



Events

SL1 version 8.12.1

Table of Contents

| | |
|---|-----------|
| What is an Event? | 1 |
| What is an Event? | 2 |
| How Are Events Triggered? | 2 |
| Viewing Events | 3 |
| Event Correlation | 4 |
| Defining Events | 5 |
| Event States | 5 |
| Viewing Events | 7 |
| Searching and Filtering the List of Events | 7 |
| Viewing Events by Organization and Business Service | 7 |
| Filtering Events by Severity | 9 |
| Filtering for Masked Events | 10 |
| Refreshing the Events Page | 10 |
| Customizing the Events Page | 11 |
| Viewing Automation Actions | 12 |
| Event Throttling | 13 |
| Responding to Events | 14 |
| Responding to Events | 15 |
| Working with Events | 15 |
| Selecting Multiple Events | 15 |
| Acknowledging and Clearing Events | 16 |
| Viewing and Editing Event Notes | 16 |
| Using the Event Drawer | 17 |
| Working with the Tools Pane | 18 |
| Creating a Ticket | 19 |
| Using the Event Investigator | 20 |
| Events and Tickets | 22 |
| Creating a Ticket from an Event | 23 |
| Event Ticket Behavior Settings | 26 |
| Event Correlation and Parent and Child Events | 28 |
| Event Correlation | 29 |
| Defining Parent and Child Devices | 30 |
| Device Categories that Don't Support Children Devices | 31 |
| Defining Suppressing and Suppressible Events | 32 |
| Event Categories | 35 |
| Assigning an Event Category to an Event | 36 |
| Creating an Event Category | 37 |
| Editing an Event Category | 38 |
| Viewing the List of Event Categories | 39 |
| Filtering the List of Event Categories | 40 |
| Special Characters | 41 |
| Deleting One or More Event Categories | 45 |
| Defining and Editing Event Policies | 46 |
| How SL1 Generates Events | 47 |
| Viewing the List of Event Policies | 48 |
| Filtering the List of Event Policies | 50 |
| Special Characters | 52 |
| Defining an Event Policy | 56 |
| Defining Basic Event Parameters in the Policy Tab | 57 |
| Defining Pattern Matching and Advanced Behavior in the Advanced Tab | 60 |



| | |
|--|------------|
| Defining Event Suppressions in the Suppressions Tab | 67 |
| Defining an Event Policy for a Specific Interface | 69 |
| Defining Custom Severity for an Interface | 71 |
| Editing an Event Policy | 73 |
| Best Practices for Event Definitions | 75 |
| Event Notification and Event Automation | 77 |
| Automation Policies | 78 |
| Action Policies | 79 |
| Creating Automation Policies and Action Policies | 79 |
| Events from Email | 80 |
| Configuring Events from Email | 80 |
| RSS Feeds and Events | 81 |
| Viewing Events with an RSS Feed | 82 |
| Defining a Custom RSS Feed | 82 |
| Editing a Custom RSS Feed | 84 |
| Viewing a Custom RSS Feed | 85 |
| Defining an External RSS Feed to Trigger Events | 86 |
| Viewing the List of Monitored RSS Feeds | 87 |
| Defining an RSS Feed to Monitor | 87 |
| Editing a Monitored RSS Feed | 88 |
| Viewing Articles from an RSS Feed | 89 |
| Performing Administrative Tasks on One or More Monitored RSS Feeds | 90 |
| Reports for Events | 92 |
| Event Statistics for a Single Device | 93 |
| Event Reports in the Reports Tab | 94 |
| Event Clear Map Report | 94 |
| Event Detections Report | 97 |
| Unique Event Detections Report | 99 |
| Event Overview Report | 102 |
| Setting the Date for Reports | 102 |
| Number of Events by Severity | 102 |
| Most Common Event Types | 103 |
| Mean Time-to-Resolution | 103 |
| Event Statistics | 103 |
| Defining the Date Range | 104 |
| Fields | 104 |
| The Graph | 104 |
| Settings that Affect Events | 106 |
| Data Retention Settings that Affect Events | 107 |
| System Settings that Affect Events | 107 |

What is an Event?

Overview

This chapter describes how to use SL1 to manage events that appear on the **Events** page.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

| | |
|--|---|
| <i>What is an Event?</i> | 2 |
| <i>How Are Events Triggered?</i> | 2 |
| <i>Viewing Events</i> | 3 |
| <i>Event Correlation</i> | 4 |
| <i>Defining Events</i> | 5 |
| <i>Event States</i> | 5 |

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 SL1.

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.

SL1 generates log messages from incoming trap and syslog data, and also when SL1 executes user-defined policies. SL1 then uses these log messages to generate events. SL1 examines each log message and compares it to each event definition. If a log message matches an event's definition, SL1 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.

SL1 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?

SL1 examines log messages to generate instances of events. When SL1 monitors a system, SL1 generates log messages when the collected data meets user-defined thresholds. Additionally, a monitored system can send log messages to SL1 asynchronously. SL1 examines each log message and compares it to each existing event definition. If a log message matches an event's definition, SL1 generates an event instance and displays the event on the **Events** page.

SL1 includes logic that correlates and groups (rolls-up) related logs and messages into a single event. SL1 includes pre-defined events for many syslog, internal, trap, and dynamic messages.

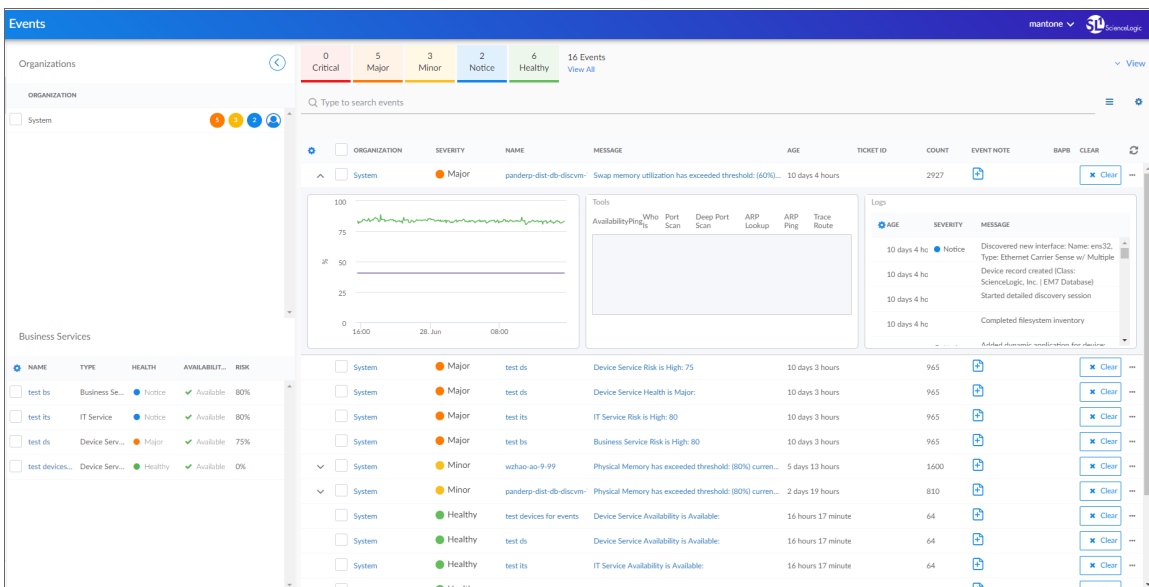
SL1 generates events by collecting log messages from the following sources:


- **Syslog**. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices like MoMs. A syslog is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.
- **Internal**. Message is generated by a ScienceLogic process. The message is about the SL1 system itself, instead of the devices that the SL1 system monitors.
- **Trap**. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like MoMs. An SNMP trap is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.

- **Dynamic.** Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users 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. SL1 examines each new message in the device log and determines if the message matches an event definition. If it does, SL1 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 F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the SL1 system inserts a message in the associated device's log files, and the SL1 system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
- **Email.** Message is generated by an email message sent to SL1. For more information on generating events with email messages, see the **Events from Email** chapter.
- **API.** Message was 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 manual **Run Book Automation**. For more information on snippet Dynamic Applications, see the manual **Snippet Dynamic Application Development**. For more information on the ScienceLogic API, see the manual **Using the ScienceLogic API**.

Viewing Events

The [Events] page displays a list of currently active events, from critical to healthy. From this tab 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 an event that is **aligned** or associated with a device, you can click the down-arrow icon () for that event to open the **Event Drawer**. The Event Drawer is a drop-down panel that displays additional data about that event, including a Vitals widget, Tools, and Logs.

In the **Message** column, you can click the linked text to view the **Event Investigator** page for an event aligned with a device. The **Event Investigator** page includes sections for Probable Cause & Resolution, Tools, Logs, Notes, Assets, a Vitals widget, and a list of masked events. All events have corresponding **Event Investigator** pages.

In the **Name** column, you can click the linked text to view the **Device Investigator** page for the device aligned with the event. If the event does not have a device aligned with it, the link goes to the **Organization** page aligned with the event.

In the **Organization** column, you can click the linked text to view the **Organization** page aligned with this event. Similarly, you can click the linked text in the **Ticket ID** column to view a ticket aligned with an event.

TIP: To adjust the time interval for updating the list of events, click the **View** menu, select *Enable auto-refresh*, and select the refresh interval. You can also manually update the list of events by clicking the Refresh icon () at the top right of the list of events.

Event Correlation

In SL1, 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 will be 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 SL1 to more efficiently align events.

SL1 performs some event correlation automatically. You can also manually configure devices and events so that SL1 treats specified events as parent events and specified events as child events. For more details, see the chapter on [event correlation](#).

Defining Events

The **Event Policy Manager** page (Events > Event Policies) displays a list of all event policies in SL1. This page also allows you to define new event definitions and edit existing event definitions.

| Event Policy Name | Type | State | P-Pack | Severity | Weight | ID | Expiry | Time | Thresh | Edited By | Last Edited | External ID | Category |
|--|---------|---------|--------|----------|--------|------|---------|--------|--------|-----------|---------------------|-------------|----------|
| 1. ADIC Global Status Failed | Dynamic | Enabled | Yes | Major | 0 | 2 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 2. ADIC Global Status OK | Dynamic | Enabled | Yes | Healthy | 0 | 4 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 3. ADIC Global Status Unknown | Dynamic | Enabled | Yes | Notice | 0 | 3 | 30 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 4. ADIC Tape Library Degraded | Dynamic | Enabled | Yes | Minor | 0 | 1 | 60 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 5. AKCP: AC Voltage sensor detects no current | Syslog | Enabled | Yes | Critical | 0 | 1288 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 6. AKCP: AC Voltage sensor now reporting Normal Status | Syslog | Enabled | Yes | Healthy | 0 | 1294 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 7. AKCP: DC Voltage High Warning | Syslog | Enabled | Yes | Major | 0 | 1299 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 8. AKCP: DC Voltage sensor High Critical | Syslog | Enabled | Yes | Critical | 0 | 1297 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 9. AKCP: DC Voltage sensor Low Critical | Syslog | Enabled | Yes | Critical | 0 | 1288 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 10. AKCP: DC Voltage sensor Low Warning | Syslog | Enabled | Yes | Major | 0 | 1300 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 11. AKCP: DC Voltage sensor returned to Normal Status | Syslog | Enabled | Yes | Healthy | 0 | 1301 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 12. AKCP: Dry Contact Sensor Low Critical | Syslog | Enabled | Yes | Critical | 0 | 1287 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 13. AKCP: Dry contact sensor now Normal | Syslog | Enabled | Yes | Healthy | 2 | 1292 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 14. AKCP: Humidity High Warning | Syslog | Enabled | Yes | Major | 0 | 1295 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 15. AKCP: Humidity Low Warning | Syslog | Enabled | Yes | Major | 0 | 1296 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 16. AKCP: Smoke Detector Alert! | Syslog | Enabled | Yes | Critical | 10 | 1293 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 17. AKCP: Smoke detector now Normal Status | Syslog | Enabled | Yes | Healthy | 4 | 1289 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 18. AKCP: Water Sensor has detected water | Syslog | Enabled | Yes | Critical | 0 | 1291 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 19. AKCP: Water sensor now Normal | Syslog | Enabled | Yes | Healthy | 0 | 1290 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 20. Aiteon: New Flash Enabled | Dynamic | Enabled | Yes | Notice | 0 | 36 | 30 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 21. Aiteon: Primary Power Supply Failure | Dynamic | Enabled | Yes | Major | 0 | 32 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 22. Aiteon: Primary Power Supply Healthy | Dynamic | Enabled | Yes | Healthy | 0 | 33 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 23. Aiteon: Redundant Power Supply Failure | Dynamic | Enabled | Yes | Major | 0 | 34 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 24. Aiteon: Redundant Power Supply Healthy | Dynamic | Enabled | Yes | Healthy | 0 | 35 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 25. APC: Batteries Do Not Need Replacement | Dynamic | Enabled | Yes | Healthy | 0 | 8 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 26. APC: Battery Charge Normal | Dynamic | Enabled | Yes | Healthy | 0 | 16 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 27. APC: Battery Run Time Remaining No Longer Critical | Dynamic | Enabled | Yes | Healthy | 0 | 10 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 28. APC: Battery Status | Dynamic | Enabled | Yes | Major | 0 | 15 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 29. APC: Calibration Test Completed | Dynamic | Enabled | Yes | Healthy | 0 | 29 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 30. APC: Calibration Test Did Not Complete | Dynamic | Enabled | Yes | Minor | 0 | 27 | 60 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |

SL1 includes pre-defined events for the most commonly encountered conditions on the most common platforms. SL1 allows you to customize these events and also to define new events. You do this in the **Event Policy Manager** page.

If your organization requires SL1 to monitor a condition for which SL1 does not already include an event policy, you can define a custom event policy to meet your needs.

For more details, see the chapter on [defining and editing events](#).

Event States

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

- **Active**. SL1 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. The magnifying-glass icon (🔍) appears to the left of the event with the highest severity or the parent event. When you click on the magnifying-glass icon, the nested events appear.

- **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 will reappear on the **Events** page.
- **Prepending**. An alert triggered the event, but additional criteria must be met before SL1 creates an event record.

Chapter



2

Viewing Events

Overview

You can view a list of all events in SL1 or view a list of events for a single device. This section describes how to perform both tasks.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ()
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

| | |
|---|----|
| <i>Searching and Filtering the List of Events</i> | 7 |
| <i>Event Throttling</i> | 13 |

Searching and Filtering the List of Events

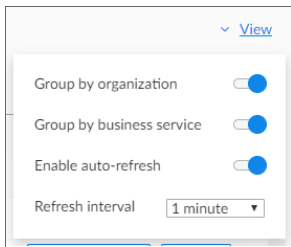
This section explains how to filter the list of events so you can quickly locate and respond to address any potential problems in your environment.

Viewing Events by Organization and Business Service

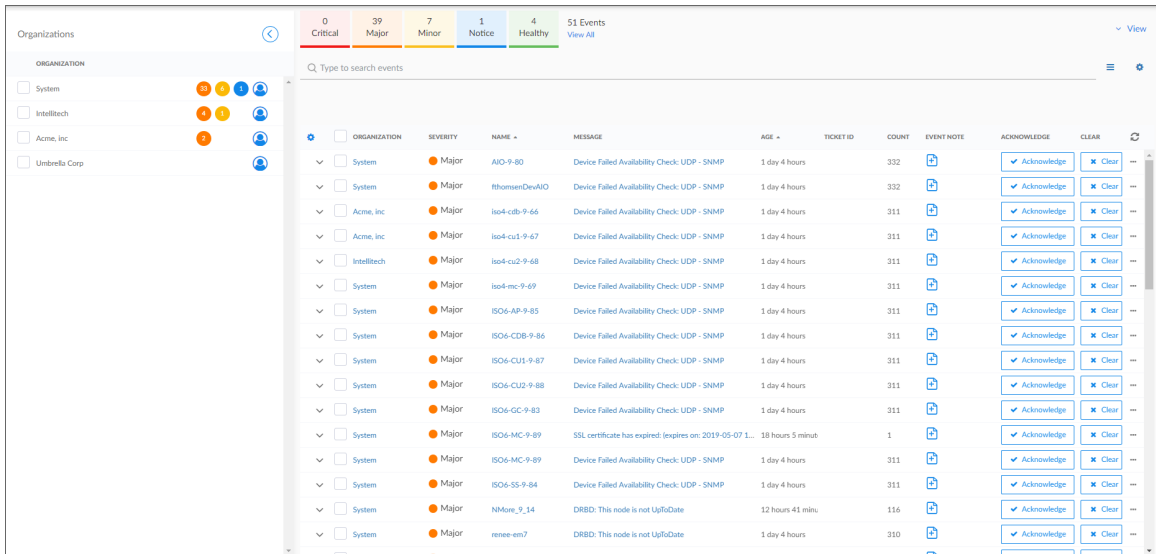
You can view events from all organizations or business services, or filter down to just the organizations or business services you want to monitor for events.

To view events by organization or business service:

1. On the **[Events]** page, click the **View** menu.



2. Click the **Group by organization** toggle to turn it blue. The **Organizations** panel appears on the **[Events]** page with a list of events sorted by severity for each organization.

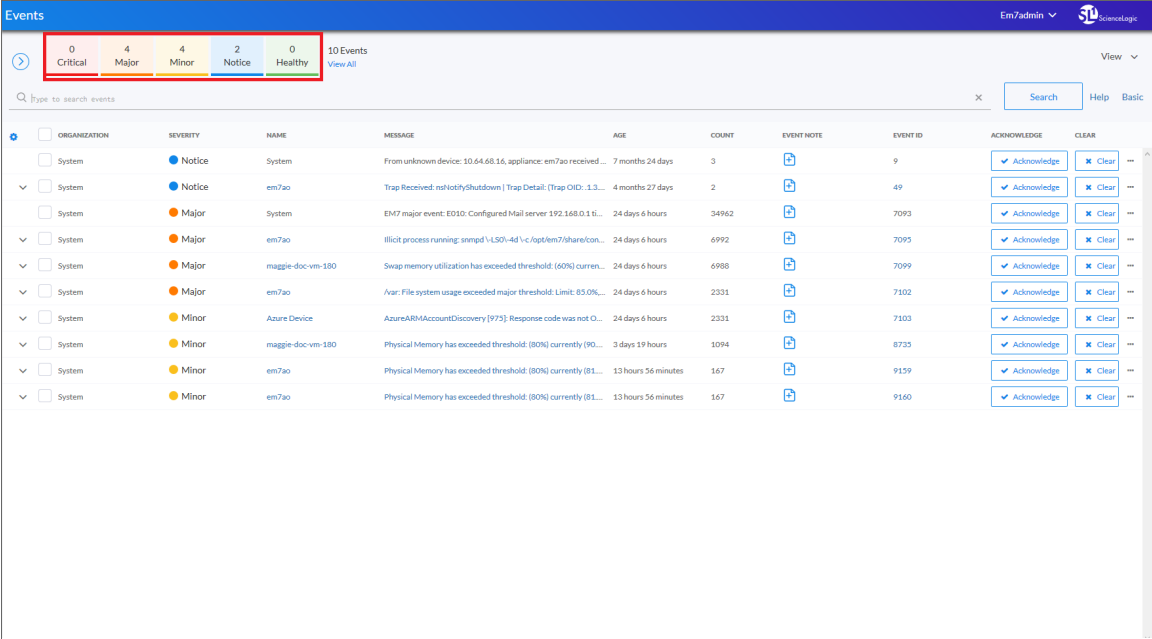


TIP: To hide the **Organizations** panel, click the left arrow icon (⏪). Click the right arrow icon (⏩) to expand the panel again.

3. On the **Organizations** panel, click the check mark icon (☑) for each organization you want to monitor.
4. To group by business service, click the **Group by business service** toggle to turn it blue. The **Business Service** panel appears on the **[Events]** page with a list of services.
5. Click the check mark icon (☑) next to a business service to view events related to that business service.

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

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

The following color codes are used throughout SL1 :

- **Red** elements have a status of **Critical**. Critical conditions are those that can seriously impair or curtail service and require immediate attention (such as service or system outages).
- **Orange** elements have a status of **Major**. Major conditions indicate a condition that is service impacting and requires immediate investigation.
- **Yellow** elements have a status of **Minor**. Minor conditions dictate a condition that does not currently impair service, but needs to be corrected before it becomes more severe.
- **Blue** elements have a status of **Notice**. Notice conditions indicate a condition that does not affect service but about which users should be aware.
- **Green** elements have a status of **Healthy**. Healthy conditions indicate that a device or service is operating under normal conditions. Frequently, a healthy condition occurs after a problem has been fixed.

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 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. For example, if a device cannot connect to the network, multiple other services on the device will raise events. SL1 would display the event with the highest severity and roll up all the other events.


To view masked events:

1. On the **Events** page, click the link in the **Message** column for the relevant event. The Event Investigator page for that event appears.
2. Scroll down to the **Masked events** section of the **Event Investigator** page to view a list of masked events:

| ORGANIZATION | SEVERITY | NAME | MESSAGE | AGE | TICKET ID | COUNT | EVENT NOTE | ACKNOWLEDGE | CLEAR |
|-------------------|----------|--------------------------|-------------------------------------|----------------|-----------|-------|------------|---------------|---------|
| NetApp C-Mode Org | Minor | SILO_JCSI/Vol/CMode_L... | No current snapshot for this volume | 1 month 7 days | | 3671 | | ▼ Acknowledge | ✕ Clear |

Refreshing the Events Page

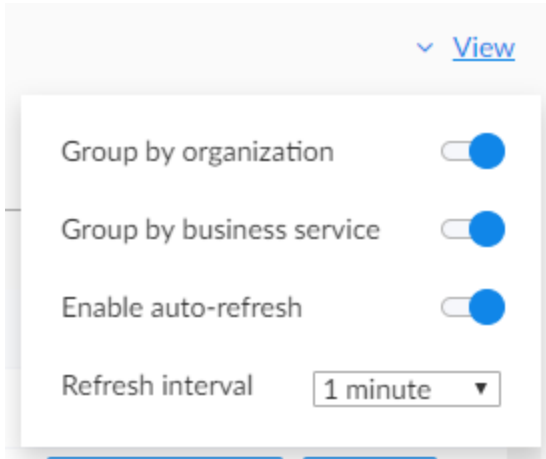
You can refresh the **Events** page manually or set it to auto-refresh.

To refresh the **Events** page manually, click the refresh icon ().

| ORGANIZATION | SEVERITY | NAME | MESSAGE | AGE | TICKET ID | COUNT | EVENT NOTE | ACKNOWLEDGE | CLEAR |
|--------------|----------|---------------|--|---------------------|-----------|-------|------------|---------------|---------|
| System | Major | AIO-9-80 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 332 | | ▼ Acknowledge | ✕ Clear |
| System | Major | rhossenDevAIO | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 332 | | ▼ Acknowledge | ✕ Clear |
| Acme, Inc | Major | iso4-c0b-9-66 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| Acme, Inc | Major | iso4-c01-9-67 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| IntelliTech | Major | iso4-c02-9-68 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | iso4-mc-9-69 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-AP-9-85 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-CDB-9-86 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-CU1-9-87 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-CU2-9-88 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-GC-9-83 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-MC-9-89 | SSL certificate has expired: (expires on: 2019-05-07 19:00:28) | 18 hours 7 minutes | | 1 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-MC-9-89 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | ISO6-SS-9-84 | Device Failed Availability Check: UDP - SNMP | 1 day 4 hours | | 311 | | ▼ Acknowledge | ✕ Clear |
| System | Major | NMore_9_14 | DRBD: This node is not UpToDate | 12 hours 43 minutes | | 116 | | ▼ Acknowledge | ✕ Clear |
| System | Major | renee-em7 | DRBD: This node is not UpToDate | 1 day 4 hours | | 310 | | ▼ Acknowledge | ✕ Clear |

To set up auto-refresh:

1. On the **Events** page, click the **View** menu.




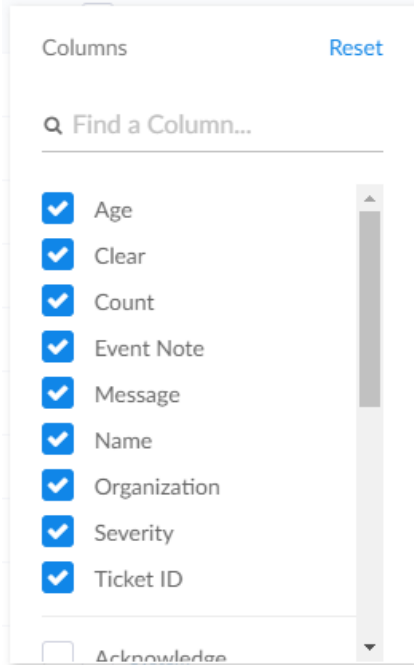
2. Click the **Enable auto-refresh** toggle to turn it blue. The **Refresh interval** drop-down appears.
3. In the **Refresh interval** drop-down, select the refresh interval for the page. Options range from 10 seconds to 60 minutes.

Customizing the Events Page

You can deselect columns that you do not want to see in the **[Events]** page, and select additional columns including custom attributes.

To select columns:

1. Click on the gear icon () in the top left of the **[Events]** page.
2. In the **Columns** menu, select the columns you want to add or deselect columns you want to hide. If you can't find a column, use the search field to find it by name. If you have created any Custom Attributes, these will appear in this list as well:

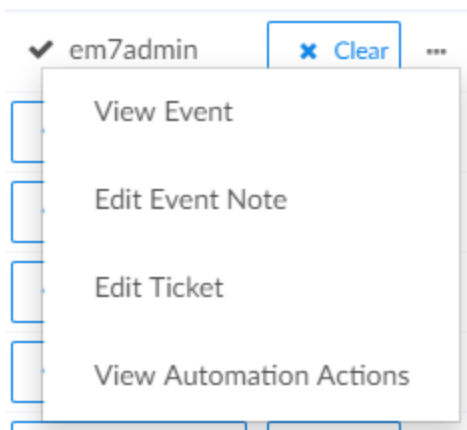


NOTE: For more information about Custom Attributes, see the *Device Management* manual.

3. When you have finished making your selections, click outside the **Columns** menu to close it.

Viewing Automation Actions

To view a log of automations that have occurred for an event, click the **[Actions]** button (⋮) for the event and select *View Automation Actions*.



Click the **[Automation]** tab in the **Ticket Editor** page that appears. The **[Automation]** tab displays a history of all automation actions that SL1 executed in response to the event associated with the ticket.

Each entry in the **Event Actions Log** page 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.

Event Throttling

When SL1 detects syslog messages or traps coming from a single device at a rate greater than 100 messages per second, SL1 throttles the messages.

When SL1 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 SL1 throttles messages, SL1 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 ten minutes. The default threshold is 100 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 message. The default threshold is 100 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: SL1 does not support message throttling on IPv6 devices monitored by CentOS5 Data Collectors.

Responding to Events

Overview

This chapter describes the different ways in which you can respond to events in SL1,

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

| | |
|--|----|
| <i>Responding to Events</i> | 15 |
| <i>Working with Events</i> | 15 |
| <i>Selecting Multiple Events</i> | 15 |
| <i>Acknowledging and Clearing Events</i> | 16 |
| <i>Viewing and Editing Event Notes</i> | 16 |
| <i>Using the Event Drawer</i> | 17 |
| <i>Working with the Tools Pane</i> | 18 |
| <i>Creating a Ticket</i> | 19 |
| <i>Using the Event Investigator</i> | 20 |

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 in the **Event Console** page and can be included in automation actions.
- **Clear**. Removes an instance of an event from the **Event Console**. The cleared instance is no longer displayed.

Working with Events

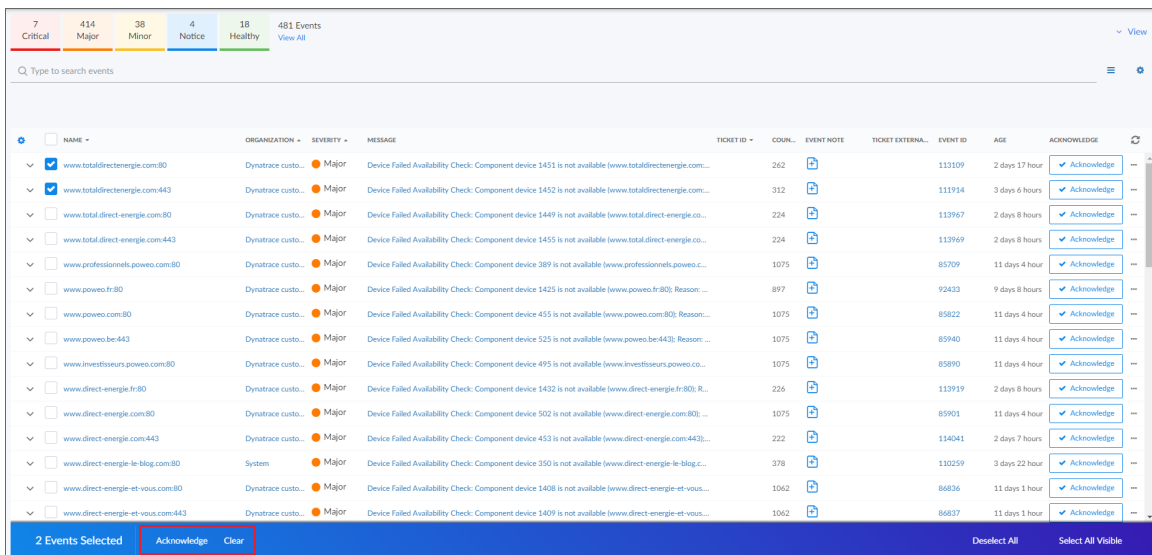
This section describes how to acknowledge and clear events in SL1, how to learn more about events, and how to use the Event Tools.

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 in the blue bar at the bottom of the window to acknowledge or clear those events simultaneously.

If you do *not* want to acknowledge or clear the selected events, click the **[Clear]** 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

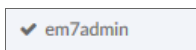
When you **acknowledge** an event, you let other users know that you are aware of that event, and you are working on a response.

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 will reappear in the **Events** page.

NOTE: If the same event occurs again on the same device, it will appear in the **[Events]** tab, even if you have previously cleared that event.


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 vent. The event is removed from the **Events** page.

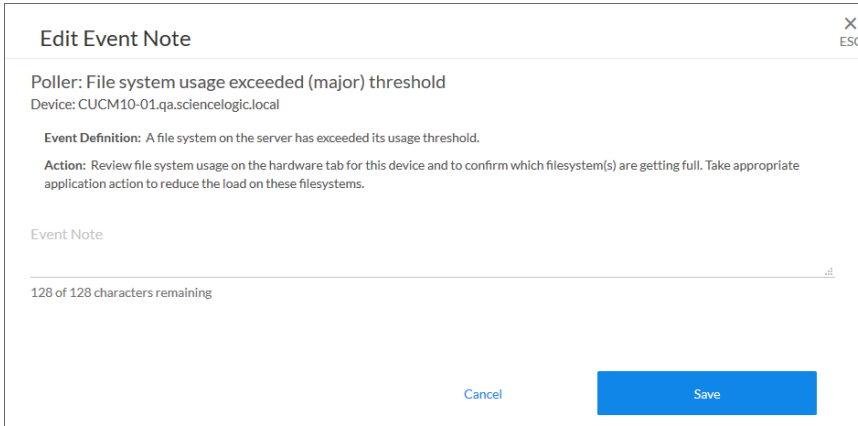
TIP: If you want to hide the **[Acknowledge]** or **[Clear]** buttons on the **Events** page, click the **Choose Columns** icon () and deselect those columns.


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** window appears:

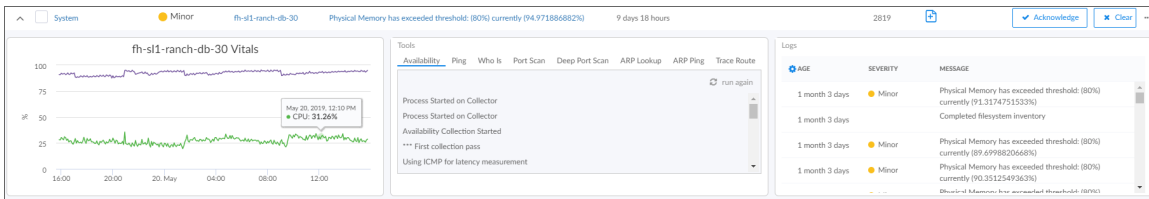


TIP: You can also edit an event note on the **Events** page by clicking the **[Actions]** button () for that event and selecting *Edit Event Note*. This is helpful if you have hidden the **Event Note** column on the **Events** page.

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

Using the Event Drawer

On the **Events** page, you can click the down-arrow icon () next to the name of an event to open a drop-down panel called the **Event Drawer**. The Event Drawer contains additional data about that event:



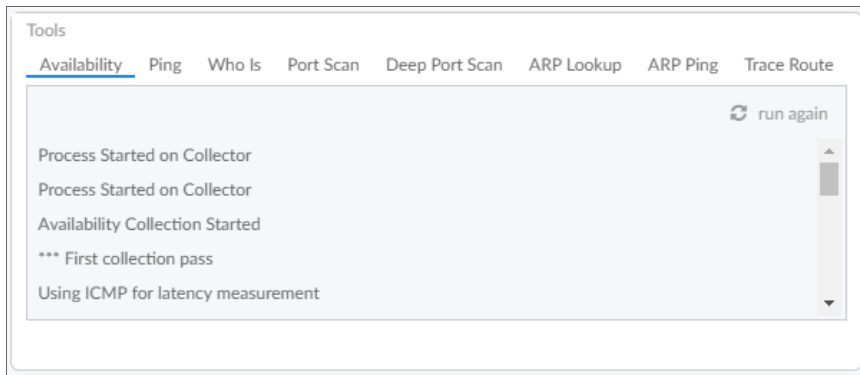
NOTE: The Event Drawer displays only for events that are aligned with devices.

On the Event Drawer, you can access the following panes:

- **Vitals.** A widget displaying 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.
- **Tools.** A set of network tools that you can run on the device associated with the event. These tools can help with troubleshooting and diagnostics.
- **Logs.** A list of the log entries from the device's log file, sorted from newest to oldest by default.

Working with the Tools Pane

The Tools pane provides access to a set of network tools. The Tools pane lets you to run diagnostics on a device associated with an event without leaving SL1.



TIP: These tools are the same tools in the Device Toolbox found in the classic user interface.

You can access the following tools from the Event Drawer on the **Events** page, the **Devices** page, and the **Device Investigator** page for a specific device:

- **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 in the **Device Settings** page.
- **Ping.** Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by SL1 to communicate with the device) and waits for a reply. SL1 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, the SL1 uses the appropriate IPv6 ping command.
- **Whols.** 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 SL1 and the device. The tool provides details on each hop to the endpoint. If the device has an IPv6 address, SL1 uses the appropriate IPv6 traceroute command.

Creating a Ticket

On the **Events** page, you can create a ticket from an event by clicking the **[Actions]** button (---) 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.

The screenshot shows the 'Ticket Editor | New Ticket' interface. At the top, there are tabs for 'Properties', 'Logs', 'Automation', and 'Message'. The main form is divided into several sections:

- Description:** (New Ticket)
- Organization:** [Dynatrace customer] [ID: 5]
- Element:** www.totaldirectenergie.com:80 [Dynatrace | Webrequest Service | IP: 1451]
- Aligned Event:** [113109] Device Failed Availability Check: Component device 1451 is not available (www.totaldirectenergie.com)

The **Ticket Properties** section includes:

- Ticket Description:** Device Failed Availability Check: Component device 1451 is not available (www.totaldirectenergie.com:80); Reason: Avail
- Ticket State:** Open
- Status:** Open
- Severity:** [Sev 2 / Major]
- Category:** Abuse
- Source:** Automated
- Queue:** Asset Management
- Assigned User:** [em7admin]

The **Notes & Attachments** section features a rich text editor with a toolbar and a text area containing the placeholder text 'Start typing or drop image here ...'. A 'Save' button is located at the bottom of the form.

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 sections for Probable Cause & Resolution, Tools, Logs, Notes, Assets, a Vitals widget, and a list of masked events:

The screenshot displays the 'Event Investigator' interface. At the top, it shows the event title 'Poller: Availability Check Failed' with a 'Major' severity indicator, '20 hours 56 minutes Ago' timestamp, '332 Occurrences', and 'First seen 2 days Ago'. There are 'Acknowledge' and 'Clear' buttons. Below this, the 'Probable Cause & Resolution' section contains an 'Event Definition' and a 'Probable Cause'. The 'Tools' section lists various diagnostic tools like 'Availability', 'Ping', 'Who Is', 'Port Scan', 'Deep Port Scan', 'ARP Lookup', 'ARP Ping', and 'Trace Route'. The 'Logs' section features a table with columns for 'AGE', 'SEVERITY', and 'MESSAGE'. The 'Note' section at the bottom has a text input field and 'Cancel' and 'Save Note' buttons.

| AGE | SEVERITY | MESSAGE |
|------------------|----------|---|
| 24 days 11 hours | Major | Device Failed Availability Check: UDP - SNMP |
| 24 days 11 hours | Minor | Network latency exceeded threshold: No Response |
| 24 days 11 hours | Major | Device Failed Availability Check: UDP - SNMP |
| 24 days 11 hours | Minor | Network latency exceeded threshold: No Response |
| 24 days 11 hours | Major | Device Failed Availability Check: UDP - SNMP |

TIP: To get to the **Event Investigator** page, click the linked text in the **Message** column of the **Events** page, or click the **[Actions]** button (☰) for the event and select **View Event**.

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]** button (☰) and select **Create Ticket** to create a ticket for that event. You can hover your mouse over an acknowledged field to see when the event was acknowledged and who acknowledged it. Also, if an event was acknowledged by another user and you have the relevant permissions, you can click the **[Reacknowledge]** button to acknowledge that event.

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

- **Probable Cause & Resolution**. Displays additional information about the event, based on the event policy.
- **Tools**. A set of network tools that you can run on the device associated with the event. This pane is the same as the Tools pane of the Event Drawer. For more information, see [Working with the Tools Pane](#).
- **Logs**. A list of log entries from the device's log, sorted from newest to oldest by default.
- **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](#).
- **Assets**. One or more asset records associated with the device, such as a piece of equipment owned by an organization. The asset record includes contact information for the technician, administrator, and vendor for that device. You can click the name of an asset to view an **Asset** page for more information.
- **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.
- **Masked events**. A list of all masked events for the device. 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.

Chapter



4

Events and Tickets

Overview

This chapter describes how to create tickets from events in SL1 .

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

| | |
|--|----|
| <i>Creating a Ticket from an Event</i> | 23 |
| <i>Event Ticket Behavior Settings</i> | 26 |

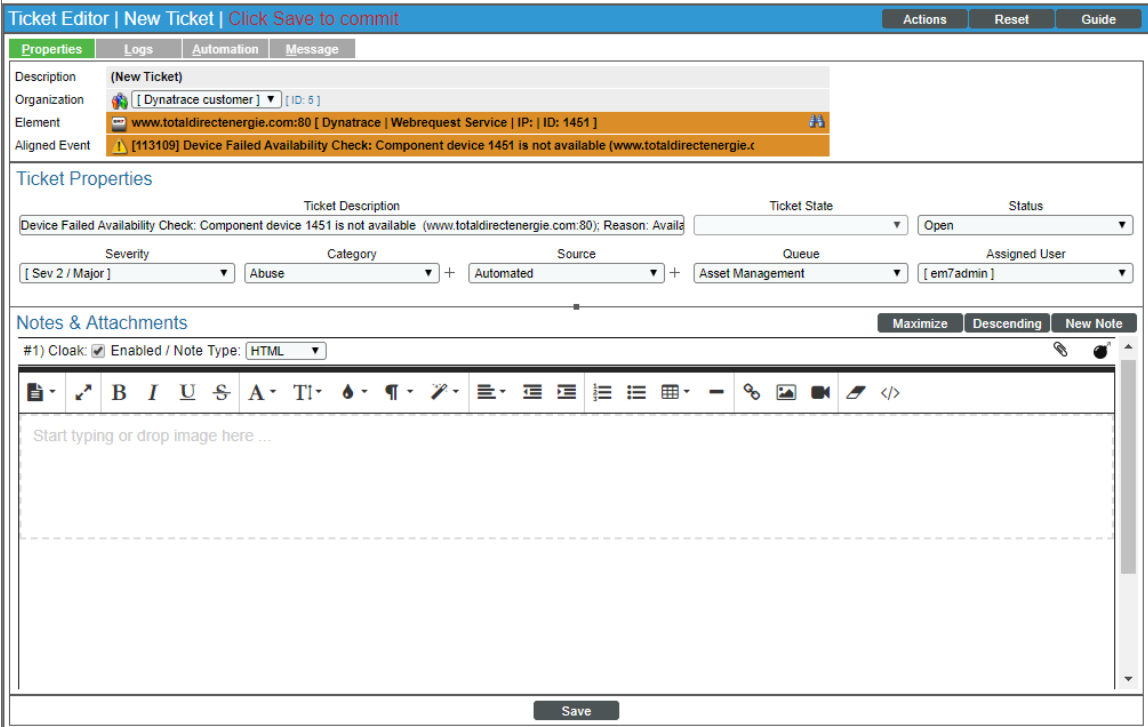
Creating a Ticket from an Event

A **ticket** is a request for work that can be tracked in SL1. 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, based on a selected event, most of the ticket fields are populated automatically by SL1.

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" will then be able to create and save tickets from the **Events** page page. For more information on Access Keys, see the manual **Access Permissions**.


1. On the **Events** page or the **Event Investigator** page for a specific event, click the **[Actions]** button (☰) for the event and select *Create Ticket*. The **Ticket Editor** page appears:



The screenshot shows the 'Ticket Editor' interface. At the top, there's a blue header with 'Ticket Editor | New Ticket | Click Save to commit' and buttons for 'Actions', 'Reset', and 'Guide'. Below the header are tabs for 'Properties', 'Logs', 'Automation', and 'Message'. The 'Properties' tab is active, showing fields for 'Description (New Ticket)', 'Organization' (Dynatrace customer), 'Element' (www.totaldirectenergie.com:80), and 'Aligned Event' ([113109] Device Failed Availability Check: Component device 1451 is not available). Below this is the 'Ticket Properties' section with fields for 'Ticket Description', 'Ticket State' (Open), 'Status' (Open), 'Severity' (Sev 2 / Major), 'Category' (Abuse), 'Source' (Automated), 'Queue' (Asset Management), and 'Assigned User' (em7admin). At the bottom is the 'Notes & Attachments' section with a 'Maximize', 'Descending', and 'New Note' button, and a rich text editor with a toolbar and a 'Save' button at the bottom.

2. Depending on the **Event Console Ticket Life Ring Button Behavior** setting in the **Behavior Settings** page (System > Settings > Behavior), SL1 creates an SL1 ticket or an external ticket. See the [Event Ticket](#)

[Behavior Settings](#) section for more information.

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 in the **Events** page, this field is populated automatically by SL1.
 - **Organization**. Select the organization with which the ticket will be associated in the drop-down menu. If you create a ticket from an event in the **Events** page, this field is populated automatically by SL1.
 - **Element**. By default, this field includes the element associated with this 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, select the binoculars 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**, this field is populated automatically by SL1 with the event's severity. The choices are:
 - Severity 5/Healthy
 - Severity 4/Notice
 - Severity 3/Minor
 - Severity 2/Major
 - Severity 1/Critical
 - **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 SL1 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 SL1.
 - *Phone.* A phone call about an issue prompted this ticket.
 - **Queue.** Ticket Queue to which the ticket will be assigned. When you select a **Ticket Queue**, SL1 will populate 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 assigned to the specified Ticket Queue and who has a Login State of *Active*. When a ticket is assigned to a user, SL1 automatically sends the user an email message as notification.
 - **Custom Fields.** If your SL1 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** will appear 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 is determined in the **Behavior Settings** page (System > Settings > Behavior). To change this behavior:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).

The screenshot shows the 'Behavior Settings' page with various configuration options. The 'Event Console Ticket Life Ring Button Behavior' dropdown menu is highlighted with a red box and is currently set to 'Create / View EM7 Ticket'. Other visible settings include 'Interface URL' (http://em7.mydomain.com), 'Password Expiration' (disabled), 'Account Lockout Type' (Lockout by Username), and 'Event Console Ticket Life Ring Button Behavior' (Create / View EM7 Ticket).

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 for an event, SL1 displays the **Ticket Editor** page, where you can define an SL1 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 for that event, SL1 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 for that event, SL1 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 details on events and external tickets, see the section on [integrating events and external tickets](#).

Event Correlation and Parent and Child Events

Overview

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

Use the following menu options to navigate the SL1 user interface:


- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

| | |
|--|----|
| <i>Event Correlation</i> | 29 |
| <i>Defining Parent and Child Devices</i> | 30 |
| <i>Device Categories that Don't Support Children Devices</i> | 31 |
| <i>Defining Suppressing and Suppressible Events</i> | 32 |
| <i>Event Categories</i> | 35 |
| <i>Assigning an Event Category to an Event</i> | 36 |
| <i>Creating an Event Category</i> | 37 |
| <i>Editing an Event Category</i> | 38 |
| <i>Viewing the List of Event Categories</i> | 39 |
| <i>Filtering the List of Event Categories</i> | 40 |
| <i>Special Characters</i> | 41 |
| <i>Deleting One or More Event Categories</i> | 45 |

Event Correlation

In SL1, there are four types of events that might not appear on the **Events** page:

- **Rolled-up events.** Multiple occurrences of the same event on the same device. When the same event occurs multiple times on a single device, SL1 does not display each occurrence on the **Events** page. Instead, SL1 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 chapter on [Responding to Events](#).
- **Topology Events.** In SL1, 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 will be incremented to indicate the number of correlated child events. Optionally, you can define event categories that allow SL1 to more efficiently align suppressing events with suppressible events. When you align an event category to a suppressing or suppressible event, that event will be 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 events masks, see the chapter on [Viewing Events](#).

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

SL1 performs two types of event correlation:

- **Automatic Event-Correlation.** During discovery, SL1 automatically discovers and defines parent-child relationships between devices.
- **Manual Event Correlation.** In SL1, you can configure devices and events so that events that are associated with child devices will be rolled-up under the parent device's events on the **Events** page. 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. 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 SL1 to more efficiently align suppressing events with suppressible events.

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

- Define parent and child devices. SL1 does this automatically when it discovers Layer-2, CDP, LLDP, Layer-3, and VMware topology. For example, if SL1 automatically discovers a switch and its clients, SL1 automatically defines the switch as the parent device and its clients as the children devices. You can also do this manually when you create Layer-2 Links, Layer-3 Links, CDP Links, LLDP Links, or Event Correlation Override links in the Maps > Classic Maps > Topology Maps pages or the Maps > Classic Maps > My Customized Maps

pages. For more information about creating parent-child relationships in views, see the **Views** manual.

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

This chapter describes the required tasks for manual event correlation.

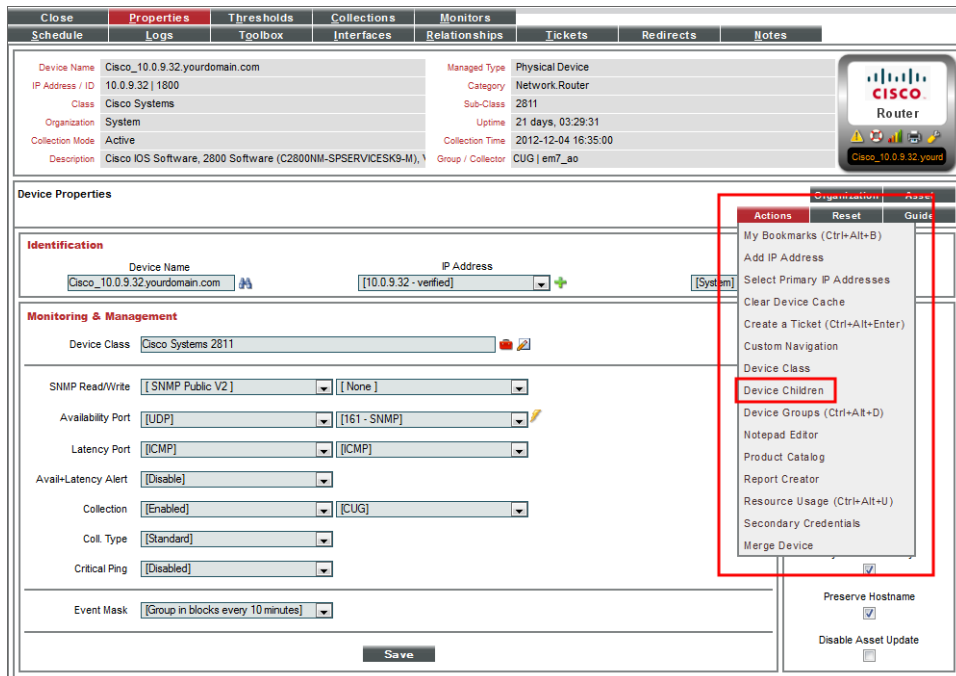
Defining Parent and Child Devices

The **Device Children** modal page allows users to select one or more devices to become children of the currently selected device.

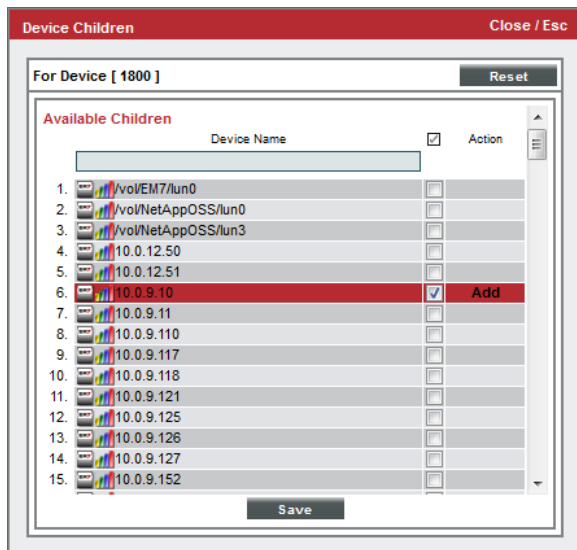
To add children to a device:

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

NOTE: You cannot create parent-child relationships for devices with a **Device Category** of *Virtual*.



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



6. In the **Device Children** page, select one or more devices to be children of the current device.
7. Click **[Save]**.

Device Categories that Don't Support Children Devices

A device category is a logical categorization of a device by primary function. SL1 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 children 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** menu of the **Device Investigator** page.


Defining Suppressing and Suppressible Events

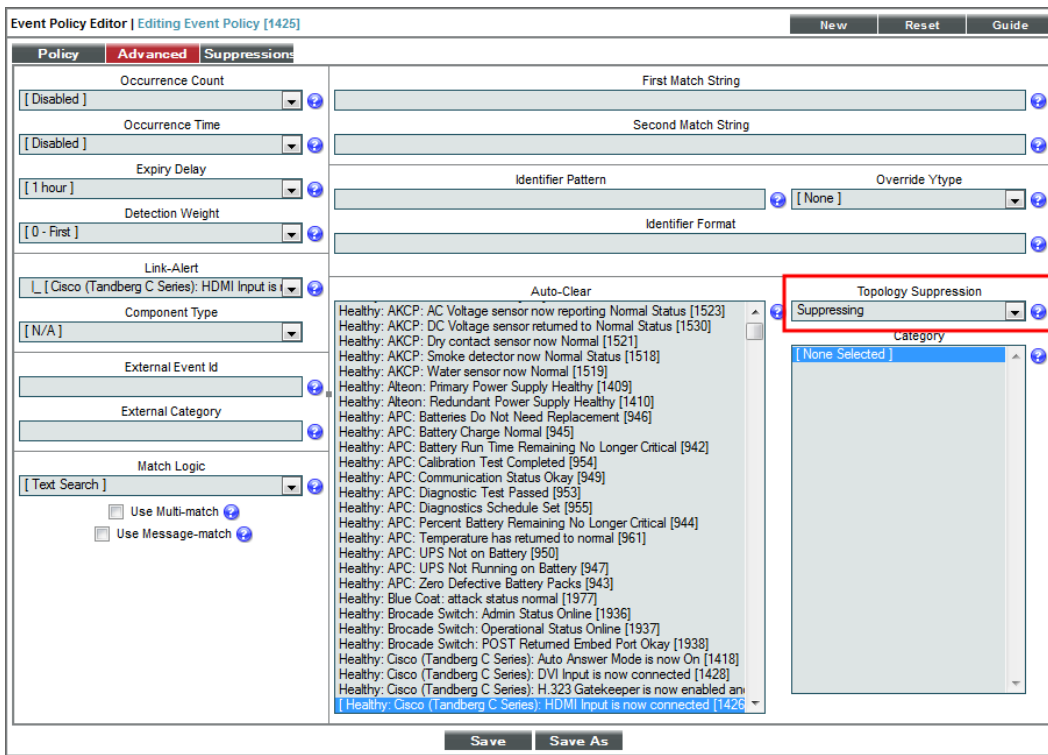
To manually configure event correlation, you must define two types of events:

- **Suppressing events.** If this event occurs on a parent device, SL1 will search all related children devices for **suppressible** events. On the children devices, all suppressible events will be suppressed. Only the suppressing event will appear in the **Events** page. The suppressible events will not appear in the **Events** page.
- **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 will cause SL1 to suppress **all suppressible** events on the associated children devices.

To define an event as a suppressing event:

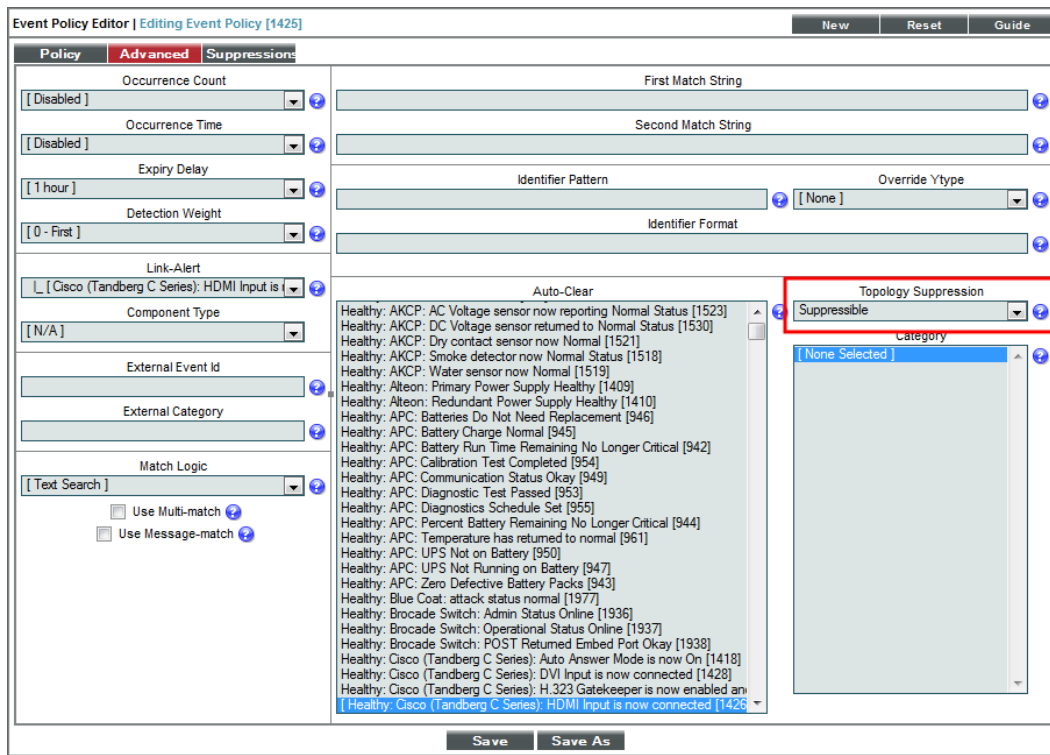
1. Go to the **Event Policy Manager** page (Events > Event Policies).
2. On the **Event Policy Manager** page, select the wrench icon () of the event that you want to define as the **suppressing** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]** tab.



4. In the **Topology Suppression** field, select *Suppressing*.
5. Click **[Save]**. In the future, when this event occurs on a device, SL1 will check if the device is a parent device. If the device is a parent device, specified events (suppressible events) with the same category will be suppressed on the children devices.

To define an event as a suppressible event:

1. Go to the **Event Policy Manager** page (Events > Event Policies).
2. On the **Event Policy Manager** page, select 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, select the **[Advanced]** tab.



4. In the **Topology Suppression** field, select *Suppressible*.
5. Click **[Save]**. In the future, when this event occurs on a device, SL1 will check if the device is a child device. If the device is a child device, SL1 will check 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 will be suppressed on the child device.

For example:

- Suppose you have a device named *Boise-DMZ*. Suppose this device is a Cisco Catalyst switch. Suppose we define this switch as a parent device.
- Suppose we have a device named *HQ-W2K3-VC01*. Suppose this device is a server. Suppose we define this server as a child device to *Boise-DMZ*.
- Suppose we define the event "Poller: Interface operationally down" as a suppressing event.
- Suppose we define the event "Poller: Device not responding" as a suppressible event.
- Suppose we associate both events with the same event category.
- If an interface goes down on the switch *Boise-DMZ*, SL1 will not be able to communicate with the server, *HQ-W2K3-VC01*, attached to the switch.
- So if the event "Poller: Interface operationally down" occurs on *Boise-DMZ*, the event "Poller: Device not responding" will be suppressed on the server *HQ-W2K3-VC01*. On the **Events** page, only the event "Poller: Interface operationally down" on the device *Boise-DMZ* will appear.

Event Categories

Event categories allow SL1 to more efficiently align suppressing events. When you align an event category to a suppressing or suppressible event, that event will be correlated only with events that are aligned with the same event category. An event can be aligned to multiple event categories; for event correlation to occur, the suppressing event and the suppressible event must both be aligned with a common event category.

Before defining suppressing events and suppressible events, you can define event categories to streamline event suppression.

- If you do not define any event categories, SL1 handles suppressing events and suppressible events like this:
 - If a suppressing event occurs on a parent device, SL1 will search all related children devices for suppressible events. On each child device, each occurrence of any event defined as suppressible will be suppressed. Only the suppressing event and the parent device will appear on the **Events** page. The suppressible events will be nested under the suppressing event and will not be displayed by default.
 - For example, suppose you have a parent device that is a chassis and a child device that is a blade.
 - Suppose you define two suppressing events: one for when SL1 can't collect data with a Dynamic Application (Dynamic App Collection Problem) and one for when a fan fails (Fan critical).
 - Suppose you define three suppressible events: one for when collection with a Dynamic Application times out (Dynamic Application taking too long to collect), one for when a device exceeds the recommended temperature (Temperature critical), and one for when a device is not available via SNMP (Availability check failed).
 - Suppose on the parent device (the chassis), the suppressing event "Dynamic App Collection Problem" occurs.
 - SL1 will search for all child devices associated with the chassis and then search for all suppressible events.
 - Suppose on the child device (the blade) two suppressible events occur: "Temperature Critical" and "Availability Check Failed".
 - On the **Events** page, SL1 will nest these two suppressible events under the parent event, even though there is no relationship between the parent event and the child events.

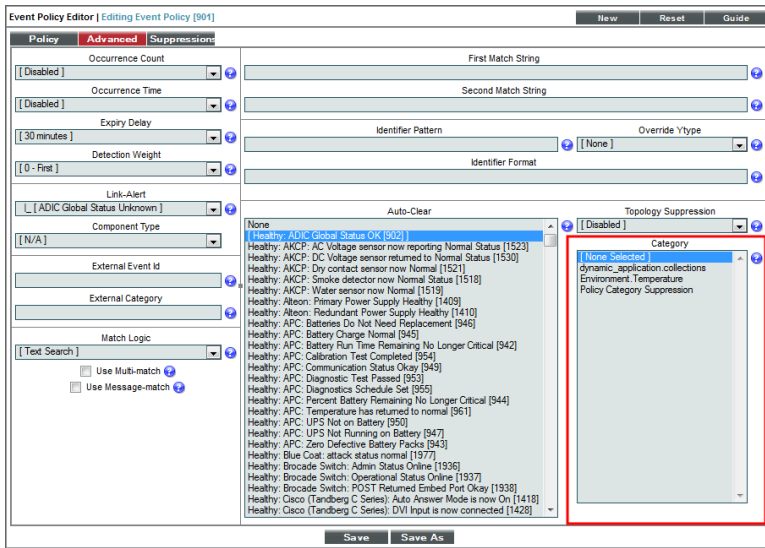
- Now suppose we define two event categories. Suppose we define "Environment.Temperature" and "Dynamic Applications.Collection":
 - Suppose you have a parent device that is a chassis and a child device that is a blade.
 - Suppose you define two suppressing events: one for when SL1 can't collect data with a Dynamic Application (Dynamic App Collection Problem) and one for when a fan fails (Fan critical).
 - Suppose you define three suppressible events: one for when collection for a Dynamic Application is timing out (Dynamic Application taking too long to collect), one for when a device exceeds the recommended temperature (Temperature critical), and one for when a device is not available via SNMP (Availability check failed).
 - Suppose when you define each event as suppressing or suppressible, you align event categories like this:

| Event Name | Event Hierarchy | Event Category |
|--|-----------------|---------------------------------|
| Dynamic App Collection Problem | Suppressing | Dynamic Applications.Collection |
| Dynamic Application taking too long to collect | Suppressible | Dynamic Applications.Collection |
| Availability check failed | Suppressible | Dynamic Applications.Collection |
| Fan critical | Suppressing | Environment.Temperature |
| Temperature critical | Suppressible | Environment.Temperature |

- Suppose on the parent device (the chassis) the suppressing event "Dynamic App Collection Problem" occurs.
- SL1 will search for all child devices and then search for all suppressible events that have the same event category, Dynamic Applications.Collection.
- Suppose on the child device (the blade) two suppressible events occur: "Temperature Critical" and "Dynamic application taking too long to collect".
- On the **Events** page, SL1 will display the event "Dynamic application taking too long to collect" under the parent event "Dynamic App collection problem", because both events belong to the same event category.
- The **Events** page will not nest the event "Temperature critical", under the parent event "Dynamic App collection problem", because the two events do not have the same event category.

Assigning an Event Category to an Event

You can assign an event category to an event in the **Event Policy Editor** page, in the **[Advanced]** tab.



If you define an event as **suppressing** and assign an event category to the event, when the event occurs, SL1 will suppress only events that meet all of these criteria:

- Occur on a child device
- Are defined as suppressible
- Are aligned with the same event category

If you define an event as **suppressible** and assign an event category to the event, when the event occurs, SL1 will suppress the event only if all the following occur:

- The event occurs on a child device.
- A suppressing event occurs on the parent device.
- The suppressing event and the suppressible event are aligned with the same event category.

NOTE: If you assign an event category to an event that is neither suppressing nor suppressible, SL1 does not use the event category. The event category will have no effect.

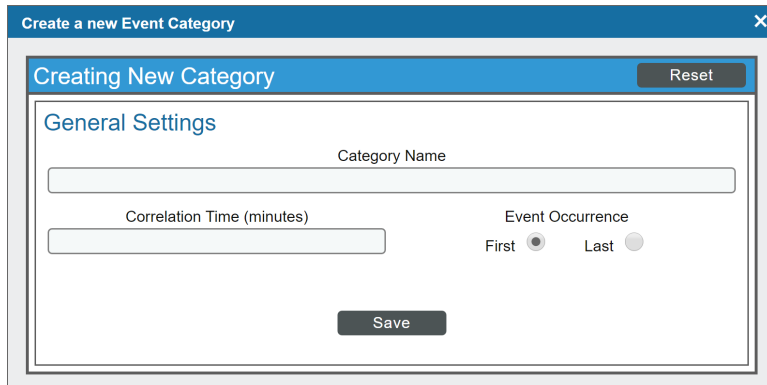
Creating an Event Category

From the **Event Category Manager** page, you can define a new event category. This allows you to customize event categories to meet your business requirements.

To create an event category:

1. Go to the **Event Category Manager** page (Events > Categories).
2. In the **Event Category Manager** page, select the **[Create]** button.

3. The **Event Category Editor** page is displayed. In this page, you can define a new event category. Supply a value in the following fields:




- **Category Name.** The name of the event category. This can be any combination of numbers, letters, and symbols.
- **Correlation Time.** You can specify an integer value of zero ("0") or greater in this field. This value can be used in custom Run Book Actions, where **Action Type** is *Run a Snippet*. For details on Run Book Actions, see the **Run Book Automation** manual.
- **Event Occurrence.** Specifies whether *Correlation Time* should start after first occurrence of the event or after most recent occurrence of the event. Possible values are *First* or *Last*.

4. Click **[Save]** to save your new event category.

Editing an Event Category

From the **Event Category Manager** page, you can edit the definition of an event category. This allows you to adjust or customize an existing category to meet your business requirements.

To edit an event category:

1. Go to the **Event Category Manager** page (Events > Categories).
2. In the **Event Category Manager** page, select the wrench icon () of the event category you want to edit.
3. The **Event Category Editor** page is displayed.

4. In the **Event Category Editor**, you can edit the following fields:

- **Category Name.** The name of the event category. This can be any combination of numbers, letters, and symbols.
- **Correlation Time.** You can specify an integer value of zero ("0") or greater in this field. This value can be used in custom Run Book Actions, where **Action Type** is *Run a Snippet*. For details on Run Book Actions, see the **Run Book Automation** manual.
- **Event Occurrence.** Specifies whether *Correlation Time* should start after first occurrence of the event or after most recent occurrence of the event. Possible values are *First* or *Last*.

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

6. You can also click **[Save As]** to save your changes as a new event category with a different name.

Viewing the List of Event Categories

The **Event Category Manager** page displays the following about each event category:

| Event_Catgory_Name | Event_count | ID | Correlation_Time | Event_Occurrence | Edited_By | Last_Edited |
|------------------------------------|-------------|----|------------------|------------------|-----------|---------------------|
| 1. Category 1 | 21 | 7 | 6 Min. | First | em7admin | 2016-08-15 16:23:09 |
| 2. Category 2 | 20 | 8 | 0 Min. | First | em7admin | 2016-08-15 16:23:17 |
| 3. Dynamic Applications.Collection | -- | 3 | 0 Min. | First | em7admin | 2016-07-24 17:31:09 |
| 4. Environment.Temperature | 7 | 2 | 4 Min. | First | em7admin | 2016-08-16 17:40:45 |
| 5. Example Category | 2 | 9 | 2 Min. | Last | em7admin | 2016-08-17 21:57:51 |

TIP: To sort the list of event categories, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Last Edited** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- **Event Category Name.** The name of the event category.
- **Event Count.** Number of events that are aligned with the event category.
- **ID.** Unique numeric ID for the event category, generated by SL1.
- **Correlation Time.** You can specify an integer value of zero ("0") or greater in this field. This value can be used in custom Run Book Actions, where **Action Type** is *Run a Snippet*. For details on Run Book Actions, see the **Run Book Automation** manual.
- **Event Occurrence.** Specifies whether *Correlation Time* should start after first occurrence of the event or after most recent occurrence of the event. Possible values are *First* or *Last*.
- **Edited By.** Name of the user who created or last edited the event category.
- **Last Edited.** Date and time the event category was created, imported into SL1, or last edited.

Filtering the List of Event Categories

The Filter-While-You-Type fields appear as a row of blank fields at the top of the list. These fields allow you to filter the items that appear in the list.

The list is dynamically updated as you select each filter. For each filter, you must make a selection from a drop-down menu or type text to match against. SL1 will search for entries that match the text, including partial matches. Text matches are not case-sensitive, and you can use special characters in each text field.

By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

You can filter by one or more of the following parameters. Only items that meet all of the filter criteria are displayed on the page.

The following describes each filter on the **Event Category Manager** page:

- **Event Category Name.** You can enter text to match, including special characters, and the **Event Category Manager** page will display only event categories that have a matching category name.
- **Event Count.** You can enter text to match, including special characters, and the **Event Category Manager** page will display only event categories that have a matching event count.
- **ID.** You can enter text to match, including special characters, and the **Event Category Manager** page will display only event categories that have a matching event category ID.
- **Correlation Time.** You can enter an integer to match, including special characters, and the **Event Category Manager** page will display only event categories that have a matching correlation time.

- **Event Occurrence.** You can enter text to match, including special characters, and the Event Category Manager page will display only event categories that have a matching value in the Event Occurrence field.
- **Edited By.** You can enter text to match, including special characters, and the **Event Category Manager** page will display only event categories that have been created or edited by a matching user.
- **Last Edited.** Only those event categories that match all the previously selected fields and have the specified last edit date will be displayed. The choices are:
 - *All.* Display all event categories that match the other filters.
 - *Last Minute.* Display only event categories that have been created within the last minute.
 - *Last Hour.* Display only event categories that have been created within the last hour.
 - *Last Day.* Display only event categories that have been created within the last day.
 - *Last Week.* Display only event categories that have been created within the last week.
 - *Last Month.* Display only event categories that have been created within the last month.
 - *Last Year.* Display only event categories that have been created within the last year.

Special Characters

You can include the following special characters to filter by each column except those that display date and time:

NOTE: When searching for a string, SL1 will match substrings by default, even if you do not include any special characters. For example, searching for "hel" will match both "hello" and "helicopter". When searching for a numeric value, SL1 will not match a substring unless you use a special character.

String and Numeric

- , (comma). Specifies an "OR" operation. Works for string and numeric values. For example:
"dell, micro" matches all values that contain the string "dell" OR the string "micro".
- & (ampersand). Specifies an "AND " operation. Works for string and numeric values. For example:
"dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.

- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:

"!dell" matches all values that do not contain the string "dell".

"! ^ micro" would match all values that do not start with "micro".

"!fer\$" would match all values that do not end with "fer".

"! ^ \$" would match all values that are not null.

"! ^ " would match null values.

"!\$" would match null values.

"!*" would match null values.

"happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

NOTE: You can also use the "!" character in combination with the arithmetic special characters (min-max, >, <, >=, <=, =) described below.

- * (asterisk). Specifies a "match zero or more" operation. Works for string and numeric values. For a string, matches any string that matches the text before and after the asterisk. For a number, matches any number that contains the text. For example:

"hel*er" would match "helpers" and "helicopter" but not "hello".

"325*" would match "325", "32561", and "325000".

"*000" would match "1000", "25000", and "10500000".

- ? (question mark). Specifies "match any one character". Works for string and numeric values. For example:

"!?ver" would match the strings "oliver", "levers", and "lover", but not "believer".

"135?" would match the numbers "1350", "1354", and "1359", but not "135" or "13502"

String

- ^ (caret). For strings only. Specifies "match the beginning". Matches any string that begins with the specified string. For example:

" ^ sci" would match "scientific" and "sciencelogic", but not "conscious".

" ^ happy\$" would match only the string "happy", with no characters before or after.

"! ^ micro" would match all values that do not start with "micro".

"! ^ \$" would match all values that are not null.

"! ^ " would match null values.

- \$ (dollar sign). For strings only. Specifies "match the ending". Matches any string that ends with the specified string. For example:

"ter\$" would match the string "renter" but not the string "terrific".

"^happy\$" would match only the string "happy", with no characters before or after.

"!fer\$" would match all values that do not end with "fer".

"!^\$" would match all values that are not null.

"!\$" would match null values.

NOTE: You can use both ^ and \$ if you want to match an entire string and only that string. For example, "^tern\$" would match the strings "tern" or "Tern" or "TERN"; it would not match the strings "terne" or "cistern".

Numeric

- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:

"1-5" would match 1, 2, 3, 4, and 5.

- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:

"1-" matches 1 and greater. So would match 1, 2, 6, 345, etc.

"-5" matches 5 and less. So would match 5, 3, 1, 0, etc.

- > (greater than). Matches numeric values only. Specifies any value "greater than". For example:

">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than". For example:

"<12" would match all values less than 12.

- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to". For example:

">=7" would match all values 7 and greater.

- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to". For example:

"<=12" would match all values 12 and less.

- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:

"=-5" would match "-5" instead of being evaluated as the "half open range" as described above.

Additional Examples

- "aio\$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo\$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!O\$". Matches only text that does not end with "O".
- "!^silo\$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!. Matches null values, typically represented as "--" in most pages.
- "!. Matches null values, typically represented as "--" in most pages.
- "!. Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s*i*i*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would match.
- "!^s*i*i*o\$". Matches all text that does not contain the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol" and it does contain "02".
- "aggr,!vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr,!vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "*". Matches all text.
- "!*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- "!silo". Matches text that does not contain "silo".
- "!^silo\$". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.

- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "1n", and "2n".
- "n*SAN". Matches text the contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".
- "^?n*SAN\$". Matches text that begins with any single character, is following by "n", and then zero or any number of any characters, and ends in "SAN".

Deleting One or More Event Categories

From the **Event Category Manager** page, you can delete an event category. To do so:

NOTE: When you remove an event category, the category is also removed from any event policy with which it is aligned.

1. Go to the **Event Category Manager** page (Events > Categories).
2. In the **Event Category Manager** page, select the checkbox () of each event category you want to delete.
3. In the **Select Action** drop-down list, select *Delete these Event Categories*, then select the **[Go]** button.
4. Each selected event category is removed from SL1.

The screenshot shows the 'Event Category Manager' interface. The main content area displays a table with the following data:

| Event Category Name | Event count | ID | Correlation Time | Event Occurrence | Edited By | Last Edited | |
|------------------------------------|-------------|----|------------------|------------------|-----------|---------------------|-------------------------------------|
| 1. Category 1 | 21 | 7 | 6 Min. | First | em7admin | 2016-08-15 16:23:09 | <input checked="" type="checkbox"/> |
| 2. Category 2 | 20 | 8 | 0 Min. | First | em7admin | 2016-08-15 16:23:17 | <input type="checkbox"/> |
| 3. Dynamic Applications.Collection | -- | 3 | 0 Min. | First | em7admin | 2016-07-24 17:31:09 | <input type="checkbox"/> |
| 4. Environment.Temperature | 7 | 2 | 4 Min. | First | em7admin | 2016-08-16 17:40:45 | <input type="checkbox"/> |
| 5. Example Category | 2 | 9 | 2 Min. | Last | em7admin | 2016-08-17 21:57:51 | <input type="checkbox"/> |

At the bottom right, a dropdown menu is open, showing the following options:

- [Select Action]
- Administration:
- DELETE these Event Categories**
- [Select Action]



A 'Go' button is visible next to the dropdown menu.

Defining and Editing Event Policies

Overview

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

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

| | |
|--|----|
| <i>How SL1 Generates Events</i> | 47 |
| <i>Viewing the List of Event Policies</i> | 48 |
| <i>Filtering the List of Event Policies</i> | 50 |
| <i>Special Characters</i> | 52 |
| <i>Defining an Event Policy</i> | 56 |
| <i>Defining Basic Event Parameters in the Policy Tab</i> | 57 |
| <i>Defining Pattern Matching and Advanced Behavior in the Advanced Tab</i> | 60 |
| <i>Defining Event Suppressions in the Suppressions Tab</i> | 67 |
| <i>Defining an Event Policy for a Specific Interface</i> | 69 |
| <i>Defining Custom Severity for an Interface</i> | 71 |
| <i>Editing an Event Policy</i> | 73 |
| <i>Best Practices for Event Definitions</i> | 75 |

How SL1 Generates Events

SL1 includes pre-defined events for the most commonly encountered conditions on the most common platforms. SL1 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 Policy Manager** page.

SL1 monitors devices (and their applications and components). SL1 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. SL1 then uses these log messages to generate events. SL1 examines each incoming log message and compares it to each event policy. If a log message matches an event policy, SL1 generates an instance of the event and displays the instance in the **Event Console** page. The event instance will be associated with the entity that triggered the original log message.

SL1 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 like MoMs. A syslog is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.
- **Internal**. Message is generated by a ScienceLogic process. The message is about the SL1 system itself, instead of the devices that the SL1 system monitors.
- **Trap**. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like MoMs. An SNMP trap is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.
- **Dynamic**. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users 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. SL1 examines each new message in the device log and determines if the message matches an event definition. If it does, SL1 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 F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the SL1 system inserts a message in the associated device's log files, and the SL1 system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
- **Email**. Message is generated by an email message sent to SL1. For more information on generating events with email messages, see the [Events from Email](#) chapter.

- **API.** Message was 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 manual *Run Book Automation*. For more information on snippet Dynamic Applications, see the manual *Snippet Dynamic Application Development*. For more information on the ScienceLogic API, see the manual *Using the ScienceLogic API*.
- **SL1 agent.** Message is generated by log file messages collected by the SL1 agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the *Monitoring Using the SL1 agent* manual.

Viewing the List of Event Policies

From the **Event Policy Manager** page, you can view a list of all event policies in SL1. 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:

| Event Policy Name | Type | State | P-Pack | Severity | Weight | ID | Expiry | Time | Thresh | Edited By | Last Edited | External ID | Category |
|--|---------|---------|--------|----------|--------|------|---------|--------|--------|-----------|---------------------|-------------|----------|
| 1. ADIC: Global Status Failed | Dynamic | Enabled | Yes | Major | 0 | 2 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 2. ADIC: Global Status OK | Dynamic | Enabled | Yes | Healthy | 0 | 4 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 3. ADIC: Global Status Unknown | Dynamic | Enabled | Yes | Notice | 0 | 3 | 30 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 4. ADIC: Tape Library Degraded | Dynamic | Enabled | Yes | Minor | 0 | 1 | 60 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 5. AKCP: AC Voltage sensor detects no current | Syslog | Enabled | Yes | Critical | 0 | 1288 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 6. AKCP: AC Voltage sensor now reporting Normal Status | Syslog | Enabled | Yes | Healthy | 0 | 1294 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 7. AKCP: DC Voltage High Warning | Syslog | Enabled | Yes | Major | 0 | 1299 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 8. AKCP: DC Voltage sensor High Critical | Syslog | Enabled | Yes | Critical | 0 | 1297 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 9. AKCP: DC Voltage sensor Low Critical | Syslog | Enabled | Yes | Critical | 0 | 1298 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 10. AKCP: DC Voltage sensor Low Warning | Syslog | Enabled | Yes | Major | 0 | 1300 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 11. AKCP: DC Voltage sensor returned to Normal Status | Syslog | Enabled | Yes | Healthy | 0 | 1301 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 12. AKCP: Dry Contact Sensor Low Critical | Syslog | Enabled | Yes | Critical | 0 | 1287 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 13. AKCP: Dry Contact sensor now Normal | Syslog | Enabled | Yes | Healthy | 2 | 1292 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 14. AKCP: Humidity High Warning | Syslog | Enabled | Yes | Major | 0 | 1295 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 15. AKCP: Humidity Low Warning | Syslog | Enabled | Yes | Major | 0 | 1296 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 16. AKCP: Smoke Detector Alert! | Syslog | Enabled | Yes | Critical | 10 | 1293 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 17. AKCP: Smoke detector now Normal Status | Syslog | Enabled | Yes | Healthy | 4 | 1289 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 18. AKCP: Water Sensor has detected water | Syslog | Enabled | Yes | Critical | 0 | 1291 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 19. AKCP: Water sensor now Normal | Syslog | Enabled | Yes | Healthy | 0 | 1290 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| 20. Alton: New Flash Enabled | Dynamic | Enabled | Yes | Notice | 0 | 36 | 30 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 21. Alton: Primary Power Supply Failure | Dynamic | Enabled | Yes | Major | 0 | 32 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 22. Alton: Primary Power Supply Healthy | Dynamic | Enabled | Yes | Healthy | 0 | 33 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 23. Alton: Redundant Power Supply Failure | Dynamic | Enabled | Yes | Major | 0 | 34 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 24. Alton: Redundant Power Supply Healthy | Dynamic | Enabled | Yes | Healthy | 0 | 35 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 25. APC: Batteries Do Not Need Replacement | Dynamic | Enabled | Yes | Healthy | 0 | 8 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 26. APC: Battery Charge Normal | Dynamic | Enabled | Yes | Healthy | 0 | 16 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 27. APC: Battery Run Time Remaining No Longer Critical | Dynamic | Enabled | Yes | Healthy | 0 | 10 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 28. APC: Battery Status | Dynamic | Enabled | Yes | Major | 0 | 15 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| 29. APC: Calibration Test Completed | Dynamic | Enabled | Yes | Healthy | 0 | 29 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| 30. APC: Calibration Test Did Not Complete | Dynamic | Enabled | Yes | Minor | 0 | 27 | 60 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |

2. The **Event Policy Manager** page displays the following about each event policy:

TIP: To sort the list of event policies, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Last Edited** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- **Event Policy Name.** The name of the event.
- **Type.** Specifies the source for the event. Possible values are:

- *Syslog*. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices like MoMs. A syslog is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.
 - *Internal*. Message is generated by a ScienceLogic process. The message is about the SL1 system itself, instead of the devices that the SL1 system monitors.
 - *Trap*. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like MoMs. An SNMP trap is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.
 - *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users 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. SL1 examines each new message in the device log and determines if the message matches an event definition. If it does, SL1 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 F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the SL1 system inserts a message in the associated device's log files, and the SL1 system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
 - *Email*. Message is generated by an email message sent to SL1. For more information on generating events with email messages, see the **Events from Email** chapter.
 - *API*. Message was 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 manual **Run Book Automation**. For more information on snippet Dynamic Applications, see the manual **Snippet Dynamic Application Development**. For more information on the ScienceLogic API, see the manual **Using the ScienceLogic API**.
 - *SL1 agent*. Message is generated by log file messages collected by the SL1 agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the **Monitoring Using the SL1 agent** manual. Monitoring
- **State**. Specifies whether 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. Choices are:
 - *Healthy*. Healthy events indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.
 - *Notice*. Notice events indicate a condition that does not affect service but about which users should be aware.

- *Minor*. Minor events indicate a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
 - *Major*. Major events indicate a condition that impacts service and requires immediate investigation.
 - *Critical*. Critical events indicate a condition that can seriously impair or curtail service and requires immediate attention (i.e., service or system outages).
- **Weight**. If two event definitions are very similar, the weight field specifies the order in which SL 1 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 will be matched first.
 - **ID**. Unique numeric ID for the event, generated by SL 1.
 - **Expiry**. If enabled, the time in which an active event will be 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 SL 1 , 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 SL 1 system where the event has a different event ID.
 - **Category**. The category for the event. This is an optional field. If SL 1 will be sending this event to an external system, this field defines the event category for use by the external system.

Filtering the List of Event Policies

The Filter-While-You-Type fields appear as a row of blank fields at the top of the list. These fields allow you to filter the items that appear in the list.

The list is dynamically updated as you select each filter. For each filter, you must make a selection from a drop-down menu or type text to match against. SL1 will search for entries that match the text, including partial matches. Text matches are not case-sensitive, and you can use special characters in each text field.

By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

You can filter by one or more of the following parameters. Only items that meet all of the filter criteria are displayed on the page.

The following describes each filter on the **Event Policy Manager** page:

- **Event Policy Name.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have a matching policy name.
- **Type.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have a matching source.
- **State.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have a matching state (enabled or disabled).
- **P-Pack.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that are or are not included in a PowerPack (yes or no).
- **Severity.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that are defined with a matching severity.
- **Weight.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies defined with a matching weight.
- **ID.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have a matching event policy ID.
- **Expiry.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have a matching expiry delay time.
- **Time.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have a matching occurrence time.
- **Thresh.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have a matching occurrence count.
- **Edited By.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have been created or edited by a matching user.
- **Last Edited.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Event Policy Manager** page will display only policies that have been created or last edited within the matching time span. Choices are:

- *All*. Display all event policies that match the other filters.
 - *Last Minute*. Display only event policies that have been created within the last minute.
 - *Last Hour*. Display only event policies that have been created within the last hour.
 - *Last Day*. Display only event policies that have been created within the last day.
 - *Last Week*. Display only event policies that have been created within the last week.
 - *Last Month*. Display only event policies that have been created within the last month.
 - *Last Year*. Display only event policies that have been created within the last year.
- **External ID**. You can enter text to match, including special characters, and the **Event Policy Manager** page will display only policies that have a matching external ID.
 - **Category**. You can enter text to match, including special characters, and the **Event Policy Manager** page will display only policies that have a matching category.

Special Characters

You can include the following special characters to filter by each column except those that display date and time:

NOTE: When searching for a string, SL1 will match substrings by default, even if you do not include any special characters. For example, searching for "hel" will match both "hello" and "helicopter". When searching for a numeric value, SL1 will not match a substring unless you use a special character.

String and Numeric

- , (comma). Specifies an "OR" operation. Works for string and numeric values. For example:
" dell, micro" matches all values that contain the string "dell" OR the string "micro".
- & (ampersand). Specifies an "AND " operation. Works for string and numeric values. For example:
"dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.

- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:

"!dell" matches all values that do not contain the string "dell".

"! ^ micro" would match all values that do not start with "micro".

"!fer\$" would match all values that do not end with "fer".

"! ^ \$" would match all values that are not null.

"! ^ " would match null values.

"!\$" would match null values.

"!*" would match null values.

"happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

NOTE: You can also use the "!" character in combination with the arithmetic special characters (min-max, >, <, >=, <=, =) described below.

- * (asterisk). Specifies a "match zero or more" operation. Works for string and numeric values. For a string, matches any string that matches the text before and after the asterisk. For a number, matches any number that contains the text. For example:

"hel*er" would match "helpers" and "helicopter" but not "hello".

"325*" would match "325", "32561", and "325000".

"*000" would match "1000", "25000", and "10500000".

- ? (question mark). Specifies "match any one character". Works for string and numeric values. For example:

"!?ver" would match the strings "oliver", "levers", and "lover", but not "believer".

"135?" would match the numbers "1350", "1354", and "1359", but not "135" or "13502"

String

- ^ (caret). For strings only. Specifies "match the beginning". Matches any string that begins with the specified string. For example:

" ^ sci" would match "scientific" and "sciencelogic", but not "conscious".

" ^ happy\$" would match only the string "happy", with no characters before or after.

"! ^ micro" would match all values that do not start with "micro".

"! ^ \$" would match all values that are not null.

"! ^ " would match null values.

- \$ (dollar sign). For strings only. Specifies "match the ending". Matches any string that ends with the specified string. For example:

"ter\$" would match the string "renter" but not the string "terrific".

"^happy\$" would match only the string "happy", with no characters before or after.

"!fer\$" would match all values that do not end with "fer".

"!^\$" would match all values that are not null.

"!\$" would match null values.

NOTE: You can use both ^ and \$ if you want to match an entire string and only that string. For example, "^tern\$" would match the strings "tern" or "Tern" or "TERN"; it would not match the strings "terne" or "cistern".

Numeric

- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:

"1-5" would match 1, 2, 3, 4, and 5.

- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:

"1-" matches 1 and greater. So would match 1, 2, 6, 345, etc.

"-5" matches 5 and less. So would match 5, 3, 1, 0, etc.

- > (greater than). Matches numeric values only. Specifies any value "greater than". For example:

">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than". For example:

"<12" would match all values less than 12.

- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to". For example:

">=7" would match all values 7 and greater.

- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to". For example:

"<=12" would match all values 12 and less.

- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:

"=-5" would match "-5" instead of being evaluated as the "half open range" as described above.

Additional Examples

- "aio\$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo\$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!O\$". Matches only text that does not end with "O".
- "!^silo\$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!. Matches null values, typically represented as "--" in most pages.
- " !\$". Matches null values, typically represented as "--" in most pages.
- " !^\$. Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s*i*i*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would match.
- " !^s*i*i*o\$". Matches all text that does not contain the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol" and it does contain "02".
- "aggr,!vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr,!vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "*". Matches all text.
- " !*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- " !silo ". Matches text that does not contain "silo".
- " !^silo\$ ". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.

- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "1n", and "2n".
- "n*SAN". Matches text the contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".
- "^?n*SAN\$". Matches text that begins with any single character, is following by "n", and then zero or any number of any characters, and ends in "SAN".

Defining an Event Policy

SL1 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, 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 Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, click the **[Create]** button. The **Event Policy Editor** page appears:

The screenshot shows the 'Event Policy Editor | Create New Event Policy' window. It has a top navigation bar with 'New', 'Reset', and 'Guide' buttons. Below this are three tabs: 'Policy', 'Advanced', and 'Suppressions'. The 'Policy' tab is active and contains several fields: 'Event Source' (a dropdown menu with 'Syslog' selected), 'Operational State' (a dropdown menu with '[Enabled]' selected), and 'Event Severity' (a dropdown menu with '[Major]' selected). There is also a 'Use Modifier' checkbox. To the right of these fields are 'Policy Name' and 'Event Message' text input fields. Below the 'Event Message' field is a 'Policy Description' section with a rich text editor toolbar (including bold, italic, underline, strikethrough, text color, background color, bulleted list, numbered list, link, unlink, and code icons) and a large text area containing the placeholder text 'Start typing ...'. At the bottom center of the window is a 'Save' button.

3. In 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 will not appear in the **Event Console** page or the **Viewing Events** page for the device.

Defining Basic Event Parameters in the Policy Tab

In 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:

The screenshot shows the 'Event Policy Editor | Create New Event Policy' window with the 'Policy' tab selected. The 'Event Source' is set to 'Internal', 'Operational State' is 'Enabled', and 'Event Severity' is 'Major'. The 'Policy Name' is 'Poller: Device not responding' and the 'Event Message' is '%M %N'. The 'Policy Description' field contains the following text:

Event Definition: The poller was not able to establish SNMP communications with the referenced device.

Probable Cause: The device may be unavailable or a change may have occurred to the system's device properties (e.g., community string or IP). This event can apply to any device that is being polled and is generated from the polling engine.

A 'Save' button is located at the bottom center of the window.

- **Event Source**. Specifies the source for the event. Choices are:
 - *Syslog*. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices like MoMs. A syslog is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.
 - *Internal*. Message is generated by a ScienceLogic process. The message is about the SL1 system itself, instead of the devices that the SL1 system monitors.

- *Trap*. Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like MoMs. An SNMP trap is an unsolicited message from a device to SL1. 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 manual **Syslogs and Traps**.
- *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users 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. SL1 examines each new message in the device log and determines if the message matches an event definition. If it does, SL1 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 F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the SL1 system inserts a message in the associated device's log files, and the SL1 system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
- *Email*. Message is generated by an email message sent to SL1. For more information on generating events with email messages, see the **Events from Email** chapter.
- *API*. Message was 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 manual **Run Book Automation**. For more information on snippet Dynamic Applications, see the manual **Snippet Dynamic Application Development**. For more information on the ScienceLogic API, see the manual **Using the ScienceLogic API**.
- *SL1 agent*. Message is generated by log file messages collected by the SL1 agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the **Monitoring Using the SL1 agent** manual.
- *Rules Engine*. Message generated by the SL1 agent, based on a set of event rules (applies only to Pod systems).

NOTE: Currently, users cannot create or edit an event with a **Source** of *Rules Engine*.

- **Policy Name**. The name of the event. Can be any combination of alphanumeric characters, up to 48 characters in length.
- **Operational State**. Specifies whether event is to be operational or not. Choices are *Enabled* or *Disabled*.
- **Event Message**. The message that appears in the **Event Console** page or the **Viewing Events** page when this event occurs. 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
```

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.

SL1 will use the regular expression to search the log message and use the matching text in the event message.

For details on the regular expression syntax allowed by SL 1, see <http://www.python.org/doc/howto/>.

- You can also use the following variables in this field:
 - %I ("eye"). For events with a source of "dynamic", this variable contains the index value from SNMP; this index value will be displayed 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:

```
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.
```

In this case, %I would return .1.1, .2.1, and .3.1, respectively.

- %I ("eye"). For events with a source of "syslog" or "trap", this variable contains the value that matches the **Identifier Pattern** field in the **[Advanced]** tab.
- %M. The full text of the log message that triggered the event will be displayed in **Event Message** field.
- %V. Data Value from log file will be displayed in the **Event Message** field.
- %T. Threshold value from the log file will be 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. Choices are:
 - *Healthy.* Healthy events indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.
 - *Notice.* Notice events indicate a condition that does not affect service but about which users should be aware.
 - *Minor.* Minor events indicate a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
 - *Major.* Major events indicate a condition that impacts service and requires immediate investigation.

- **Critical.** Critical events indicate a condition that can seriously impair or curtail service and requires immediate attention (i.e., service or system outages).
- **Use Modifier.** If selected, when the event is triggered, SL1 will check to see if the interface associated with this event has a custom severity modifier. If so, the event will appear 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 will appear 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

The **[Advanced]** tab in the **Event Policy Editor** page allows you 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 SL1 will create 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 SL1 will generate 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, SL1 will create a new event message on the **Events** page. On the **Events** page, the **Age/Elapsed** column will specify the time since the very first occurrence of the event, even though that occurrence did not appear on the **Events** page. The **Count** column will specify 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 will be 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 SL1 should match messages against the similar event definitions. The event definition with the lowest weight will be 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 SL1 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:
 - Will match the expression:

KTLD [ERROR]
 - Has a weight of "10"
- Event 2:
 - Will match the two expressions:

KTLD [ERROR]

and

exception 347

Has a weight of "5"

Both event definitions match the log message. However, SL1 uses only the event definition with the lowest weight. So SL1 would first validate the incoming message against Event 2.

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

NOTE: The **Log Policy** field appears only when you select SL1 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 SL1.

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 will include 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 will include 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 SL1. 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 will match 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 will include only traps that match the string.

NOTE: Before selecting a trap OID, check the **SNMP Trap Filters** page (Registry > Events > SNMP Trap Filters) to be sure that the trap is not being filtered out. For more information on the **SNMP Trap Filters** page, see the *Syslogs and Traps* manual.

- **Source Host Varbind.** For events with a source of "trap," specifies an OID that is included in the trap. This OID will contain 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 SL1, see the manual *Syslogs and Traps*.
 - If a value is specified in this field, SL1 examines the OID specified in this field. If the value stored in the OID matches the primary IP address of a device in SL1, the resulting event will be aligned with that device.
 - If a value is specified in this field, SL1 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 SL1, the resulting event will be aligned with the device that sent the trap.
 - If no value is specified in this field, but the trap includes the default snmpTrapAddress OID, SL1 will examine 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 SL1, the resulting event will be aligned with that device.
 - If no value is specified in this field and the trap does not include the snmpTrapAddress OID, SL1 will align 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 <http://www.rfc-archive.org/getrfc.php?rfc=5424>.

- **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 SL1 will be sending 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 SL1 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 manual on **Run Book Automation**.
- **External Category.** Optional. If SL1 will be sending 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 manual on **Run Book Automation**.
- **Match Logic.** Specifies whether SL1 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, SL1 will match a log message or alert to only one event policy. If a log message or alert matches multiple event policies, SL1 will use the **Detection Weight** setting to determine which event policy the log message or alert will match. If you select the **Use Multi-match** checkbox in all events that can match the same log message or alert, SL1 will generate an event for every event policy that matches that single log message or alert.
- **Use Message-match.** If SL1 has generated an event and then a second log message or alert matches the same event policy for the same entity, SL1 will not generate a second event, but will increase 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 will occur 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. SL1'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 SL1 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 SL1'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, SL1 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. SL1 will assign 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, s01) and is unique on the device, but is not unique in SL1.

NOTE: SL1's expression matching is case-sensitive.

For details on the regular-expression syntax allowed by SL1, 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 (e.g. Interfaces = 7). If SL1 knows an interface's "yName" (specified in the **Identifier Pattern** field) and the "yType" (specified in the **Override YType** field), SL1 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.** 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. This field is optional.
 - %1. First match with identifier pattern. This is the default behavior if no value is supplied in the **Identifier Format** field.
 - %2. Second match with identifier pattern.
 - etc.
 - For example, users could specify "%2:%1" for "Interface %2: Peer %1"

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 will be for an interface and will lead 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 Actions Policies and using Ticket Templates, see the section on *Creating an Action Policy that Creates a New Ticket* in the manual *Run Book Automation*.

- **Auto-Clear.** If enabled, this field specifies whether an event can be cleared from the event list automatically. You can select one or more events from the list. SL1 automatically removes the current event from the **Events** page if one of the selected events occurs.

For example, suppose you have an event "Device not responding to ping". If the next polling session produces the event "Device now responding normally to ping," the auto-clear feature could automatically clear the original event from the **Events** 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 alphanumeric string in the field, the **Auto-Clear** field will include 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. SL1 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 chapter on [event correlation](#) in the **Events** manual.

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, SL1 will search all related children devices for suppressible events.
 - If you have assigned a **Category** to this event, SL1 will search all the children devices and suppress all events that have been defined as *Suppressible* and are assigned to the same **Category**. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.
 - If you have not assigned a **Category** to this event, SL1 will search all children devices and suppress all events that have been defined as *Suppressible* and are not assigned to a **Category**. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.
 - The suppressible events will not appear on the **Events** page. They will be 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, SL1 will suppress 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 chapter on [event correlation](#) in the **Events** manual.
 - 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 SL1 will search all children devices and suppress all events that have been defined as *Suppressible* and are not assigned to a **Category**. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.
 - The suppressible events will not appear on the **Events** page. They will be 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 SL1 to more efficiently align suppressing events with suppressible events. When you align an event category to a suppressing or suppressible event, that event will be 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 chapter on [event correlation](#) in the **Events** manual.

NOTE: You can use the field at the top of the **Category** field to filter the list of events. If you enter an alphanumeric string in the field, the **Category** field will include only events that match the string.

NOTE: If you assign a topology category to an event that is neither suppressing nor suppressible, SL1 does not use the **Category**. The **Category** will have no effect.

- If you have assigned a **Category** to a *Suppressing* event, SL1 will search all the children devices and suppress 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 SL1 will search all children devices and suppress all events that have been defined as *Suppressible* and are not assigned to a **Category**.

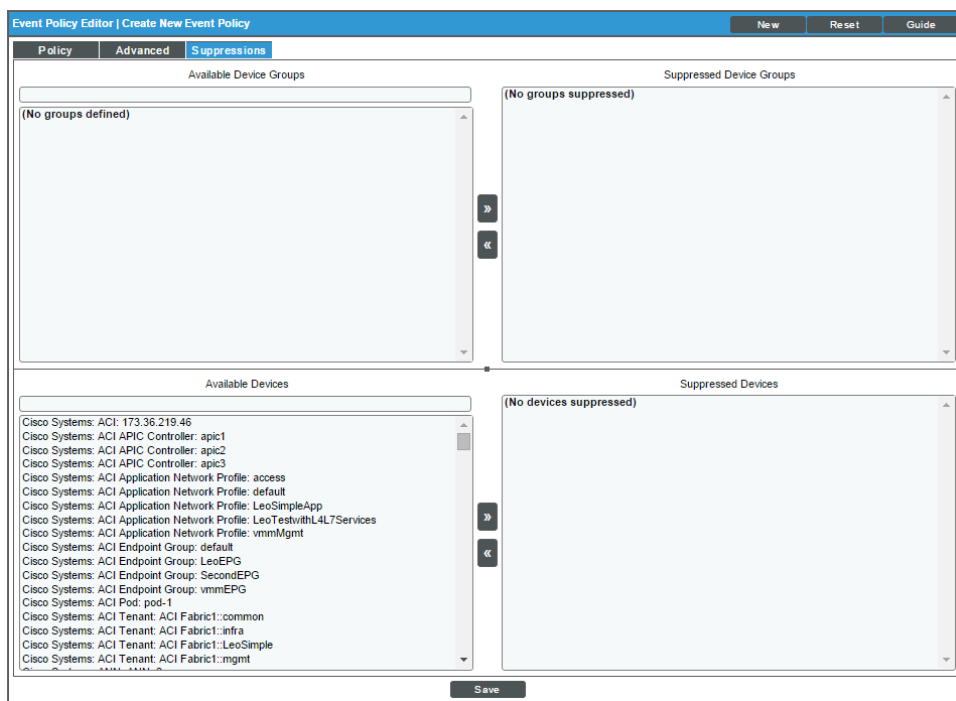
Defining EventSuppressions in the Suppressions Tab

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 will 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 will appear on the **Events** page.

NOTE: If you want to disable an event for all devices, see the section on [disabling an event](#) in the chapter on responding to events.

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 select 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 **Device Groups and Templates** manual.

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 will include only device groups that match the string.

NOTE: Device groups that have *Event/View Suppression* enabled will appear in this field. For information on creating device groups, see the **Device Groups and Templates** manual.

- **Suppressed Device Groups.** Device groups on which the event is already suppressed. For information on device groups, see the *Device Groups and Templates* manual.
- **Available Devices.** Devices on which you can suppress the current event. To suppress the current event on a device, highlight the device and select 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 will include 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.

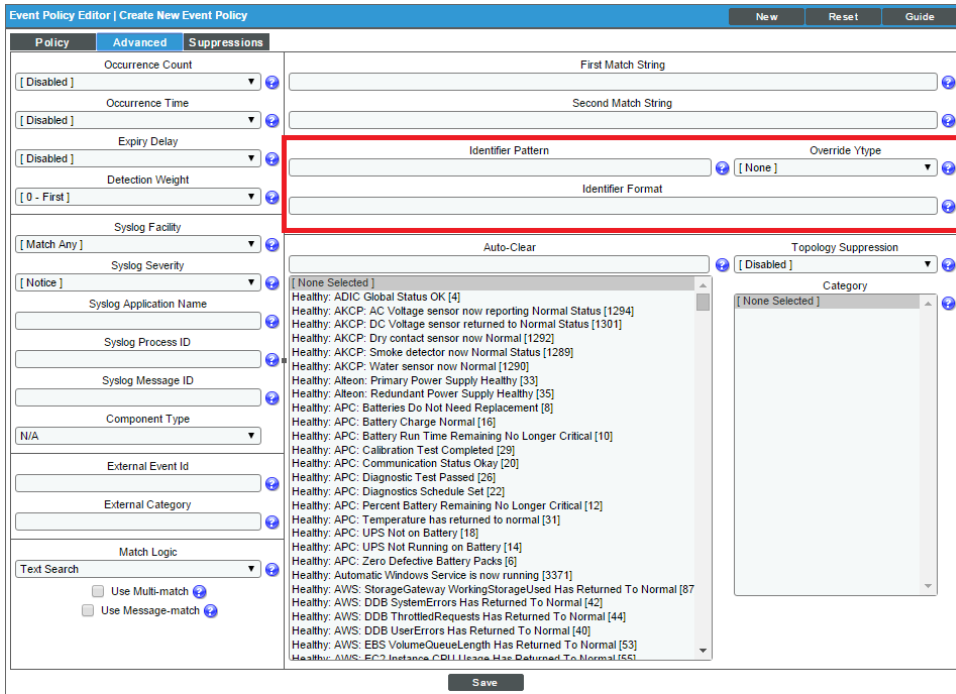
You can also include the interface name and SL1's unique interface ID in automation policies associated with the event.

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

There are three database fields that SL1 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 (e.g., 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 SL1.

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. SL1 will use this value as the yName of the interface. By identifying the sub-entity, SL1 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. SL1's expression matching is case-sensitive.

For details on the regular-expression syntax allowed by SL1, see <http://www.python.org/doc/howto/>.

- **Identifier Format.** 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. This field is optional.
 - %1. First match with identifier pattern. This is the default behavior if no value is supplied in the **Identifier Format** field.
 - %2. Second match with identifier pattern.
 - For example, users could specify "%2:%1" for "Interface %2: Peer %1".
- **Override YType.** Specifies a yType for the interface (yType for interfaces is 7). If SL1 knows the device name, the interface's yName (specified in the **Identifier Pattern** field) and the yType (specified in the **Override YType** field), SL1 can determine the unique yID for the interface.

If these fields are used in an event:

- On the **Events** page, the link icon for this event will be for an interface and will lead 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* in the manual **Run Book Automation**.

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 the chapter on *Network Interfaces* in the **Devices** manual.


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 will have an increased severity.

To define a custom severity for an interface:


1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).
2. Select 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. Select the **[Save]** button.

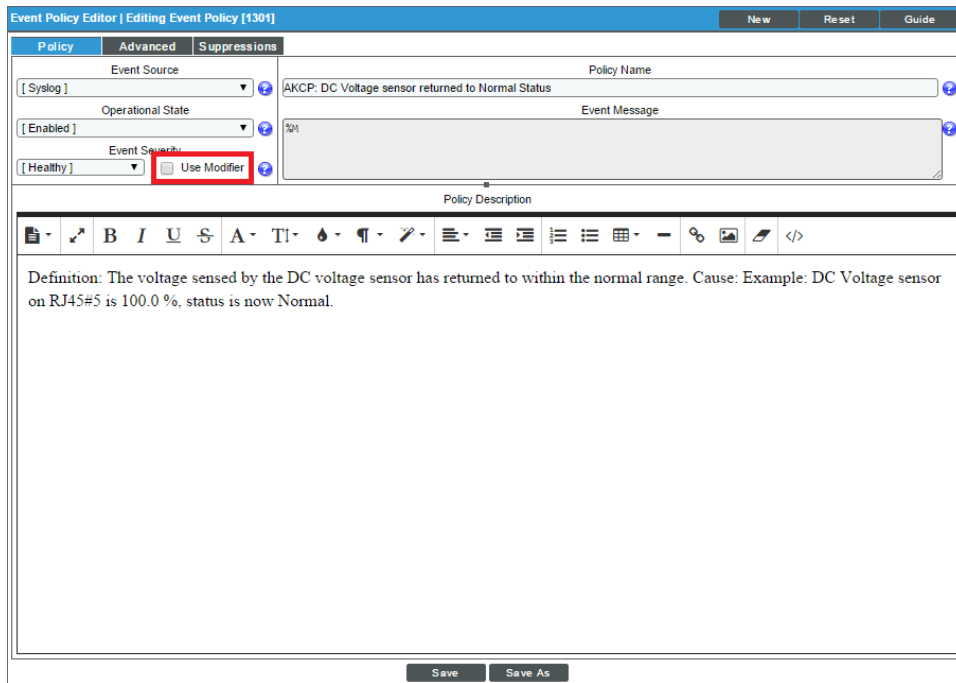
The screenshot shows the 'Interface Properties' window for interface 'e0a'. The window is titled 'Interface Properties' and has a subtitle 'For Interface [46]'. It contains several sections:

- Interface Information:** Interface Name (e0a), Port Description (e0a), MAC Address (00:A0:98:04:C5:4A / NetworkApp), IANA Type (ethernetCsmacd [6]), Speed & Counter (1000 Mbps. [Counter 32]), Position & IfIndex (1 / 1), Admin/Oper Status (Up / Up), and TCP IP Address (10.0.0.31 / 255.255.255.0 [10.0.0.0]).
- Configuration Section:** Interface Name (e0a), Naming (Set Name As: [e0a:0/1]), Interface Tags, Interface Speed (1000000000 [Bits]), Linked-Device ([None]), Linked-Interface, Collect State / Frequency ([Enabled] / [5 Min.]), Alerting / Pollers ([Enabled] / [Disabled]), **Event Severity Adjust ([Default Severity])** (highlighted with a red box), Errors / Discards ([Disabled] / [Disabled]), Measurement / Percentile ([Mega] / [Accumulative]), and Display on Summary.
- Thresholds Section:** Inbound % Threshold (65 % [Default: 65%]), Outbound % Threshold (65 % [Default: 65%]), Inbound [Mbps] Thresh. (0 Mbps. [Default: 0 Mbps.]), and Outbound [Mbps] Thresh. (0 Mbps. [Default: 0 Mbps.]).

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

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Select the wrench icon () for the event policy you want to edit.
3. Select the **[Policy]** tab.

4. In the **Event Policy Editor** page, select the **Use Modifier** checkbox .



5. Click **[Save]**.

Editing an Event Policy


SL1 includes pre-defined events for the most commonly encountered conditions on the most common platforms. SL1 allows you to customize these events to meet the needs of your organization. You can edit existing event policies in the **Event Policy Manager** page.

CAUTION: If you edit an event policy that was imported into your SL1 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 will be over-written. For more information on PowerPacks, see the manual **PowerPacks**.

To edit an existing event policy:

1. Go to the **Event Policy Manager** page (Events > Event Policies).

| Event Policy Name | Type | State | P-Pack | Severity | Weight | ID | Expiry | Time | Threshold | Edited By | Last Edited | External ID | Category |
|---|---------|---------|--------|----------|--------|------|---------|--------|-----------|-----------|---------------------|-------------|----------|
| ADIC Global Status Failed | Dynamic | Enabled | Yes | Major | 0 | 2 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| ADIC Global Status OK | Dynamic | Enabled | Yes | Healthy | 0 | 4 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| ADIC Global Status Unknown | Dynamic | Enabled | Yes | Notice | 0 | 3 | 30 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| ADIC Tape Library Degraded | Dynamic | Enabled | Yes | Minor | 0 | 1 | 60 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| AKCP: AC Voltage sensor detects no current | Syslog | Enabled | Yes | Critical | 0 | 1288 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: AC Voltage sensor now reporting Normal Status | Syslog | Enabled | Yes | Healthy | 0 | 1294 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: DC Voltage High Warning | Syslog | Enabled | Yes | Minor | 0 | 1299 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: DC Voltage sensor High Critical | Syslog | Enabled | Yes | Critical | 0 | 1297 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: DC Voltage sensor Low Critical | Syslog | Enabled | Yes | Critical | 0 | 1298 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: DC Voltage sensor Low Warning | Syslog | Enabled | Yes | Major | 0 | 1300 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: DC Voltage sensor returned to Normal Status | Syslog | Enabled | Yes | Healthy | 0 | 1301 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Dry Contact Sensor Low Critical | Syslog | Enabled | Yes | Critical | 0 | 1287 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Dry contact sensor now Normal | Syslog | Enabled | Yes | Healthy | 2 | 1292 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Humidity High Warning | Syslog | Enabled | Yes | Major | 0 | 1295 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Humidity Low Warning | Syslog | Enabled | Yes | Major | 0 | 1296 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Smoke Detector Alert! | Syslog | Enabled | Yes | Critical | 10 | 1293 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Smoke detector now Normal Status | Syslog | Enabled | Yes | Healthy | 4 | 1288 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Water Sensor has detected water | Syslog | Enabled | Yes | Critical | 0 | 1291 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| AKCP: Water sensor now Normal | Syslog | Enabled | Yes | Healthy | 0 | 1290 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:25:44 | -- | -- |
| Alteon: New Flash Enabled | Dynamic | Enabled | Yes | Notice | 0 | 36 | 30 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| Alteon: Primary Power Supply Failure | Dynamic | Enabled | Yes | Major | 0 | 32 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| Alteon: Primary Power Supply Healthy | Dynamic | Enabled | Yes | Healthy | 0 | 33 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| Alteon: Redundant Power Supply Failure | Dynamic | Enabled | Yes | Major | 0 | 34 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| Alteon: Redundant Power Supply Healthy | Dynamic | Enabled | Yes | Healthy | 0 | 35 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| APC: Batteries Do Not Need Replacement | Dynamic | Enabled | Yes | Healthy | 0 | 8 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| APC: Battery Charge Normal | Dynamic | Enabled | Yes | Healthy | 0 | 16 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| APC: Battery Run Time Remaining No Longer Critical | Dynamic | Enabled | Yes | Healthy | 0 | 10 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| APC: Battery Status | Dynamic | Enabled | Yes | Major | 0 | 15 | 90 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:53 | -- | -- |
| APC: Calibration Test Completed | Dynamic | Enabled | Yes | Healthy | 0 | 29 | 15 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |
| APC: Calibration Test Did Not Complete | Dynamic | Enabled | Yes | Minor | 0 | 27 | 60 Min. | 0 Min. | 0 | em7admin | 2015-05-14 11:24:54 | -- | -- |

2. In the **Event Policy Manager** page, select 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 will 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 will 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 SL1 systems and to download customized content from ScienceLogic. For details on creating and using PowerPacks, see the manual **PowerPacks**.
- When creating new **event definitions**, make sure to set the **Event Source** field to the type of message you will be working with.
- **Regular-expression matching** in SL1 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.

Event Notification and Event Automation

Overview

SL1 includes automation features that allow you to define specific event conditions and the actions you want SL1 to execute when those event conditions are met.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ()
- To view a page containing all of the menu options, click the Advanced menu icon ()

This chapter provides an overview of these features, and it includes the following topics:

| | |
|---|----|
| <i>Automation Policies</i> | 78 |
| <i>Action Policies</i> | 79 |
| <i>Creating Automation Policies and Action Policies</i> | 79 |

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 is 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.
- Event(s) 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).
- Specific amount of time that must elapse while the status does not change.

The screenshot shows the 'Automation Policy Editor' interface. At the top, there's a title bar 'Automation Policy Editor | Editing Automation Policy [2]' and a 'Reset' button. The main area is divided into several sections:

- Policy Name:** A text input field with 'Apply Template' as a placeholder.
- Policy Type:** A dropdown menu set to '[Active]'.
- Policy State:** A dropdown menu set to '[Enabled]'.
- Organization:** A dropdown menu set to '[System]'.
- Criteria Logic:** A dropdown menu set to '[Severity >=]'.
- Match Logic:** A dropdown menu set to '[Text search]'.
- Match Syntax:** A text input field.
- Repeat Time:** A dropdown menu set to '[Only once]'.
- Align With:** A dropdown menu set to '[Devices]'.
- Include events for entities other than devices (organizations, assets, etc.):** A checkbox that is currently unchecked.
- Available Devices:** A list of devices including 'Deep Thought', 'ScienceLogic, Inc.: EM7 Database: em7', 'System', 'Avocent: OEM: acs-dev-001', and 'Cisco Systems: 2811: Cisco_10.0.9.32.yourdomain.com'.
- Aligned Devices:** A list containing '(All devices)'.
- Available Events:** A list of events including 'Critical: AKCP: AC Voltage sensor detects no current', 'Critical: AKCP: DC Voltage sensor High Critical', 'Critical: AKCP: DC Voltage sensor Low Critical', 'Critical: AKCP: Dry Contact Sensor Low Critical', and 'Critical: AKCP: Smoke Detector Alert'.
- Aligned Events:** A list containing 'Notice: Poller: Added application monitoring for device'.
- Available Actions:** A list of actions including 'Send Email: Send Email', 'SNMP Trap: EM7 Event Trap', 'Snippet: Apply Device Template', 'Snippet: EM7 Ping Snippet', and 'SQL Query: Apply Device Template'.
- Aligned Actions:** A list containing '1. Snippet: Apply Device Template'.

At the bottom of the interface, there is a 'Save' button.

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 SL1 when certain criteria are met. The triggers are defined in an automation policy (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 SL1 to an external device.
- Create a new ticket (using ticket templates defined in Registry > Ticketing > Templates page).
- 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).

Creating Automation Policies and Action Policies

For details on creating automation policies and action policies, see the manual *Using Run Book Automation*.

Chapter

8

Events from Email

Overview

SL1 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 SL1, 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 SL1 to trigger events from those log entries.

Configuring Events from Email

To configure SL1 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 SL1 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 SL1.
- In the **Mailer Redirection** page (Events > Inbound Email), define an email originator policy.
- Configure the third-party system to send event messages to SL1 via email.
- Define events based on incoming email messages. In the **Event Policy Editor** page (Events > Event Policies > create or edit), in the **Event Source** field, select *Email*.

For detailed instructions on how to complete each of these steps, see the chapter on *Events from Email* in the manual *Inbound Email*.



RSS Feeds and Events

Overview

SL1 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 SL1 and configure SL1 to create an event each time the external RSS feed is updated.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter will describe how to define and use each type of RSS feed:

| | |
|---|-----------|
| Viewing Events with an RSS Feed | 82 |
| Defining a Custom RSS Feed | 82 |
| <i>Editing a Custom RSS Feed</i> | 84 |
| Viewing a Custom RSS Feed | 85 |
| Defining an External RSS Feed to Trigger Events | 86 |
| <i>Viewing the List of Monitored RSS Feeds</i> | 87 |
| <i>Defining an RSS Feed to Monitor</i> | 87 |
| <i>Editing a Monitored RSS Feed</i> | 88 |
| <i>Viewing Articles from an RSS Feed</i> | 89 |
| <i>Performing Administrative Tasks on One or More Monitored RSS Feeds</i> | 90 |

Viewing Events with an RSS Feed

Custom RSS feeds allow you to view information about tickets and events without being logged in to SL1. Custom RSS feeds from SL1 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. Select the **[Refresh]** button to clear any values from the fields in the editor pane.

| Feed Name | Feed ID | Ticket Status | Ticket Severity | Enabled | Ticket Assigned | Event Sev | Event Age | Unsub'd Events |
|-----------|---------|---------------|-----------------|---------|-----------------|-----------|-----------|----------------|
| Test | 1 | Open | Healthy | Enabled | Ticket Assigned | Healthy | 0 hours | Disabled |

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

the chapter on *Ticket Queues* in the **Ticketing** manual.

- **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 tickets 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. For details on acknowledging events, see the [section on acknowledging events](#).
 - **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 tickets will be included in the RSS feed.
 - *Notice.* Healthy tickets will **not** be included in the RSS feed.
 - *Minor.* Healthy tickets and Notice tickets will **not** be included in the RSS feed.
 - *Major.* Healthy, Notice, and Minor tickets will **not** be included in the RSS feed.
 - *Critical.* Healthy, Notice, Minor, and Major tickets 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.

The screenshot shows the 'Custom RSS Feeds' configuration interface. It is divided into two main panes. The top pane contains configuration options for a selected RSS feed, including 'Global Settings' (Feed Name), 'Ticket Settings' (Ticket Queues, Assigned Only, Status, Minimum Severity), and 'Event Settings' (For Organization, Unacknowledged Only, Age Less than, Minimum Severity, Device Group Filter). The bottom pane is a table titled 'RSS Feeds' with columns for Feed Name, Feed ID, Ticket Status, Ticket Severity, Ticket Assigned, Event Sev, Event Age, and Unack'd Events. A red circle highlights a wrench icon in the first row of the table.

| Feed Name | Feed ID | Ticket Status | Ticket Severity | Ticket Assigned | Event Sev | Event Age | Unack'd Events |
|-----------|---------|---------------|-----------------|-----------------|-----------|-----------|----------------|
| | 1 | Open | Healthy | Enabled | Healthy | 0 Hours | Disabled |

3. Select the wrench icon () of the RSS feed you want to edit.
4. The top pane will be 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. Select the bomb icon (🧨) of the RSS feed you want to delete.

| Feed Name | Feed ID | Ticket Status | Ticket Severity | Ticket Assigned | Event Sev | Event Age | Unack'd Events |
|-----------|---------|---------------|-----------------|-----------------|-----------|-----------|----------------|
| Test | 1 | Open | Healthy | Enabled | Healthy | 0 Hours | Disabled |


4. The RSS feed will be deleted from SL1.

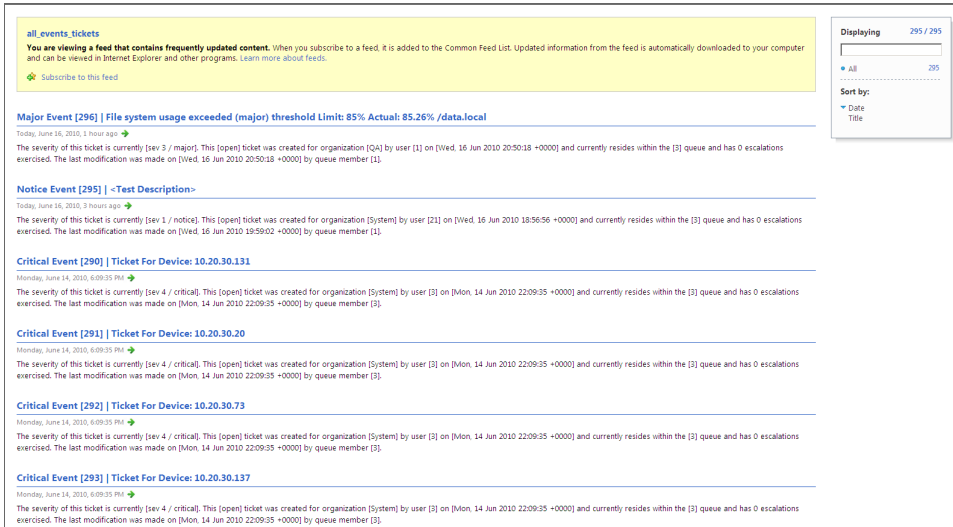
Viewing a Custom RSS Feed

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

To view a 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. Select the RSS icon () of the RSS feed you want to view.



The screenshot shows an RSS feed interface. At the top, there is a yellow banner with the text: "all events, tickets. You are viewing a feed that contains frequently updated content. When you subscribe to a feed, it is added to the Common Feed List. Updated information from the feed is automatically downloaded to your computer and can be viewed in Internet Explorer and other programs. Learn more about feeds." Below this is a "Subscribe to this feed" link. The main content area lists several entries, each with a heading and a brief description. The entries are: "Major Event [296] | File system usage exceeded (major) threshold Limit: 85% Actual: 85.26% /data.local", "Notice Event [295] | <Test Description>", "Critical Event [290] | Ticket For Device: 10.20.30.131", "Critical Event [291] | Ticket For Device: 10.20.30.20", "Critical Event [292] | Ticket For Device: 10.20.30.73", and "Critical Event [293] | Ticket For Device: 10.20.30.137". On the right side, there is a control panel with "Displaying 295 / 295", a dropdown menu set to "All" with "295" items, and a "Sort by:" section with options for "Date" and "Title".

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 the user to the SL1 appliance where the ticket resides. Depending upon key privileges, users 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 SL1.

Defining an External RSS Feed to Trigger Events

You can view and monitor external RSS feeds from SL1. In SL1, you define one or more RSS feeds to monitor. You can then view the feeds directly from SL1. When new items are added to the feed, SL1 can generate an event to notify users. So SL1 allows you to:

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

SL1 allows you to monitor the following types of RSS feeds:

- RSS 1.0+
- RSS 2.0+
- ATOM

The following sections will describe how to define and/or edit an external RSS feed to monitor, and how to view the feed from within SL1 .

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: To sort the list of RSS feeds, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Edit Date** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

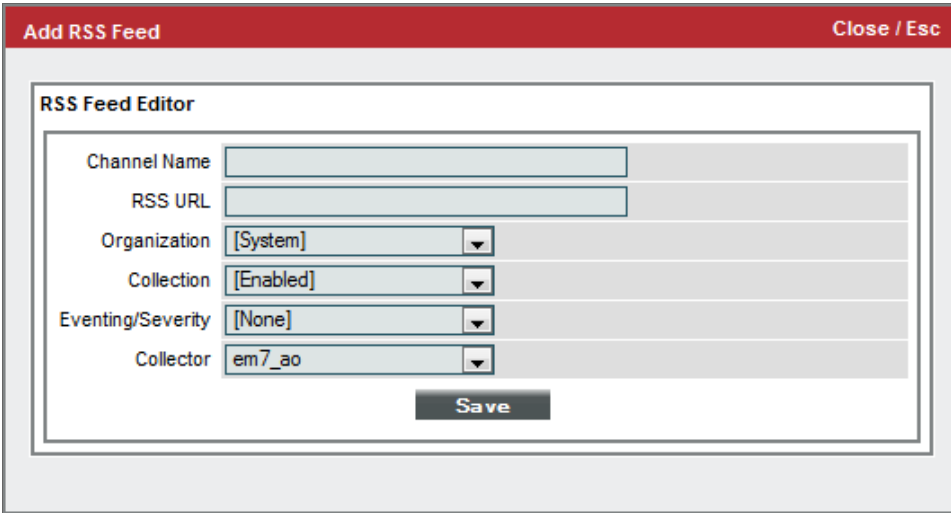
- **Channel Name.** Name of the RSS feed that is monitored by the policy.
- **Feed URI.** URL of the RSS feed.
- **Organization.** Organization to associate with this monitoring policy.
- **Feed Count.** Specifies the number of articles in the feed.
- **State.** Specifies whether SL1 is currently retrieving 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 SL1 . 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, select the **[Create]** button.

3. The **RSS Feed Editor** modal page appears.



4. In the **RSS Feed Editor** modal page, 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 will appear 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 SL1 should retrieve data from the RSS feed. Choices are *Enabled* or *Disabled*.
 - **Eventing**. Specifies whether SL1 will create 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 will 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 will monitor 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:

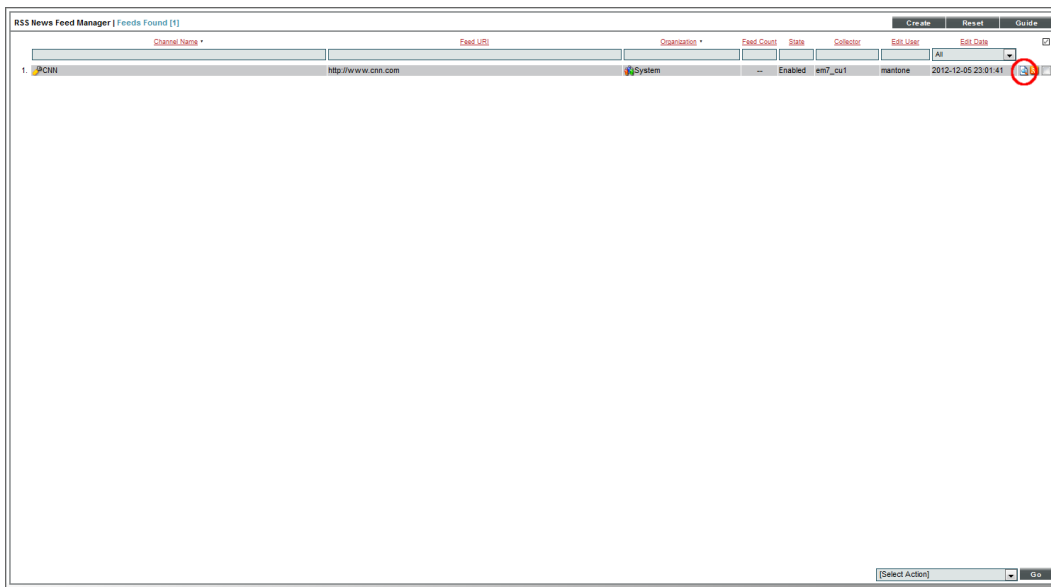
1. In the **RSS News Feed Manager** page, select the wrench icon (🔧) of the monitored RSS feed you want to edit.

2. The **RSS Feed Editor** page appears, populated with values from the monitored RSS feed you selected.
3. In the **RSS Feed Editor**, you can edit the values in one or more fields. For a description of each field, see the previous 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, select the page icon (📄) of the monitored RSS feed you want to view.



2. The **Article Catalog** page appears.

| Date | Title | Bookmark | |
|-------------------------|---|------------------------------|--|
| 1. 2012-12-05 23:10:00 | 'Call of Duty: Black Ops II': Disjointed but compelling | <input type="checkbox"/> [1] | |
| 2. 2012-12-05 23:10:00 | 'Gangnam' to 'Kony': 2012's top videos | <input type="checkbox"/> [1] | |
| 3. 2012-12-05 23:10:00 | 10 smartphone habits to avoid | <input type="checkbox"/> [1] | |
| 4. 2012-12-05 23:10:00 | 5 big tech issues await Obama in second term | <input type="checkbox"/> [1] | |
| 5. 2012-12-05 23:10:00 | Airport Wi-Fi and mobile services are lacking | <input type="checkbox"/> [1] | |
| 6. 2012-12-05 23:10:00 | An open letter to texting-mad teenagers | <input type="checkbox"/> [1] | |
| 7. 2012-12-05 23:10:00 | Five texts you should never send | <input type="checkbox"/> [1] | |
| 8. 2012-12-05 23:10:00 | How devices make us superhuman | <input type="checkbox"/> [1] | |
| 9. 2012-12-05 23:10:00 | iTunes11 finally available for download | <input type="checkbox"/> [1] | |
| 10. 2012-12-05 23:10:00 | Le blog: All the action from LeWeb Paris '12 | <input type="checkbox"/> [1] | |
| 11. 2012-12-05 23:10:00 | Lottery 'winner' a Facebook hoax | <input type="checkbox"/> [1] | |
| 12. 2012-12-05 23:10:00 | Microsoft opens a social network | <input type="checkbox"/> [1] | |
| 13. 2012-12-05 23:10:00 | OMG ... the text message turns 20 | <input type="checkbox"/> [1] | |
| 14. 2012-12-05 23:10:00 | Post-Katrina, New Orleans startups take flight | <input type="checkbox"/> [1] | |
| 15. 2012-12-05 23:10:00 | South Korea gaming: Skill or addiction? | <input type="checkbox"/> [1] | |
| 16. 2012-12-05 23:10:00 | Why the Pope and Obama turn to Twitter | <input type="checkbox"/> [1] | |

3. In the **Article Catalog** page, you can select and view articles from a monitored RSS feed. To view an article, select its globe icon (or).

News Feed Articles

Airport Wi-Fi and mobile services are lacking

Mobile technology is critical at the airport. Yet a new survey shows that most travelers are not satisfied with airport Wi-Fi. And airports are missing opportunities to offer vital mobile services.

[Email this](#) [Add to del.icio.us](#) [Digg This!](#) [Share on Facebook](#) [Stumble It!](#)

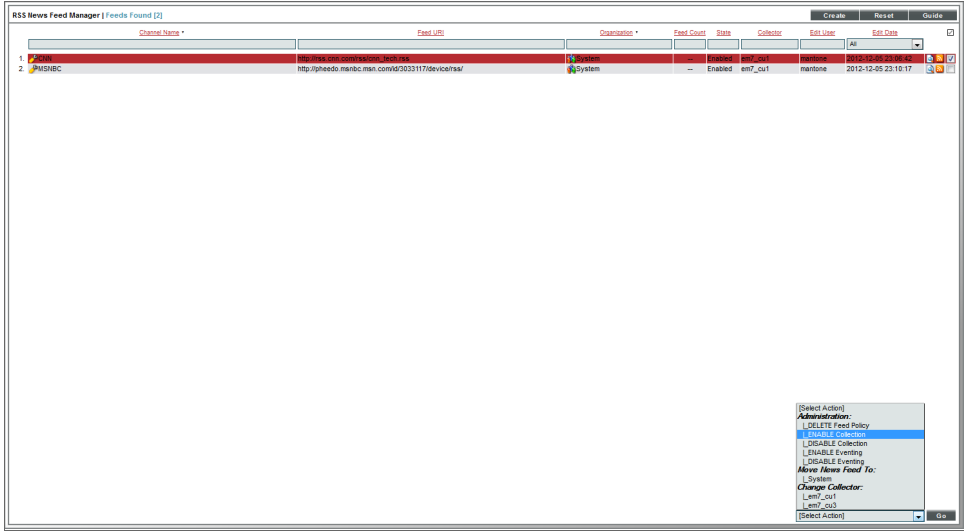
Copyright © 2003 - 2012 ScienceLogic, Inc. All rights reserved.

Performing Administrative Tasks on One or More Monitored RSS Feeds

SL1 allows you to edit multiple RSS feeds simultaneously. The **Select Action** drop-down list in the **RSS News Feed Manager** page (Events > RSS Feeds) allows you to apply an action to multiple monitored RSS feeds at once.

1. In the **RSS News Feed Manager** page (Events > RSS Feeds), select the checkbox for each RSS feed to which you want to apply the action. To select all checkboxes for all RSS feeds, select the checkbox icon at the top of the page.

TIP: To sort the list of RSS feeds, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Edit Date** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.



2. In the **Select Action** drop-down list, select one of the following actions:
 - *DELETE Feed Policy*. Deletes the monitored RSS feed. SL1 no longer monitors that RSS feed.
 - *ENABLE Collection*. SL1 will retrieve data from the selected news-feed policies.
 - *DISABLE Collection*. SL1 will not retrieve data from the selected news-feed policies.
 - *ENABLE Eventing*. SL1 will display an event when a new article is detected in the RSS feed.
 - *DISABLE Eventing*. SL1 will not display an event when a new article is detected in the RSS feed.
 - *Move News Feed To (list of organizations)*. Associate selected news feed policies with selected organization.
 - *Change Collector (list of collectors)*. Associate selected news feed policies with selected collector.
3. The selected action will be applied to each selected RSS feed.



Reports for Events

Overview

SL1 provides the following types of reports on events:

- **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 SL1.
- **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 Collection Server, or Message Collection Server.

Use the following menu options to navigate the SL1 user interface:

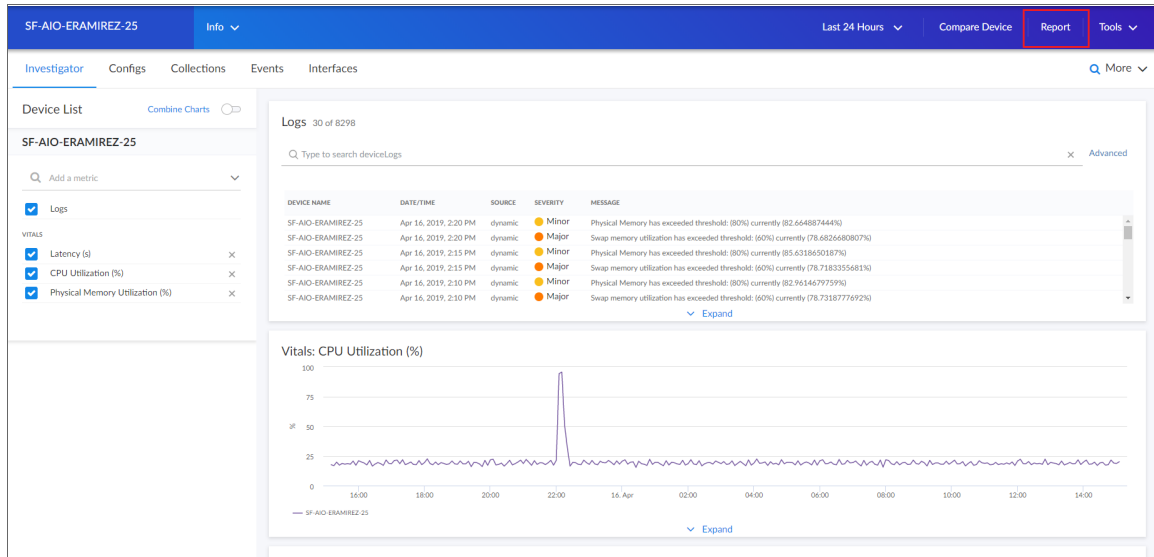
- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

The following sections describe each type of event report:

| | |
|---|-----|
| <i>Event Statistics for a Single Device</i> | 93 |
| <i>Event Reports in the Reports Tab</i> | 94 |
| <i>Event Overview Report</i> | 102 |
| <i>Event Statistics</i> | 103 |

Event Statistics for a Single Device

From the **Device Investigator** page, you can generate an Events report on that device.



1. On the **Device Investigator** page, click the **[Report]** button. The **Device Report** modal page appears.
2. In the **Select Type** drop-down, select **Events**.
3. In the **Select Format** drop-down, select the format for the report. Options include *HTML*, *PDF*, *DOC*, *XLS*, or *CSV*.
4. Click the **[Create Report]** button to generate the report.

The report appears displaying events that have occurred for that device, including the event message, severity, last occurrence, and the number of times that event has occurred.



Device Report For: SILO.qa.sciencelogic.local
May 14, 2019, 5:43 pm

Print Report

| Active Events | | | |
|---|----------|---------------------|---|
| Event Message | Severity | Last Occurance | |
| SSL Certificate Has Expired: (expires On: 2016-04-27 10:10:44) | Major | 2019-05-14 02:19:13 | 8 |
| Netapp: Cluster Logical Interface 'TEST_lif04' Has Moved From Its Home Node Or Port | Minor | 2019-05-14 17:36:26 | 3 |
| Netapp: Cluster Logical Interface 'TEST_lif06' Has Moved From Its Home Node Or Port | Minor | 2019-05-14 17:36:26 | 3 |
| Netapp: Cluster Logical Interface 'cluster_mgmt' Has Moved From Its Home Node Or Port | Minor | 2019-05-14 17:36:26 | 3 |

Event Reports in the Reports Tab

The **Reports** page (Reports > Reports) allows you to create custom reports as well as view predefined reports. SL1 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, SL1 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 can display 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 chapter on *Default Reports* in the **Reports** manual.

Input and Output for Quick Reports complies 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 will be organized. Choices are:
 - *Severity.* Events will be grouped by severity.
 - *Event Name.* Events will be listed alphabetically by event name. The secondary sort will be by severity.
 - *Event ID.* Events will be listed by event policy ID. Event ID is a unique numerical ID assigned by SL 1 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 will be included in the report. Choices are:
 - *Critical.* Has a value of "4" (four). When you select this severity, only events with the severity "4" are included in the report.
 - *Major.* Has a value of "3" (three). When you select this severity, events with severities 3-4 are included in the report.
 - *Minor.* Has a value of "2" (two). When you select this severity, events with severities 2-4 are included in the report.
 - *Notice.* Has a value of "1" (one). When you select this severity, events with severities 1-4 are included in the report.
 - *Healthy.* Has a value of "0" (zero). So when you select this severity, events of all severities are included in the report.

- **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 will include only events that are defined as auto-clear.
 - *Including non-cleared.* The generated report will include 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, Clearing Event.**
- **Output Format.** Select the format in which SL1 will save 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 will contain only the default columns: **Cleared Event, Severity, Direction, and Clearing Event.**

- **Cleared Event.** The name of the event.
- **Severity.** The severity of the event. Choices are Healthy, Notice, Minor, Major, and Critical.
- **Source.** Specifies the source for the event. Choices are:
 - *Syslog.* 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.
 - *Internal.* Message generated by SL1 .
 - *Trap.* SNMP trap. SNMP traps can be sent by devices and proxy devices like MoMs. An SNMP trap is an unsolicited message from a device to SL1 . A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device.
 - *Dynamic.* Message generated by SL1's Dynamic Application tool. This tool allows SL1 to monitor applications and devices that are not monitored by SNMP or other agents.
 - *Email.* Message was generated by an email from an external agent, for example, Microsoft Operations Manager (MOM).
 - *API.* Message was generated by another application and forwarded to SL1 with an integration API.

- **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 will be 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 will be included in the report.
 - **Organizations.** This list contains an entry for each organization in SL1. Events associated with each selected organization will be 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 will be included in this report.
- **Events.** This list contains an entry for each event in SL1.
 - 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 will be organized. Choices are:
 - *Event Name.* Events will be listed alphabetically by event name.
 - *Org/Device.* Events will be 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 will use 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 will be 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 will be 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 SL1 will save 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.

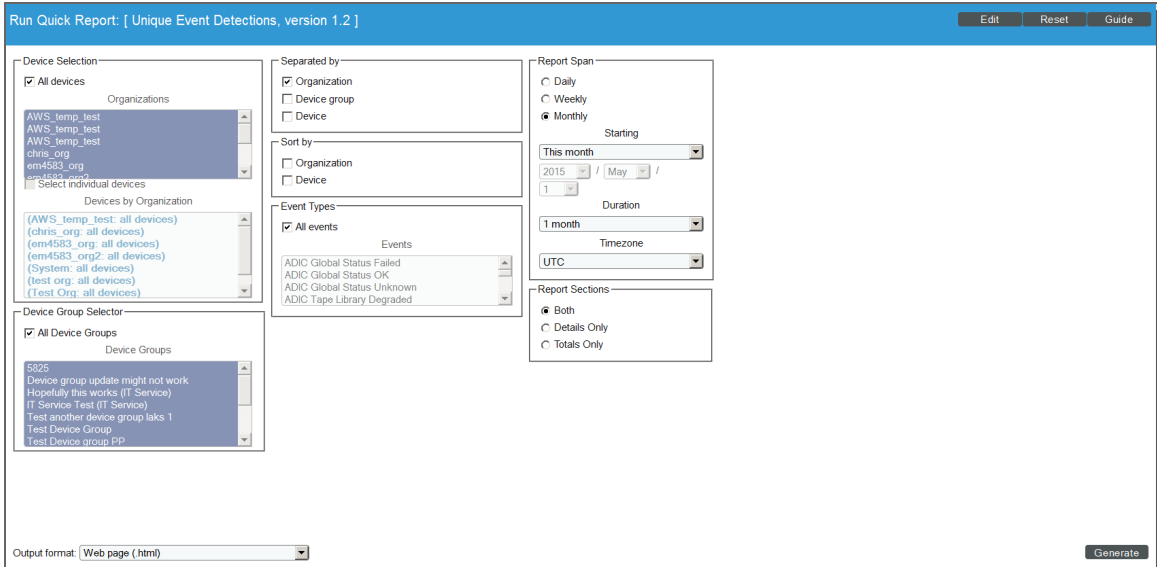
Unique Event Detections Report

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.

| Device | | Event Type | Jul 2015 | Total |
|----------------------------------|--|---|-----------|-----------|
| em7-4b1.lit [4] | | Net-SNMP: Physical Memory exceeded threshold | 1 | 1 |
| em7-4b1.lit [4] | | Poller: Added application monitoring for device | 2 | 2 |
| WIN-2012-22.DOCS.LOCAL [74] | | Poller: Availability Check Failed | 1 | 1 |
| WIN-2012-22.DOCS.LOCAL [74] | | Poller: Network Latency Exceeded Threshold | 1 | 1 |
| em7_ao [1067] | | Dynamic App Snippet Exception | 2 | 2 |
| em7_ao [1067] | | Poller: Added application monitoring for device | 2 | 2 |
| em7_ao [1067] | | Poller: Device or agent recently restarted | 1 | 1 |
| em7_ao [1067] | | Poller: Network Latency Exceeded Threshold | 1 | 1 |
| em7_ao [1067] | | Poller: Network Latency Healthy | 1 | 1 |
| MOSS_ISO_MC [1096] | | Poller: Availability Check Failed | 1 | 1 |
| MOSS_ISO_MC [1096] | | Poller: Network Latency Exceeded Threshold | 1 | 1 |
| MOSS_ISO_IS [1097] | | Poller: Availability Check Failed | 1 | 1 |
| MOSS_ISO_IS [1097] | | Poller: Network Latency Exceeded Threshold | 1 | 1 |
| MOSS_ISO_AP [1098] | | Poller: Availability Check Failed | 1 | 1 |
| MOSS_ISO_AP [1098] | | Poller: Network Latency Exceeded Threshold | 1 | 1 |
| MOSS_ISO_CU [1099] | | Poller: Availability Check Failed | 1 | 1 |
| MOSS_ISO_CU [1099] | | Poller: Network Latency Exceeded Threshold | 1 | 1 |
| Sum for Organization: TCP | | | 20 | 20 |

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 will 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 unselected, select one or more Organizations. The report will contain 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 unselected, 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 will 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 unselected, select one or more device groups. The report will contain 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 will appear in the report. The choices are:
 - *All events.* Select this checkbox to include all event types.
 - *Events.* If the All events checkbox is unselected, select one or more event types. The report will contain only the event types that you select.

Report Span. Specifies the time interval to use to select data for this report. The **Duration** field will use 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 will be 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 will be 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 will be arranged. Select whether you want the report to display *Details Only*, *Totals Only*, or *Both*.
 - **Output Format.** Select the format in which SL1 will save 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.** Display total number of unique events that occurred during the time period for each device group.
- **Sum for Device.** Display 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 SL1. 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

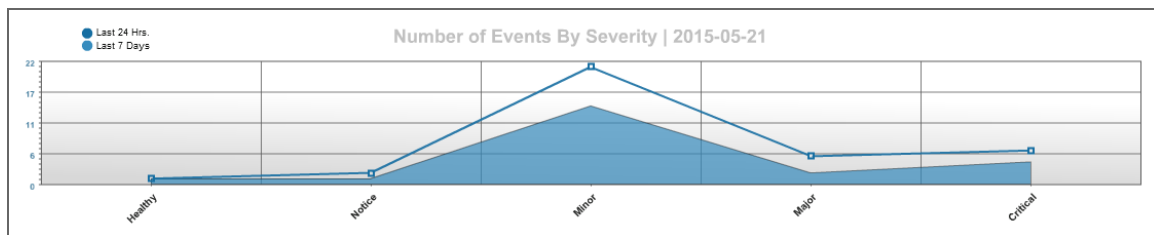
The **Event Overview** page includes a **Select Date** drop-down list in the upper right of the page. This drop-down allows you to define the date for the reports on this page.

- **Select Date.** Allows you to select a date. SL1 will generate 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, SL1 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.

Number of Events by Severity

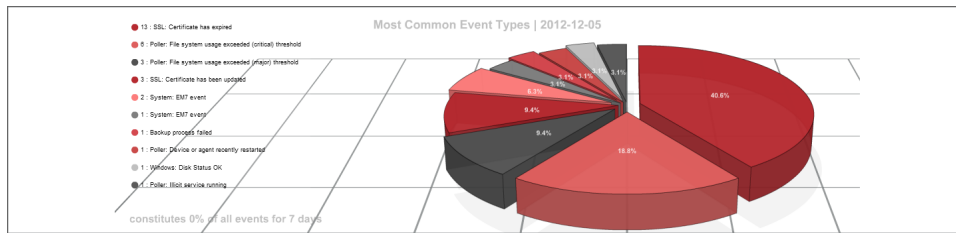
This graph displays event distribution by severity for the last 24 hours and for the last 7 days.



- The y-axis displays number of events.
- The x-axis displays severity.
- The blue line represents events in the last 24 hours.
- The blue solid area represents events in the last 7 days.
- Mousing over a data point in the red line displays the number of events of the specified severity in the last 24 hours.
- Mousing over the blue solid area displays the number of events of the specified severity in the last 7 days.

Most Common Event Types

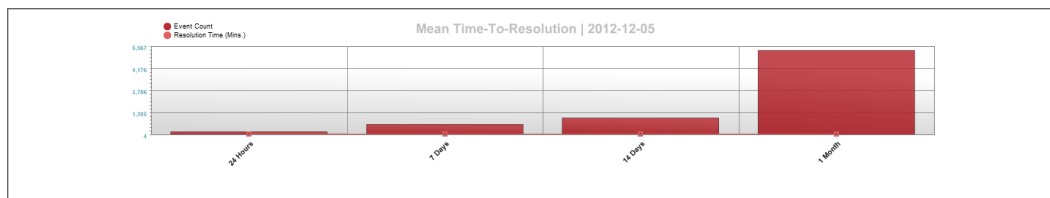
This pie graph displays the ten most frequently occurring events for the last seven days.



- Each slice of the pie represents an event type. The legend on the left maps slice color to event and lists the actual number of events of that type.
- The graph displays percent. Compared to the total number of occurrences for the top ten events, each slice displays the percent that belong to a specific event.

Mean Time-to-Resolution

This bar graph displays the number of events generated in the last 24 hours, 7 days, 14 days, and 30 days and their average resolution time.



- The y-axis displays number of events.
- The x-axis displays the time span. There is a bar for 24 hours, 7 days, 14 days, and 30 days.
- The bars represent the average number of events associated with the time-to-resolution.
- Mousing over a bar displays the number of events associated with the time-to-resolution.

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.

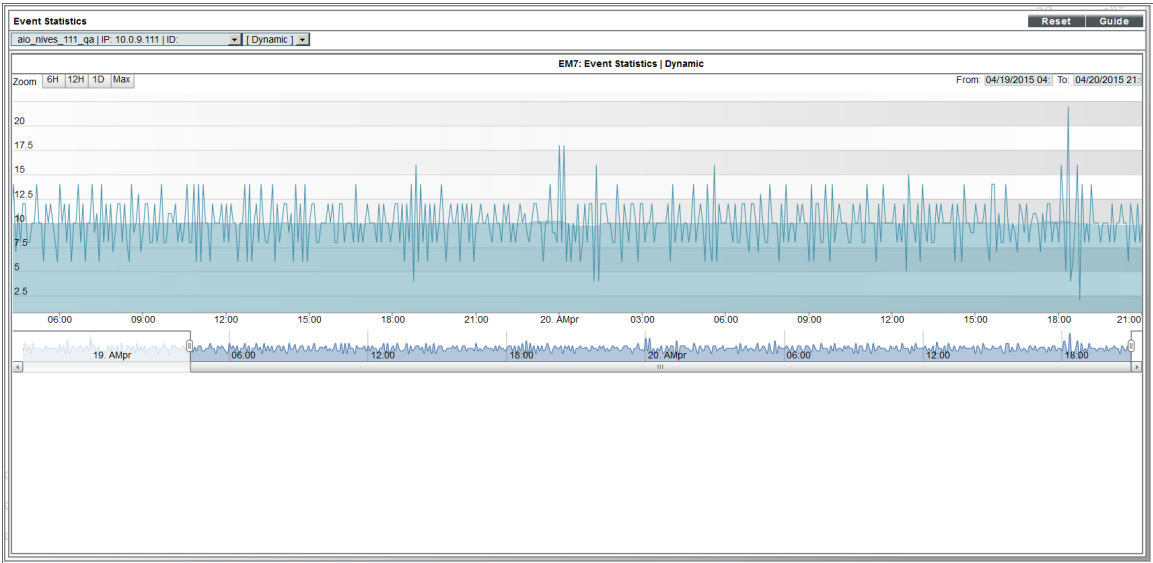
Fields

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. The choices are:
 - *Syslog*. Event was generated from a system log generated by a monitored device.
 - *Internal*. Event was generated by SL1.
 - *Trap*. Event was generated by an SNMP trap.
 - *Dynamic*. Event was generated by a Dynamic Application alert.
 - *API*. The event was generated by an external API.
 - *Email*. The event was generated by an incoming email.

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.

Settings that Affect Events

Overview

SL1 allows you to define default behavior for all events. You can do this by defining data retention settings and system settings.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ()
- To view a page containing all of the menu options, click the Advanced menu icon ()

This chapter includes the following topics:

| | |
|---|-----|
| <i>Data Retention Settings that Affect Events</i> | 107 |
| <i>System Settings that Affect Events</i> | 107 |

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. In the **Data Retention Settings** page, the system settings described below affect events:

The screenshot shows the 'Data Retention Settings' interface. It is divided into three main sections: System Data Retention, Collection Data Retention, and Subscription Data Retention. Each section contains a list of data types with a corresponding retention period and a 'Save' button. The 'Event Logs' setting in the System Data Retention section is highlighted with a red box, indicating its retention period is 3 months. Other settings include Audit Logs (3 months), Access Logs (12 months), System Logs (31 days), Collector Unit Data Buffer (2 days), Raw Performance Data (7 days), Hourly Rollup Performance Data (120 days), Daily Rollup Performance Data (24 months), Configuration Data (7 days), Journal Data (60 days), Bandwidth Data (31 days), Hourly Rollup Bandwidth Data (120 days), Daily Rollup Bandwidth Data (24 months), Bandwidth Billing Data (24 months), Device Logs Age (90 days), Device Logs Max (10000 records), Raw ITSM Data (31 days), ITSM Service Metrics Data (30 days), Hourly Rollup ITSM Service Metrics Data (120 days), Daily Rollup ITSM Service Metrics Data (12 months), ITSM Key Metrics Data (120 days), Hourly Rollup ITSM Key Metrics Data (365 days), Daily Rollup ITSM Key Metrics Data (24 months), and Subscriber Device Configuration Data (6 months).

- **Event Logs.** You can select the number of days that SL1 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. In the **Behavior Settings** page, the following system setting affects events:

The screenshot shows the 'Behavior Settings' page with various configuration options. The 'Event Clearing Mode' dropdown menu is highlighted with a red box, and the selected option is 'Clear All in Group'. Other settings include Interface URL, Password Expiration, Account Lockout Type, and various polling and timeout settings.

- **Event Clearing Mode.** Describes how clearing an event will affect 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 will appear on the **Events** page.

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010