Report Span*** field.
- ***Timezone***. Specifies the timezone conversion for the dates and times that display in the report.
- ***Report Sections***. Specify how the report is arranged. Select whether you want the report to display ***Details Only***, ***Totals Only***, or ***Both***.
- ***Output Format***. Select the format in which Skylar One saves the generated report. Choices are:
    - *ODF Spreadsheet*. Displays the output in the OpenOffice spreadsheet application.
    - *Microsoft Excel*. Displays the output in an .xlsx file.
    - *Web page*. Displays the output in an .html file.
    - *Adobe Acrobat*. Displays the output in a .pdf file.
- **[Generate]**. This button generates the report, using the parameters you specified in this page.

For each unique instance of an event, the report displays:

- ***Device***. Specifies the device name where the event occurred.
- ***Event Type***. Specifies the event description of the event.
- ***Time Period.*** Specifies the number of times the event occurred during the time period.
- ***Total***. Specifies the total number of times the event occurred on the specified device.
- ***Sum for Organization***. Displays total number of unique events that occurred during the time period for each organization.
- ***Sum for Device Group***. Displays total number of unique events that occurred during the time period for each device group.
- ***Sum for Device***. Displays total number of unique events that occurred during the time period for each device.

Event Overview Report

The **Event Overview** page (System > Monitor > Event Overview) provides a graphical overview of all events in Skylar One. The **Event Overview** page displays the number of events by severity, the most common event types, and the mean time-to-resolution.

Setting the Date for Reports

The **Event Overview** page includes a ***Select Date*** drop-down list in the upper right of the page. From this drop-down, you can define the date for the reports on this page.

- ***Select Date***. Allows you to select a date. Skylar One generates the reports on this page using the selected date as the current date. If you do not select a value in this field, the default date is today's current date.

> **NOTE:** When you select a date, Skylar One uses that date as "today's date" to generate reports. So results for "24 hours" are for the 24-hours of the selected date. Results for "7 Days" are for the selected date and the six days preceding it, etc.

Event Statistics

The **Event Statistics** page (System > Monitor > Event Statistics) displays a graph of the number of events processed by a selected All-In-One Appliance, Database Server, Data Collector, or Message Collector. To generate the report, you select from a list of ScienceLogic servers and then select an event type from a list of event types.

Defining the Date Range

- **[Presets]**. Allows you to select from a list of pre-defined time spans for the report.

Fields

To generate the report, supply values in the following fields:

- ***EM7 Server***. This field does not appear on All-In-One Appliances. Select from the list of all Database Servers, Data Collectors, and Message Collectors.
- ***Event Type***. Select from the list of event types. For more information, see the section on *Event Sources*.

The Graph

The graph displays the average number of events processed by the selected ScienceLogic server, for the selected duration.

- The y-axis displays the average number of events.
- The x-axis displays time. The increments vary, depending upon the selected date range (from the ***Preset*** buttons).
- Mousing over any point in any line displays the high, low, and average value at that time-point in the

Data Table pane.

- You can use your mouse to scroll the report to the left and right.

Chapter 13

Settings That Affect Events

Overview

In Skylar One, you can configure the default behavior for all events by defining data retention settings and system settings.

This chapter covers the following topics:

Data Retention Settings That Affect Events

To define data retention settings for events:

1. Go to the **Data Retention Settings** page (System > Settings > Data Retention).
2. On the **Data Retention Settings** page, use the ***Event Logs*** field to select the number of days that Skylar One should store event logs. Event history data is used to generate the **Event Overview** page (System > Monitor > Event Overview).

System Settings That Affect Events

To define system settings for events:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. On the **Behavior Settings** page, the following system setting affects events:

- ***Event Clearing Mode***. Describes how clearing an event affects correlated events. Options include:
    - *Clear All in Group*. When the parent event is cleared, clear all events correlated with the parent event. This is the default behavior.
    - *Clear Selected Only*. Clear only the selected events. If a parent event is cleared, the previously suppressed, correlated events appear on the **Events** page (or the **Event Console** page in the classic Skylar One user interface).

System Settings That Affect Event Tickets

The behavior of the *Create Ticket* option on the **Events** page (or the life-ring icon ( ) in the **Event Console** page in the classic Skylar One user interface) is determined on the **Behavior Settings** page (System > Settings > Behavior) in the classic Skylar One user interface. To change this behavior:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Select from the following options in the ***Event Console Ticket Life Ring Button Behavior*** field:
    - *Create/View EM7 Ticket*. When you select the *Create Ticket* option or click the life-ring icon ( ) for an event, Skylar One displays the **Ticket Editor** page, where you can define a Skylar One ticket and automatically associate it with the selected event. This is the default behavior.
    - *Create/View External Ticket*. If an external ticket is aligned with an event, when you select the *Create Ticket* option or click the life-ring icon ( ) for that event, Skylar One spawns a new window and displays the external ticket (as specified in the `force_ticket_uri` database field). If an external ticket is not yet aligned with an event, when you select the *Create Ticket* option or click the life-ring icon ( ) for that event, Skylar One sets a "request" flag for the ticket and displays an acknowledgment that a new ticket has been requested. You can then use the "request" in run book logic to create the ticket on the external system.
3. Click **[Save]** to save your changes.

> **NOTE:** For more information on events and external tickets, see *integrating events and external tickets*.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010