



Events

SL1 version 11.1.0

Table of Contents

Introduction to Events	5
What is an Event?	5
How Are Events Triggered?	6
Viewing Events	7
Viewing Events in the Classic SL1 User Interface	8
Event Correlation	8
Defining Events	9
Event States	9
Viewing Events	11
Viewing the List of Events	12
Searching and Filtering the List of Events	12
Filtering Events by Organization and Service	12
Filtering Events by Severity	14
Filtering for Masked Events	15
Viewing Additional Data about an Event	16
Viewing Automation Actions	16
Refreshing the Events Page	17
Customizing the Events Page	18
Using the Event Investigator	19
Using the Action Runner	20
Viewing Events for a Single Device	22
Event Throttling	25
Viewing Events from the Event Console in the Classic SL1 User Interface	26
Events that Are Not Displayed in the Event Console	28
Information About Each Displayed Event	29
Global Search Field	31
Filter While You Type	33
Advanced Filter	35
Custom View	37
Viewing Events for a Single Device in the Classic SL1 User Interface	38
Viewing Events for a Single Organization	40
Viewing Event Details in the Event Console	43
Customizing the Display in the Event Console	45
Account Preferences	45
Event Console Preferences	50
Hiding the Header Bar	52
Event Masks in the Event Console	53
Responding to Events	54
Responding to Events	55
Selecting Multiple Events	55
Acknowledging and Clearing Events	56
Viewing and Editing Event Notes	57
Viewing the Event Policy	57
Suppressing and Unsuppressing an Event for a Device	58
Suppressing an Event	58
Suppressing an Event on Multiple Devices	59
Unsuppressing an Event	61
Unsuppressing All Instances of an Event	62
Enabling and Disabling Events	62
Disabling Events	63

Enabling Events	63
Creating a Ticket from an Event	64
Responding to Events in the Event Console in the Classic SL1 User Interface	65
Adding a Note About an Event	66
Adding a Note to Multiple Events	67
Clearing One or More Events	68
Suppressing an Event on a Single Device	70
Suppressing an Event On Multiple Devices	71
Unsuppressing an Event	73
Unsuppressing All Instances of an Event	74
Disabling an Event	75
Enabling an Event	76
Events and Tickets	78
Creating a Ticket from the List of Events	79
Event Ticket Behavior Settings	82
Integrating Events with External Tickets	83
External Tickets in the Events Page or Event Console	83
Using Run Book Automation to Populate the ScienceLogic Database with Values from External Tickets ..	84
Aligning an External Ticket with Multiple Events	84
Aligning an External Ticket with Multiple Events in the Classic User Interface	85
Event Correlation and Parent and Child Events	87
Event Correlation	88
Defining Parent and Child Devices	89
Device Categories that Don't Support Child Devices	91
Defining Event Topology Masking and Suppression	91
Defining Event Topology Suppression in the Classic SL1 User Interface	92
Example: Child Event Suppression	94
Event Categories	95
Assigning an Event Category to an Event	96
Assigning an Event Category to an Event in the Classic SL1 User Interface	97
Creating an Event Category	98
Editing an Event Category	98
Viewing the List of Event Categories	99
Filtering the List of Event Categories	100
Special Characters	101
Deleting One or More Event Categories	105
Defining and Editing Event Policies	106
How SL1 Generates Events	107
Viewing the List of Event Policies	108
Defining an Event Policy	110
The Match Logic Tab	112
The Event Message Tab	115
The Suppression Tab	119
Editing an Event Policy	121
Duplicating an Event Policy	122
Deleting an Event Policy	122
Selecting Multiple Event Policies	122
Using Event Policies in the Classic SL1 User Interface	123
Viewing the List of Event Policies in the Classic SL1 User Interface	124
Filtering the List of Event Policies in the Classic SL1 User Interface	126
Special Characters	128
Defining an Event Policy in the Classic SL1 User Interface	131

Defining Basic Event Parameters in the Policy Tab	133
Defining Pattern Matching and Advanced Behavior in the Advanced Tab	136
Defining Event Suppressions in the Suppressions Tab	144
Defining an Event Policy for a Specific Interface	146
Defining Custom Severity for an Interface	148
Editing an Event Policy in the Classic SL1 User Interface	150
Best Practices for Event Definitions	151
Event Notification and Event Automation	153
Automation Policies	153
Action Policies	154
Events from Email	156
Configuring Events from Email	156
Reports for Events	157
Event Statistics in the Event Console Page in the Classic SL1 User Interface	158
Event Statistics for a Single Device	162
Event Reports in the Reports Tab	164
Event Clear Map Report	164
Event Detections Report	167
Unique Event Detections Report	169
Event Overview Report	172
Setting the Date for Reports	172
Number of Events by Severity	172
Most Common Event Types	173
Mean Time-to-Resolution	173
Event Statistics	173
Defining the Date Range	174
Fields	174
The Graph	174
Settings that Affect Events	176
Data Retention Settings that Affect Events	176
System Settings that Affect Events	177
System Settings that Affect Event Tickets	178

Chapter



1

Introduction to Events

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 the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<i>What is an Event?</i>	5
<i>How Are Events Triggered?</i>	6
<i>Viewing Events</i>	7
<i>Viewing Events in the Classic SL1 User Interface</i>	8
<i>Event Correlation</i>	8
<i>Defining Events</i>	9
<i>Event States</i>	9

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 alerts that are triggered when a specific condition is met. For example, an event can signal if a server has gone down, if a device is exceeding CPU or disk-space thresholds, or if communication with a device has failed. 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 such as managers of managers (MoM). 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.
- **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.

- **Dynamic.** Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. SL1 examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, 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 Fahrenheit. If you do so, then if the chassis temperature exceeds 100 degrees at some point in the future, the alert evaluates to TRUE and the SL1 system inserts a message in the associated device's log files. The SL1 system matches that message with an existing event, and then triggers the event.
- **Email.** Message is generated by an email message sent to SL1.
- **API.** Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API.

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 more information about using the Events page, see the section on [Viewing the List of Events](#)

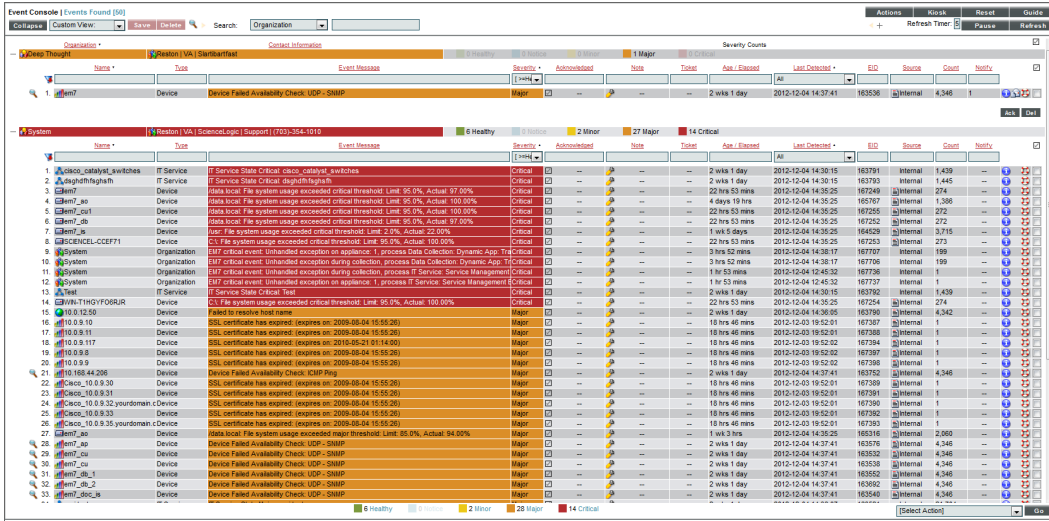
The screenshot displays the ScienceLogic Events page. At the top, there's a navigation bar with 'Events', 'Activity', and 'Em7admin'. A summary bar shows event counts: 4 Critical, 21 Major, 5 Minor, 22 Notice, 7 Healthy, and 59 Events total. Below this is a search bar and a table of events. The table has columns: ORGANIZATION, SEVERITY, NAME, MESSAGE, AGE, COUNT, EVENT NOTE, MASKED EVENTS, ACKNOWLEDGE, and CLEAR. The first event is a 'Notice' from 'System' titled 'EM_Test PP check' with an age of '6 days 12 hours' and a count of '1'. The second event is a 'Major' from 'RC_SNMP' titled 'RC-8pp2v3' with a message 'Cisco: FRU Control Configuration (RSP720-3CKL...)' and an age of '6 days 12 hours' with a count of '1879'. Below the table, there are sections for 'Vitals' (a line chart) and 'Tools' (a search bar for running actions on a device). On the right, there's a 'Logs' section showing recent log entries with their ages and severities.

In addition, you can also use the **[Investigator]** or **[Event]** tabs in the **Device Investigator** or run a device report to view a list of events for a single device. For more information, see the chapter "Using the Device Investigator" in the **Device Management** manual.

You can also use the **Organization Administration** panel and the **Organizational Events** page to view a list of events for a single organization. For more information, see the chapter "Managing Organizations" in the **Organizations and Users** manual.

Viewing Events in the Classic SL1 User Interface

The **Event Console** page in the classic SL1 user interface also displays a list of all currently active events that you are allowed to view. From this page, you can view, acknowledge, clear, suppress, or disable an event. Depending on your configuration, you can also create an event-based ticket in SL1 or a third-party ticketing system. For more information, see the section on [Viewing Events from the Event Console in the Classic SL1 User Interface](#).



You can use the **Device Administration** panel and the **Device Reports** panel to view a list of events for a single device. The events are displayed in a page that is similar to the **Event Console** page, but displays only events that occurred on the selected device. For more information, see the chapter "Managing a Single Device with the Device Administration Panel" in the **Device Management** manual.

You can also use the **Organization Administration** panel and the **Organizational Events** page to view a list of events for a single organization. For more information, see the chapter "Managing Organizations" in the **Organizations and Users** manual.

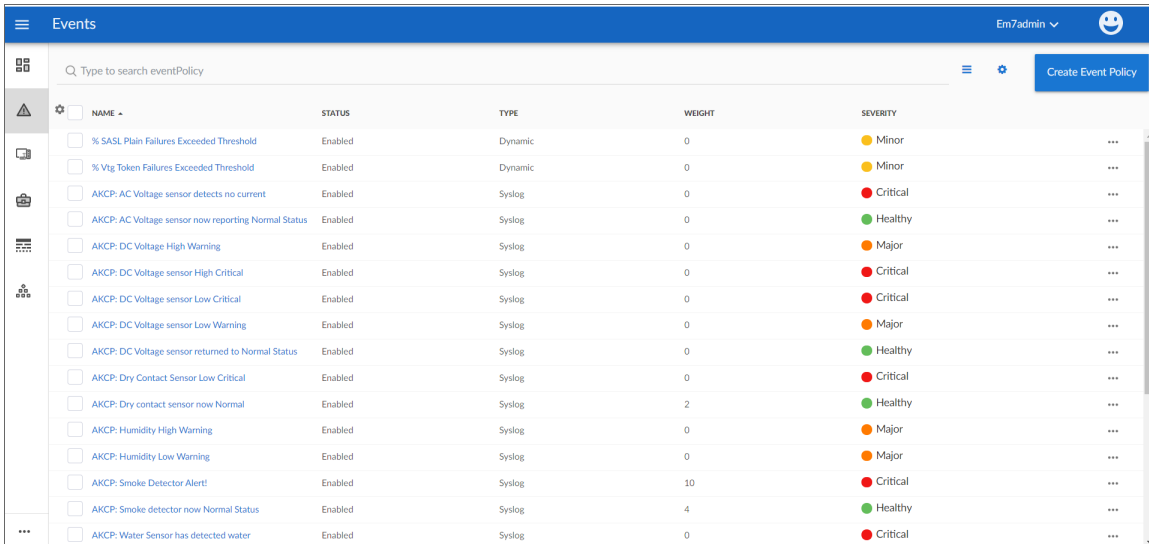
Event Correlation

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 section on [event correlation](#).

Defining Events

The **Event Policies** 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.



NAME	STATUS	TYPE	WEIGHT	SEVERITY
<input type="checkbox"/> % SASL Plain Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
<input type="checkbox"/> % Vtg Token Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
<input type="checkbox"/> AKCP: AC Voltage sensor detects no current	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: AC Voltage sensor now reporting Normal Status	Enabled	Syslog	0	Healthy
<input type="checkbox"/> AKCP: DC Voltage High Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: DC Voltage sensor High Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: DC Voltage sensor Low Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: DC Voltage sensor Low Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: DC Voltage sensor returned to Normal Status	Enabled	Syslog	0	Healthy
<input type="checkbox"/> AKCP: Dry Contact Sensor Low Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: Dry contact sensor now Normal	Enabled	Syslog	2	Healthy
<input type="checkbox"/> AKCP: Humidity High Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: Humidity Low Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: Smoke Detector Alert!	Enabled	Syslog	10	Critical
<input type="checkbox"/> AKCP: Smoke detector now Normal Status	Enabled	Syslog	4	Healthy
<input type="checkbox"/> AKCP: Water Sensor has detected water	Enabled	Syslog	0	Critical

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 Policies** 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 section on [defining and editing event policies](#).

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. Prepending events are grayed out in device logs.

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 the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

Viewing the List of Events	12
Searching and Filtering the List of Events	12
<i>Filtering Events by Organization and Service</i>	12
<i>Filtering Events by Severity</i>	14
<i>Filtering for Masked Events</i>	15
Viewing Additional Data about an Event	16
<i>Viewing Automation Actions</i>	16
<i>Refreshing the Events Page</i>	17
<i>Customizing the Events Page</i>	18
Using the Event Investigator	19
<i>Using the Action Runner</i>	20
Viewing Events for a Single Device	22
Event Throttling	25

Viewing Events from the Event Console in the Classic SL1 User Interface	26
<i>Events that Are Not Displayed in the Event Console</i>	28
<i>Information About Each Displayed Event</i>	29
<i>Global Search Field</i>	31
<i>Filter While You Type</i>	33
<i>Advanced Filter</i>	35
<i>Custom View</i>	37
<i>Viewing Events for a Single Device in the Classic SL1 User Interface</i>	38
<i>Viewing Events for a Single Organization</i>	40
<i>Viewing Event Details in the Event Console</i>	43
<i>Customizing the Display in the Event Console</i>	45
<i>Account Preferences</i>	45
<i>Event Console Preferences</i>	50
<i>Hiding the Header Bar</i>	52
<i>Event Masks in the Event Console</i>	53

Viewing the List of Events

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

Searching and Filtering the List of Events

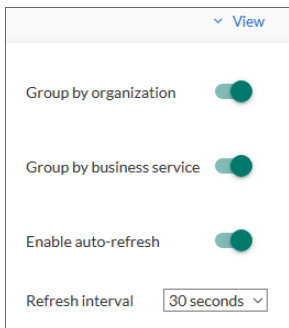
This section explains how to filter the list of events so you can quickly locate and address any potential issues in your environment.

Filtering Events by Organization and Service

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

To view events by organization or service:

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



2. Select the **Group by organization** and/or the **Group by business service** toggle. The relevant panel appears on the left with a list of events sorted by severity for each organization and/or service:

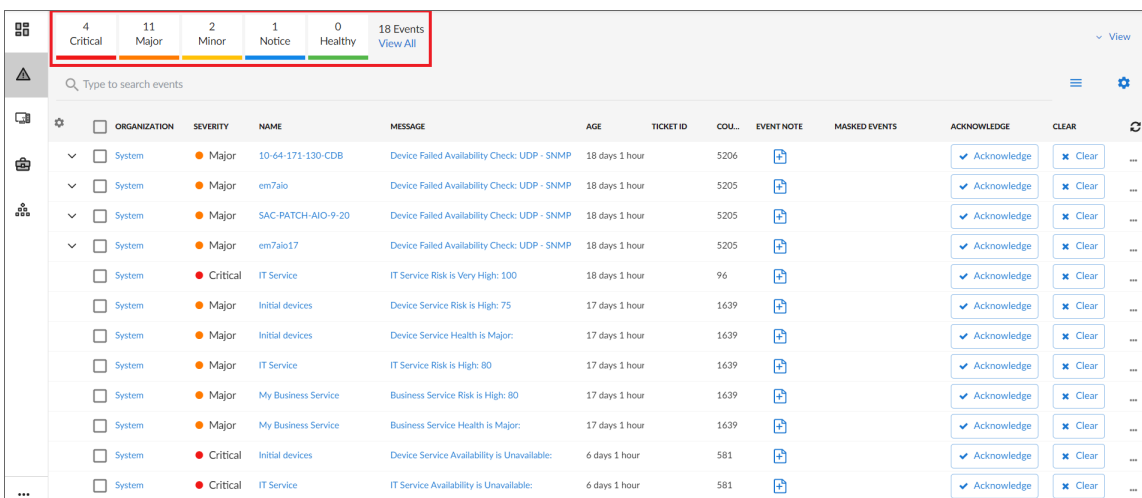
TIP: To hide the **Organizations** and **Business Services** panels, click the left arrow icon (⏪). Click the right arrow icon (⏩) to expand the panel again.

3. On the left panel, click the check mark icon (☑) to filter the list of events based on the organization or service you selected.

TIP: Click the name of a service to go to the **Service Investigator** page for that service. Click the name of an organization to go the **Organizational Summary Page** for that organization.

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:



ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	TICKET ID	COL...	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR
System	Major	10-64-171-130-CDB	Device Failed Availability Check: UDP - SNMP	18 days 1 hour	5206				Acknowledge	Clear
System	Major	em7aio	Device Failed Availability Check: UDP - SNMP	18 days 1 hour	5205				Acknowledge	Clear
System	Major	SAC-PATCH-AIO-9-20	Device Failed Availability Check: UDP - SNMP	18 days 1 hour	5205				Acknowledge	Clear
System	Major	em7aio17	Device Failed Availability Check: UDP - SNMP	18 days 1 hour	5205				Acknowledge	Clear
System	Critical	IT Service	IT Service Risk is Very High: 100	18 days 1 hour	96				Acknowledge	Clear
System	Major	Initial devices	Device Service Risk is High: 75	17 days 1 hour	1639				Acknowledge	Clear
System	Major	Initial devices	Device Service Health is Major:	17 days 1 hour	1639				Acknowledge	Clear
System	Major	IT Service	IT Service Risk is High: 80	17 days 1 hour	1639				Acknowledge	Clear
System	Major	My Business Service	Business Service Risk is High: 80	17 days 1 hour	1639				Acknowledge	Clear
System	Major	My Business Service	Business Service Health is Major:	17 days 1 hour	1639				Acknowledge	Clear
System	Critical	Initial devices	Device Service Availability is Unavailable:	6 days 1 hour	581				Acknowledge	Clear
System	Critical	IT Service	IT Service Availability is Unavailable:	6 days 1 hour	581				Acknowledge	Clear

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.

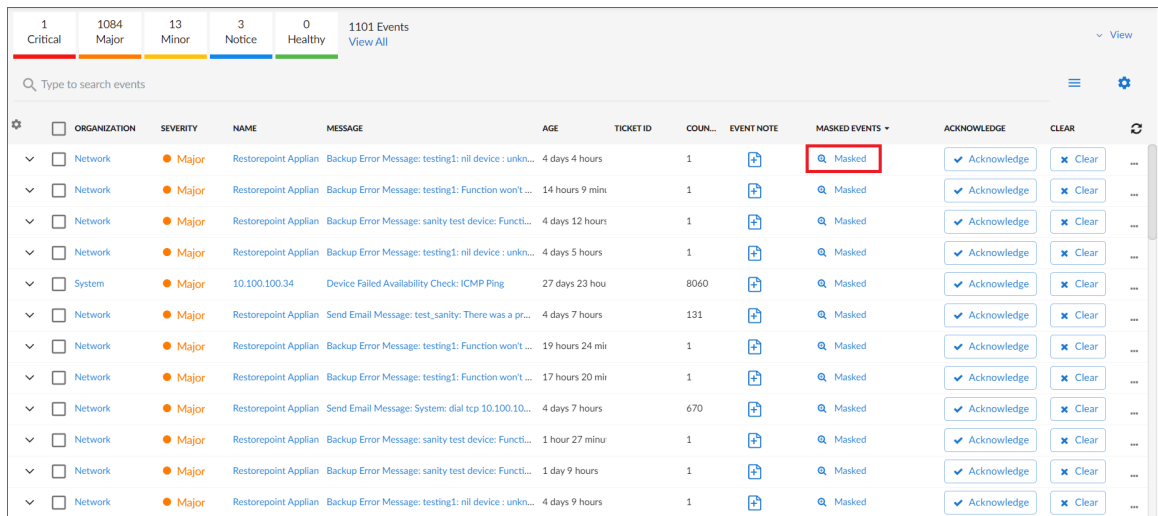
The following color codes are used throughout SL1:

- **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 users should be aware of but does not affect service.
- **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 on the **Events** page. This allows related events that occur in quick succession on a single device to be rolled-up and posted together under one event description. For example, if a device cannot connect to the network, multiple other services on the device will raise events. SL1 would display the event with the highest severity and roll up all the other events.

On the **Events** page, any event that contains masked events includes a magnifying glass icon (🔍) and the word "Masked" in the **Masked Events** column:

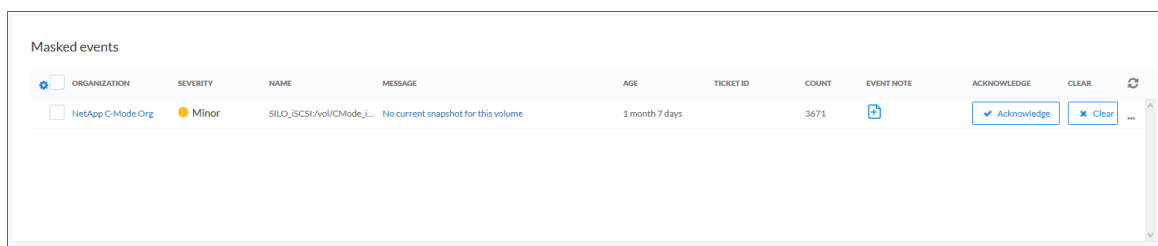


1 Critical	1084 Major	13 Minor	3 Notice	0 Healthy	1101 Events	View All		View			
ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	TICKET ID	COUN...	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR	
Network	Major	Restorepoint Applian	Backup Error Message: testing1: nil device : unkn...	4 days 4 hours		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: testing1: Function won't ...	14 hours 9 min		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: sanity test device: Functi...	4 days 12 hours		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: testing1: nil device : unkn...	4 days 5 hours		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
System	Major	10.100.100.34	Device Failed Availability Check: ICMP Ping	27 days 23 hou		8060		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Send Email Message: test_sanity: There was a pr...	4 days 7 hours		131		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: testing1: Function won't ...	19 hours 24 mi		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: testing1: Function won't ...	17 hours 20 mi		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Send Email Message: System: dial tcp 10.100.10...	4 days 7 hours		670		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: sanity test device: Functi...	1 hour 27 min		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: sanity test device: Functi...	1 day 9 hours		1		🔍 Masked	✓ Acknowledge	✕ Clear	...
Network	Major	Restorepoint Applian	Backup Error Message: testing1: nil device : unkn...	4 days 9 hours		1		🔍 Masked	✓ Acknowledge	✕ Clear	...

TIP: Click the **Select Columns** icon (⚙️) to add the **Masked Events** column, if it is not currently visible.

To view more information about masked events:

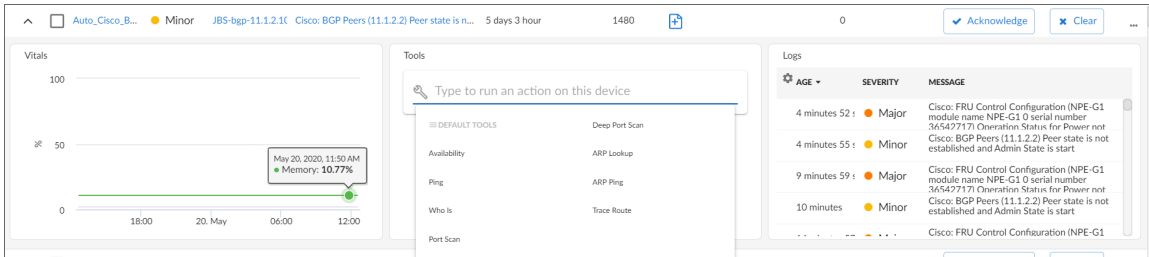
1. On the **Events** page, click the magnifying glass icon (🔍) or the **Masked** link in the **Masked Events** column for the relevant event. The **Event Investigator** page for that event appears.
2. Scroll down to the **Masked events** section to view the details about the masked events:



ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	ACKNOWLEDGE	CLEAR	
NetApp C-Mode Org	Minor	SILO_JSCSI:/vol/CModeJ...	No current snapshot for this volume	1 month 7 days		3671		✓ Acknowledge	✕ Clear	...

Viewing Additional Data about an Event

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.

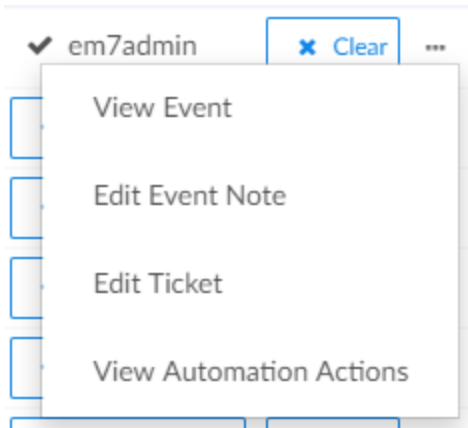
On the Event Drawer, you can access the following panes:

- The **Vitals** pane displays graph data for 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.
- The **Tools** pane enables you to run a set of network diagnostic tools or user-initiated actions in the **Activity Center**. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions. For more information, see the section on [Using the Action Runner](#).
- The **Logs** pane displays a list of the log entries from the device's log file, sorted from newest to oldest by default.

Viewing Automation Actions

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

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




The **Event Actions Log** displays a history of all automation actions that SL1 executed in response to the event.

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

Refreshing the Events Page

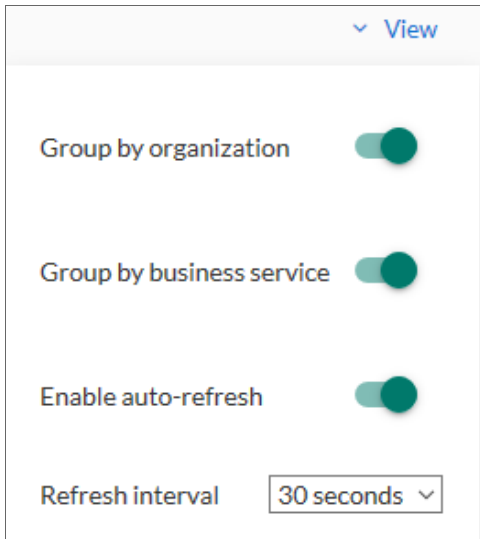
You can refresh the **Events** page manually or set it to auto-refresh.

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

ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	ACKNOWLEDGE	CLEAR	REFRESH
System	Major	AIO-9-80	Device Failed Availability Check: UDP - SNMP	1 day 4 hours		332		Acknowledge	Clear	
System	Major	#thomsenDevAIO	Device Failed Availability Check: UDP - SNMP	1 day 4 hours		332		Acknowledge	Clear	
Acme, Inc	Major	iso4-cdb-9-66	Device Failed Availability Check: UDP - SNMP	1 day 4 hours		311		Acknowledge	Clear	
Acme, Inc	Major	iso4-cu1-9-67	Device Failed Availability Check: UDP - SNMP	1 day 4 hours		311		Acknowledge	Clear	
IntelliTech	Major	iso4-cu2-9-68	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	NIMon_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:



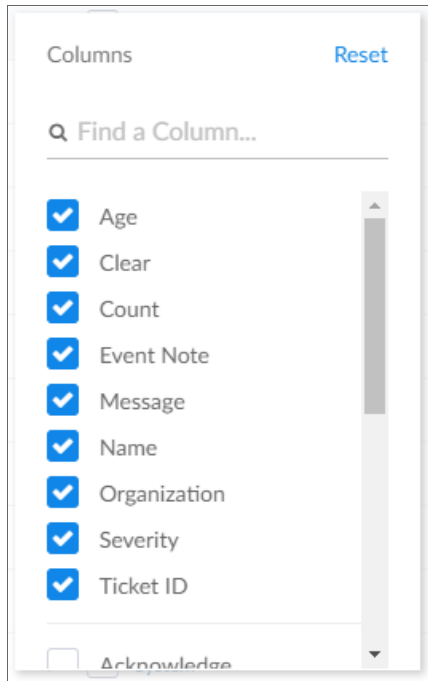
2. Click the **Enable auto-refresh** toggle to turn it blue. The **Refresh interval** drop-down appears.
3. In the **Refresh interval** drop-down, select the refresh interval for the page. Options range from 10 seconds to 60 minutes.

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.

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

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.

TIP: On the **Event Investigator** page, click the name of an aligned device or service to go to the Investigator page for that device or service. You can also click the name of the aligned organization to view its **Organizational Summary** page.

Using the Action Runner

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

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

NOTE: For more information about user-initiated actions, see the chapter on "Automation Policies" in the *Run Book Automation* manual.

To use the **Action Runner**:

1. Access the **Action Runner** for events in one of the following ways:
 - On the **Action Runner** page, open the Event Drawer for a particular event. Click the search bar in the **Tools** pane.
 - On the **Action Runner** page, click the search bar in the **Tools** pane.
 - Click **[Activity]** in the navigation bar at the top of any page in SL1. Click the search bar.
2. When you click the search bar, a list displays the default tools, actions, or custom links that are available for the selected device. Click one of these tools, actions, or custom links, or use the search bar to search for a tool or action that is not listed. The following default tools are available in the **Action Runner**:
 - **Availability.** Displays the results of an availability check of the device, using the port and protocol specified in the **Availability Port** and **Availability Protocol** fields on the **[Settings]** tab for this device.

- **Ping**. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by 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, SL1 uses the appropriate IPv6 ping command.
- **Who Is**. Displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
- **Port Scan**. Displays a list of all open ports on the device at the time of the scan.
- **Deep Port Scan**. Displays a list of all open ports and as much detail about each open port as the deep port scanner can retrieve.
- **ARP Lookup**. Displays a list of IP addresses for the device and the resolved Ethernet physical address (MAC address) for each IP address.
- **ARP Ping**. Displays the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it uses the ARP protocol instead of ICMP. The ARP Ping tool can be used only on the local network.
- **Trace Route**. Displays the network route between 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.

TIP: The tools found in the **Action Runner** can also be found in the Device Toolbox in the classic SL1 user interface.

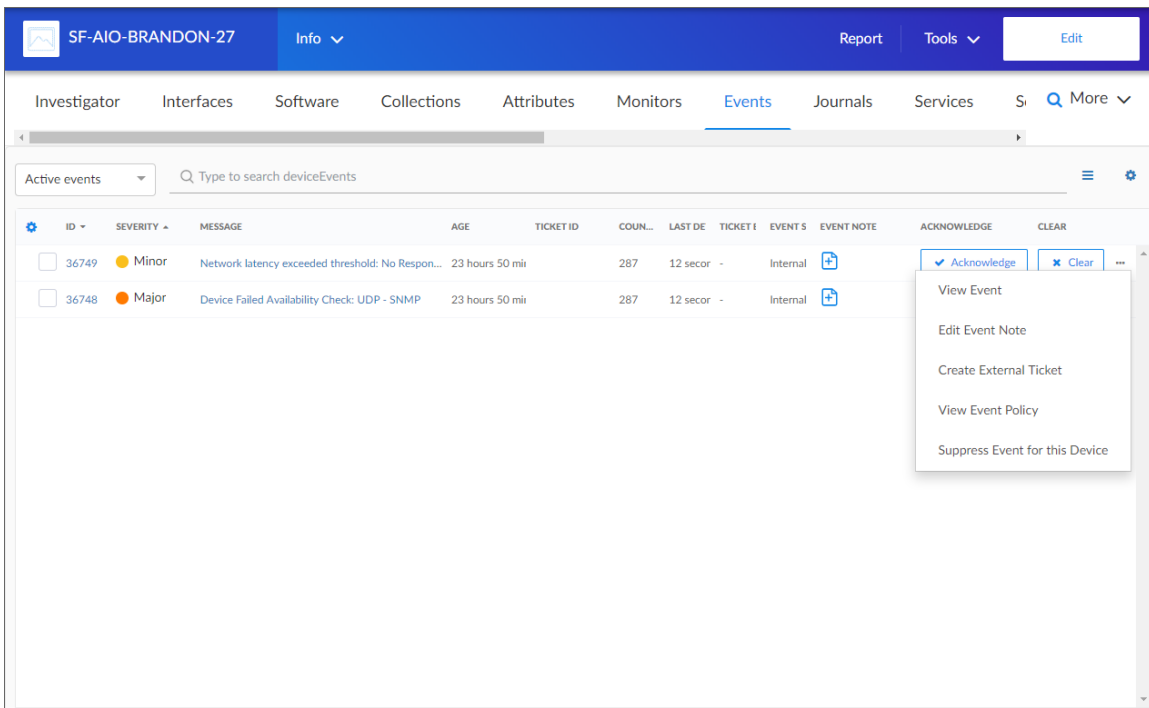
3. If you clicked a custom link, the link opens in a new browser window or tab. If you clicked on a tool or action, then as it runs, its progress and results appear in a log in the **Activity Center**.
4. After the tool or action has run, if you want to run it again, click the **[Run Again]** button.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

The screenshot shows the 'Activity' window. On the left, under 'RECENT DEVICES', there is a list with 'lenny-nightly-dist-mc-10-2-4-125' selected. The main area contains a search bar and two log entries. The first entry is a 'Ping' action from May 16, 2020, at 2:33 PM, with a 'Run Again' button. The log text for the ping is: 'Process Started on Collector', 'PING 10.2.4.125 (10.2.4.125) 56(84) bytes of data.', followed by five lines of ping results showing 64 bytes received with various TTL and time values, and a summary: '--- 10.2.4.125 ping statistics ---', '5 packets transmitted, 5 received, 0% packet loss, time 4000ms', 'rtt min/avg/max/mdev = 0.254/0.296/0.404/0.058 ms', and 'Process Completed on Collector'. The second entry is a 'Deep Port Scan' from May 16, 2020, at 2:14 PM, also with a 'Run Again' button. Its log text is: 'Process Started on Collector', 'Starting Nmap 6.40 (http://nmap.org) at 2020-05-16 18:14 UTC'.

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

Viewing Events for a Single Device

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





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

- **ID**. The unique ID for the event, generated by SL1. The ID appears as a hyperlink. To view the **Event Investigator** page for the event, click the **ID** hyperlink. For more information about the **Event Investigator** page, see the **Events** manual.
- **Severity**. The severity of the event. Possible values are:
 - *Critical*
 - *Major*
 - *Minor*
 - *Notice*
 - *Healthy*
- **Message**. The message generated for the event. The message appears as a hyperlink. To view the **Event Investigator** page for the event, click the **Message** hyperlink. For more information about the **Event Investigator** page, see the **Events** manual.
- **Age**. The amount of time (in days, hours, and minutes) since the event first occurred or since its last occurrence without having been cleared.
- **Ticket ID**. If a ticket has been created for the event, this column displays the ticket ID of that ticket.
- **Count**. The number of times this event has occurred, the number of child events associated with the event, or the number of masked events associated with the event.
- **Last Detected**. The date and time at which the event last occurred on the device.


- **Ticket External Reference.** The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in SL1). If this field displays a value, you can click on that value to spawn a new window and view the external ticket.

NOTE: To link an external ticket to an event, you must create a custom Run Book Automation policy and a custom Run Book Action or use the ScienceLogic APIs. For help with these tasks, contact ScienceLogic Customer Care.

- **Event Source.** The system or application that generated this event. Possible values are:
 - *Syslog.* Event was generated from a system log generated by a device.
 - *Email.* Event was generated by an email from an external agent. For example, Microsoft Operations Manager (MOM).
 - *Internal.* Event was generated by SL1.
 - *Trap.* Event was generated by an SNMP trap.
 - *Dynamic.* Event was generated by a Dynamic Application collecting data from the device.
 - *API.* Event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
 - *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 Device Infrastructure Health** manual .
- **Event Note.** A user-defined note to accompany the event. To create or edit a note, click the **Note** icon (). The **Edit Event Note** window appears, where you can create or edit a note and save your changes.
- **Acknowledge.** If the event has been acknowledged, this column displays a check mark and the username of the user who acknowledged the event. If the event has not yet been acknowledged, this column displays an **[Acknowledge]** button; click the **[Acknowledge]** button to acknowledge the event. When you **acknowledge** an event, you let other users know that you are aware of that event and are working on a response.
- **Clear.** Click the **[Clear]** button to clear the event. When you **clear** an event, you let other users know that this event has been addressed. Clearing an event removes a single instance of the event from the **[Events]** tab. If the same event occurs again on the same device, it will reappear in the **[Events]** tab, even if you have previously cleared that event.

TIP: To rearrange the columns in the List View, click and drag the column name to a new location. You can adjust the width of a column with by clicking and dragging the right edge of the column. You can click the **Select Columns** icon () to add or remove columns, or to reset columns to their default settings.

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

Clicking the **Actions** menu () next to an event gives you the following options, based on your permissions:

- *View Event*. Navigates to the **Event Investigator** page for that event.
- *Edit Event Note*. Lets you update the Note associated with this event.
- *Create Ticket*. Opens a new ticket in the SL1 **Ticket Editor**, if you are using SL1 for your ticketing.
- *Edit Ticket*. Opens an existing ticket in the SL1 **Ticket Editor**, if you are using SL1 for your ticketing.
- *Create External Ticket*. Creates a new ticket for the event if you are using an external ticketing system instead of SL1.
- *View Event Policy*. Opens the **Event Policy** page for the policy aligned with this event.
- *Suppress Event for this Device*. Suppresses the current event on the current device. When you suppress an event, you are specifying that in the future, if this event occurs again on the same device, the event will not appear in
- *View Automation Actions*. Displays a log of automations that have occurred for that event. This option is hidden if the event does not have any automation actions aligned to it.

Event Throttling

When SL1 detects syslog messages or traps coming from a single device at a rate greater than 25 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 25 messages per second.
- **Event with a Severity of Notice and the message "Inbound Message Spikes"**. This event is triggered when a single IP exceeds the threshold of syslog messages or trap message. The default threshold is 25 messages per second.

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

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

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

NOTE: SL1 does not support message throttling on IPv6 devices monitored by CentOS5 Data Collectors.

Viewing Events from the Event Console in the Classic SL1 User Interface

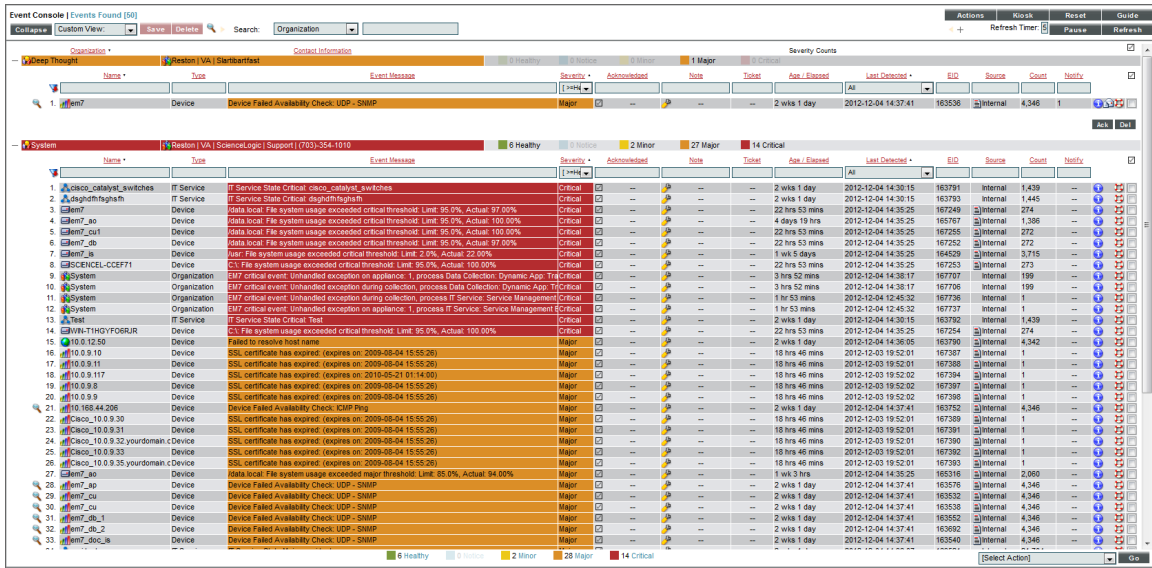
The **Event Console** page in the classic user interface includes the following tools for searching and filtering the list of events that is displayed in the page:

- The **Global Search** drop-down list and field in the upper left allows you to filter the entire list of events by one of the columns or by device group ID or device group name.
- The **filter-while-you-type** fields allow you to filter the list of events by one or more of the event parameters.
- You can access the **Advanced Filter Tool**, where you can enter more complex filters, based on your current configuration of SL1 (for example, for the **Acknowledged** field, you can search for multiple usernames).
- You can save the results of a Global Search as a **Custom View**.

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

To view a list of all active events, click the **[Events]** tab. The **Event Console** page is displayed:

NOTE: To view the **Event Console** page, accounts of type "user" must be granted one or more access keys that includes the following access hook: Events/Event:View. Accounts of type "user" will then be able to view events that have the same organization as the user. For more information on Access Keys, see the manual **Access Permissions**.



Each event is color-coded to make it easy for you to determine severity:

Color	Severity	Description
Red	Critical	Critical Events indicate a condition that can seriously impair or curtail service and requires immediate attention (i.e., service or system outages).
Orange	Major	Major Events indicate a condition that impacts service and requires immediate investigation.
Yellow	Minor	Minor Events indicate a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
Blue	Notice	Notice Events indicate a condition that users should be aware of but does not affect service.
Green	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.

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

NOTE: The settings in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page (Events > Actions > Console Preferences) affect the display in the **Event Console** page.

If you select the **Group by Organization** checkbox in the **Account Preferences** page or the **Event Console Preferences** page:

- Events in the **Event Console** will be grouped by organization.
- The **filter-while-you-type** fields will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single filter to events in multiple organizations.
- The **advanced filter tool** will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single advanced filter to events in multiple organizations.

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


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

Events that Are Not Displayed in the Event Console


In SL1, there are four types of events that might not be displayed in the **Event Console**:

- **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 in the **Event Console**. Instead, SL1 displays a single entry and notes the number of occurrences in the **Count** column.
- **Suppressed Events.** [Suppressed events](#) do not appear in the **Event Console**.

NOTE: For details on suppressed events, see the section on [Suppressing an Event](#).

- **Topology Events.** In SL1, [event correlation or topology suppression](#) means the ability to build parent-child relationships between events and to create categories for events. When events are correlated, only the parent event is displayed in the **Event Console** page. The child events are rolled up under the parent event and are not displayed in the **Event Console** page. For the parent event, the value in the **Count** column will be incremented to indicate the number of correlated child events. The magnifying-glass icon () appears to the left of the event. When you click on the magnifying-glass icon, the **Event Console** page expands the event to display the child event(s).

NOTE: For details on Topology Events, see the section on [Event Correlation](#).

- **Event Masks.** In the **Device Properties** page for each device, you can define an Event Mask. When a device uses the Event Mask setting, all events that occur on a single device within a specified span of time are grouped together. In the **Event Console**, masked events are displayed under a single event, the one with the highest severity. The magnifying-glass icon () appears to the left of the event. When you click on the magnifying-glass icon, the **Suppression Group** modal page is displayed. This page displays details about all events that are masked under the displayed event.

NOTE: For details on Event Masks, see the section on [Event Masks](#).

Information About Each Displayed Event

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

TIP: By default, the list of events is displayed from newest to oldest. To sort the list of events, 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. You can sort this way in both normal mode and kiosk mode.


- **Report Icon.** Icon that leads you to more information about the element or policy associated with the event.
- **Organization.** Appears only if you have not selected the **Group by Organization** checkbox in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page (Events > Actions > Console Preferences). Specifies the organization that the event is associated with.
- **Name.** Name of the entity associated with the event.

- **Type.** Type of entity associated with the event. The possible options are:
 - Organizations
 - Devices
 - Assets
 - IP networks
 - Interfaces
 - IT Services
 - Vendors
 - User Accounts
 - Virtual Interfaces

- **Event Message.** Message generated for the event.

- **Severity.** Severity of the event. Possible values are:
 - *Critical*
 - *Major*
 - *Minor*
 - *Notice*
 - *Healthy*

- **Acknowledged.** If the event has been acknowledged, this column displays a red check-mark character and specifies the user who acknowledged the event. If the event has not been acknowledged, this field displays a gray check-mark character. To acknowledge an event, click in this column.






- **Note.** User-defined note to accompany the event. To create or edit a note, select the wrench icon () in this column. The **Add a Note** modal page appears, where you can create or edit a note and save your changes.

- **Ticket.** If a ticket has been created for the event, this column displays the ticket ID of that ticket.

- **External Ticket.** The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in SL1). If this field displays a value, you can click on that value to spawn a new window and view the external ticket.

NOTE: To link an external ticket to an event, you must create a custom Run Book Automation policy and a custom Run Book Action or use the ScienceLogic APIs. For help with these tasks, contact ScienceLogic Customer Care.

- **Age/Elapsed .** Number of days, hours, and minutes since the first occurrence of the event. This is also the time since the event occurred without the event having been cleared.
- **Last Detected.** Date and time the event last occurred on this entity.
- **EID.** Unique ID for the event, generated by SL1 .

- **Source.** System or application that generated this event. Choices are:
 - *Syslog.* Event was generated from a system log generated by a device.
 - *Email.* Event was generated by an email from an external agent. For example, Microsoft Operations Manager (MOM).
 - *Internal.* Event was generated by SL1.
 - *Trap.* Event was generated by an SNMP trap.
 - *Dynamic.* Event was generated by a Dynamic Application collecting data from the device.
 - *API.* Event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
 - *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 Device Infrastructure Health* manual . .
- **Count.** Number of times this event has occurred or number of child events associated with the event or number of masked events associated with the event.
- **Notify.** Number of times the event has triggered the execution of an Automation Policy.
- **Information icon** (). Displays the **Event Information** page, where you can view an overview of the selected event, suppress the selected event, or edit the definition of the selected event.
- **View Notifications icon** (). Leads to the **Event Actions Log**, where you can view details about each automation policy that has triggered for the event.
- **Ticket icon** (). Depending upon the setting **Ticket Life Ring Button Behavior** (found in System > Settings > Behavior), one of the following will happen:
 - The **Ticket Editor** page appears. If a ScienceLogic ticket is already aligned with this event, you can view details about the ticket. If a ScienceLogic ticket is not yet aligned with this event, you can define a ticket and the SL1 system will automatically associate the new ticket with the selected event.
 - If an external ticket is aligned with an event, when you select the life-ring icon () for that event (from the **Event Console**), 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 life-ring icon () 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.

Global Search Field

The **Global Search** field in the upper left of the page allows you to filter the entire list of displayed events by a single parameter. SL1 will update the **Event Console** and display only events that have a matching parameter.

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

- **Search.** You can select one of the following search parameters:
 - *Organization.* Appears only if you have not selected the **Group by Organization** checkbox in the **Account Preferences** page (Preferences > Account > Preferences) or in the **Event Console Preferences** page (Events > Actions > Console Preferences). Name of the organization associated with the event.
 - *Name.* Name of the entity associated with the event.
 - *Type.* Type of entity associated with the event.
 - *Event Message.* Message generated for the event.
 - *Severity.* Severity of the event.
 - *Acknowledged.* If the event has been acknowledged, search for the user who acknowledged the event.
 - *Note.* User-defined note associated with the event.
 - *Ticket.* If a ticket has been created for the event, this parameter searches by the ticket ID of that ticket.
 - *External Ticket.* The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in SL1).
 - *Age/Elapsed.* You can enter time in seconds, and the **Event Console** page will display only events that last occurred within that number of seconds or less.
 - *Event ID.* Unique ID for the event, generated by SL1.
 - *Source.* System or application that generated this event.
 - *Count.* Number of times this event has occurred.
 - *Notify.* Number of times the event has triggered the execution of an Automation Policy.
 - *Device Group ID.* Unique ID for the device group associated with the event.
 - *Device Group Name.* Name of the device group associated with the event.
- **Text.** For each search parameter, you must enter text to match. SL1 will search for events that match the text, including partial matches. Text matches are not case-sensitive. You can use special characters in each filter.

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

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

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

Filter While You Type

The **Event Console** page includes a filter for each column you selected to display, except **Age/Elapsed**. You can specify one or more parameters to filter the display of events. Only events that meet all the filter criteria will be displayed in the **Event Console**.

You can filter by one or more parameters. The list of events is dynamically updated as you select each filter.

NOTE: To return to the default list of events, click the **[Reset]** button.

To access the **Filter-While-You-Type** feature in the **Event Console**:

1. Go to the **Event Console** page.
2. The settings in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page (Events > Actions > Console Preferences) affect the scope of the **filter-while-you-type** fields. If you select the **Group by Organization** checkbox in the **Account Preferences** page or the **Event Console Preferences** page, events in the **Event Console** will be grouped by organization. The **filter-while-you-type** fields will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single filter to events in multiple organizations.
3. If you selected the **Group by Organization** checkbox, find the organization for which you want to filter the list of events. Expand the list of events by clicking on the plus sign (+) next to the organization name.
4. If you have not selected the **Group by Organization** checkbox, go to the top of the **Event Console** page.
5. The **filter-while-you-type** fields are displayed in the row under the column headings.
 - For each filter except **Severity**, **Last Detected**, and **Age/Elapsed**, you must enter text to match against. SL1 will search for events that match the text, including partial matches. Text matches are not case-sensitive. You can use special characters in each filter.
 - **Organization**. Appears only if you have not selected the **Group by Organization** checkbox in the **Account Preferences** page (Preferences > Account > Preferences) or in the **Event Console Preferences** page (Events > Actions > Console Preferences). You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching organization.
 - **Name**. You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching entity name.
 - **Type**. You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching entity type.
 - **Event Message**. You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching event message.

- **Severity.** You can select a severity value, and the **Event Console** page will display only events that have a matching severity. Choices are:
 - *>=Healthy.* Will display all events with a severity greater than or equal to "Healthy". Healthy has a numeric value of "0" (zero).
 - *>=Notice.* Will display all events with a severity greater than or equal to "Notice". Notice has a numeric value of "1" (one).
 - *>=Minor.* Will display all events with a severity greater than or equal to "Minor". Minor has a numeric value of "2" (two).
 - *>=Major.* Will display all events with a severity greater than or equal to "Major". Major has a numeric value of "3" (three).
 - *>=Critical.* Will display all events with a severity greater than or equal to "Critical". Critical has a numeric value of "4" (four).
- **Acknowledged.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have been acknowledged by a matching user account.
- **Note.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have matching note text.
- **Ticket.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching ticket ID.
- **External Ticket.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching external ticket name or ID.
- **Age/Elapsed.** You can enter time in seconds, and the **Event Console** page will display only events that last occurred within that number of seconds or less.
- **Last Detected.** Only those events that match the specified detection date will be displayed. The choices are:
 - *All.* Display events from all detection dates and times.
 - *Last Minute.* Display only events that have been detected within the last minute.
 - *Last Hour.* Display only events that have been detected within the last hour.
 - *Last Day.* Display only events that have been detected within the last day.
 - *Last Week.* Display only events that have been detected within the last week.
 - *Last Month.* Display only events that have been detected within the last month.
 - *Last Year.* Display only events that have been detected within the last year.
- **EID.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching event ID.
- **Source.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching source.

- **Count.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching count number.
- **Notify.** You can enter text to match, including special characters, and the **Event Console** page will display only events that have a matching number of notifications.

Advanced Filter

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

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

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

- Events in the **Event Console** page will be grouped by organization.
- The Advanced Filter tool will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single advanced filter to events in multiple organizations.
- The Advanced Filter tool will not allow you to filter by Organization.
- The possible filter options will be pre-filtered by each organization. For example, suppose that for the organization named "Networking," all the events are associated with either a device or an interface. The **Type** filter will be pre-populated with two types: "Interface" and "Device." You can then select one or both of these options to include in your filter.


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

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

For each filter except **Severity** and **Last Detected**, you must enter text to match against. SL1 will search for events that match the text, including partial matches. For the **Type** and **Source** filters, you can enter text to match against or you can select from the list of possible values. Text matches are not case-sensitive. You can use **special characters** in each filter.

To access the Advanced Filter Tool:

1. Go to the **Event Console** page.

2. The settings in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page (Events > Actions > Console Preferences) affect the scope of the **filter-while-you-type** fields. If you select the **Group by Organization** checkbox in the **Account Preferences** page or the **Event Console Preferences** page, events in the **Event Console** page will be grouped by organization. The Advanced Filter Tool will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single filter to events in multiple organizations.
3. If you selected the **Group by Organization** checkbox, find the organization for which you want to apply the advanced filter tool. Expand the list of events by clicking on the plus sign (+) next to the organization name.
4. If you have not selected the **Group by Organization** checkbox, go to the top of the **Event Console** page.
5. Click on the funnel icon ().
6. The Advanced Filter Tool will display advanced filters for each column in your default display. To change the columns that are displayed in the **Event Console** page, see the section [Customizing the Display in the Event Console](#).

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

7. In the Advanced Filter Tool, you can filter by one or more of the following filters.
 - **Organization.** Appears only if you have not selected the **Group by Organization** checkbox in the **Account Preferences** page (Preferences > Account > Preferences) and in the **Event Console Preferences** page (Events > Actions > Console Preferences). In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching organization.
 - **Name.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching entity name.
 - **Type.** This field will display a list of all the entity types currently in use by the list of events. You can enter text or select one or more of the types, and the **Event Console** page will display only events that have a matching entity type.
 - **Event Message.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching event message.
 - **Severity.** This field will display a list of all the severities currently in use by the list of events. You can select one or more severities, and the **Event Console** page will display only events that have a matching severity. Choices are:
 - *Healthy.* Will display all events with a severity of "Healthy".
 - *Notice.* Will display all events with a severity of "Notice".
 - *Minor.* Will display all events with a severity of "Minor".
 - *Major.* Will display all events with a severity of "Major".
 - *Critical.* Will display all events with a severity of "Critical".

- **Acknowledged.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have been acknowledged by a matching user.
 - **Note.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have matching note text.
 - **Ticket.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching ticket ID.
 - **External Ticket.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching external ticket ID or external ticket name.
 - **Age/Elapsed.** You can enter time in seconds, and the **Event Console** page will display only events that last occurred within that number of seconds or less.
 - **Last Detected.** In the *From* and *To* field, you can specify a range of dates, in the format *yyyy-mm-dd hh:mm:ss*. The **Event Console** page will display only events with a detection date that falls within that range of dates.
 - **EID.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching event ID.
 - **Source.** This field will display a list of all the sources currently in use by the list of events. You can enter text or select one or more sources, and the **Event Console** page will display only events that have a matching source.
 - **Count.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching count number.
 - **Notify.** In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Event Console** page will display only events that have a matching number of notifications.
8. Click **[Apply]** to apply the advanced filters. Click **[Reset]** to clear the advanced filters and start again.
 9. Click **[Reset]** for the **Event Console** page to return to the default list of events.

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

Custom View

You can save a filtered list of events created with the [Global Search tool](#). When you do so, you are creating a **custom view**. You can then return to the page at any time and display the custom view, without having to filter the list again.

To save a custom view:

1. Go to the **Event Console** page.
2. Using the [Global Search tool](#), filter the list of events.

3. In the **Custom View** drop-down field, select *new custom view*.
4. Click the **[Save]** button.
5. You will be prompted to enter a name for the new custom view.
6. The new custom view now appears in the **Custom View** drop-down list.
7. To edit the custom view, select it from the **Custom View** drop-down list, make changes with the **Global Search** tool and then click the **[Save]** button for the custom view to save your changes.
8. To display the custom view, select it from the **Custom View** drop-down list.
9. To delete the custom view, select it from the **Custom View** drop-down field and then click the **[Delete]** button. The custom view will no longer appear in the **Custom View** drop-down list.


NOTE: In Kiosk mode, you cannot create, edit, or delete a custom view. You can perform these actions only in normal mode.

Viewing Events for a Single Device in the Classic SL1 User Interface

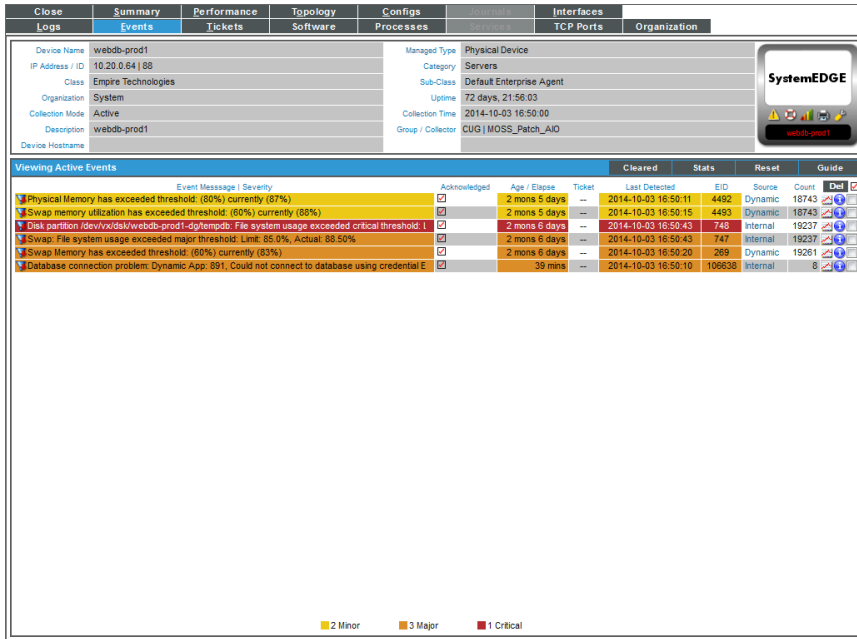
To view a list of events for a single device in the classic user interface, you can go to the **Viewing Active Events** page in the **Device Reports** panel.

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

To view a list of events for a single device:




1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Find the device that you want to view events for and select its bar graph icon (.
3. In the **Device Reports** panel, select the **[Events]** tab.

4. The **Viewing Active Events** page appears.



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

- **Event Message | Severity.** Message generated by event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). The message is color-coded for severity.
- **Acknowledged.** Specifies whether a ScienceLogic user has acknowledged this event.
 - *Red check.* Event has not been acknowledged.
 - *Gray check with name.* Event has been acknowledged.
- **Age / Elapse.** Number of days, hours, and minutes since the first occurrence of the event.
- **Ticket.** Ticket ID associated with this event, if applicable.
- **Last Detected.** Date and time of last occurrence of the event.
- **EID.** Unique ID for the event, generated by SL1.

- **Source.** Source of the log message that triggers the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). Choices are:
 - *Syslog.* Event was generated from standard system log generated by device.
 - *Internal.* Event was generated by SL1.
 - *Trap.* Event was generated by an SNMP trap.
 - *Dynamic.* Event was generated by a Dynamic Application collecting data from the device.
 - *Email.* Event was generated by an email from an external agent; for example, Microsoft Operations Manager (MOM).
 - *API.* Event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
- **Count.** Number of times this event has occurred.
- **View Notifications icon** (). Leads to the **Event Actions Log**, where you can view details about each automation policy that has triggered for the event.
- **Statistics icon** (). Displays the **Event Statistics** page, where you can view historical statistics for the selected event.
- **Information icon** (). Displays the **Event Information** page, where you can view an overview of the selected event, suppress the selected event, or edit the definition of the selected event.

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

Viewing Events for a Single Organization

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

Each instance of an event in SL1 is associated with an organization. Each occurrence of an event is grouped by organization (the organization associated with the device where the event occurred or the organization associated with the policy that generated the event).

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

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

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).

- In the **Organizational Account Administration** page, find the organization with associated events that you want to view.

Organizational Account Administration | Organizations Found [7]

Organization Name	City	State	Contact	Phone	Email	Users	Devices	Assets	Events	ID	Edited By	Last Edited
1. Acme Corporation	New York	NY		--	--	1	7	--	12	6	em7admin	2012-03-15 18:18:48
2. PDC - Servers	Washington	DC		--	--	1	11	--	1	1	em7admin	2012-03-16 11:40:45
3. PDC - Switches	Washington	DC		--	--	--	--	--	7	--	em7admin	2012-03-16 11:40:13
4. Engineering	Reston	VA	Kint, Roger	703-354-3333	rkint@super.com	1	--	--	5	--	em7admin	2012-03-13 19:54:52
5. NOC	Reston	VA	Illk, Griffin	704-354-1111	gillk@super.com	1	--	--	4	--	em7admin	2012-03-13 19:52:57
6. QA	Reston	--	--	--	--	1	2	1	1	--	em7admin	2012-02-22 22:39:54
7. System	Reston	VA	Support, ScienceLogic	(703)-354-1010	support@sciencelogic.com	5	27	3	1	0	em7admin	2007-12-01 15:51:17

[Select Action] Go




- If a value appears in the *Events* column, click the event icon (🚨).
- The **Organizational Events** page appears for the organization.

Organizational Events | For Organization [Acme Corporation] | Viewing [Active Events]

Name	Event Message	Acknowledged	Age / Elapse	Ticket	External Ticket	Last Detected	Source	Count	Del
LAB-2010-EX.LAB	C:\ File system usage exceeded critical threshold: Limit: 95%, Actual: 95%	☑	2012-05-01 18:40:08	--	--	2012-05-02 11:55:07	Internal	208	🗑️
10.100.100.8	backup_complete	☑	2012-03-28 19:44:13	--	--	2012-03-28 19:44:13	3rd Party	2	🗑️
10.100.100.28	Device Failed Availability Check: ICMP Ping	☑	2012-04-20 18:22:13	--	--	2012-05-02 11:52:13	Internal	3391	🗑️
LAB-2010-SPLAB	Device Failed Availability Check: UDP - SNMP	☑	2012-04-20 18:22:13	--	--	2012-05-02 11:52:13	Internal	3391	🗑️
LAB-2010-EX.LAB	Mailbox Mailbox Database 0301049544 Average Delivery Time has exceeded threshold: (1500s)	☑	2012-02-22 20:25:30	--	--	2012-02-27 16:35:25	Dynamic	1385	🗑️
10.100.100.28	Network latency exceeded threshold: No Response	☑	2012-04-20 18:22:13	--	--	2012-05-02 11:52:13	Internal	3391	🗑️
10.2.2.16	System or agent has recently restarted	☑	2012-04-20 18:20:17	--	--	2012-05-02 11:55:15	Internal	3367	🗑️
10.2.2.27	System or agent has recently restarted	☑	2012-04-20 18:20:17	--	--	2012-05-02 11:55:15	Internal	3373	🗑️
LAB-2010-EX.LAB	Mailbox_Total Average Delivery Time has exceeded threshold: (1500s)	☑	2012-04-23 09:30:51	--	--	2012-05-02 11:55:40	Dynamic	2544	🗑️
LAB-2010-EX.LAB	Mailbox Exchange Mailbox Database Average Delivery Time has exceeded threshold: (1500s)	☑	2012-04-23 09:30:51	--	--	2012-05-02 11:55:40	Dynamic	2544	🗑️
10.100.100.28	Drive \\.\PHYSICALDRIVE0 now OK.	☑	2012-03-30 11:11:27	--	--	2012-03-30 11:11:27	Dynamic	1	🗑️

■ 1 Healthy
 ■ 6 Minor
 ■ 3 Major
 ■ 1 Critical

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

- **Name.** Name of the element associated with the event.
- **Event Message | Severity.** Message generated by event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). The message is color-coded for severity.
- **Acknowledged.** Specifies whether a ScienceLogic user has acknowledged this event.
 - *Red check.* Event has not been acknowledged.
 - *Gray check with name.* Event has been acknowledged.
- **Age / Elapse.** Number of days, hours, and minutes since the first occurrence of the event.
- **Ticket.** Ticket ID associated with this event, if applicable.
- **Last Detected.** Date and time of last occurrence of the event.
- **EID.** Unique ID for the event, generated by SL1.
- **Source.** Source of the log message that triggers the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). Choices are:
 - *Syslog .* Event was generated from standard system log generated by device.
 - *Internal.* Event was generated by SL1.
 - *Trap.* Event was generated by an SNMP trap.
 - *Dynamic.* Event was generated by a dynamic application collecting data from the device.
 - *Email.* Event was generated by an email from an external agent; for example, Microsoft Operations Manager (MOM).
 - *API.* Event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
- **Count.** Number of times this event has occurred.
- **View Notifications icon** . Leads to the **Event Actions Log**, where you can view details about each automation policy that has triggered for the event.
- **Statistics icon** . Displays the **Event Statistics** page, where you can view historical statistics for the selected event.
- **Information icon** . Displays the **Event Information** page, where you can view an overview of the selected event, suppress the selected event, or edit the definition of the selected event.

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

Viewing Event Details in the Event Console

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

NOTE: To view the **Event Information** page, accounts of type "user" must be granted one or more access keys that includes the following access hook: Events/Event:View. Accounts of type "user" will then be able to view details for all events in the same organization as the user.

To access the **Event Information** page:

1. Go to the **[Events]** tab.
2. Find the event you are interested in and select its information icon (📄).
3. The **Event Information** page appears.

The screenshot shows the 'Event Information' window for event ID 421. The window title is 'Event_Information'. At the top, it says 'For Event [421]' and has buttons for 'Actions', 'Acknowledge', and 'Clear'. The event message is 'Fan problem, Fan (Fan 1 Critical) state: shutdown'. The severity is 'Critical'. The device is 'ISR-4331-RTR-01'. The first occurrence was on 2016-06-08 at 11:39:59, and the last occurrence was on 2016-07-24 at 17:30:12. The occurrence count is 4100. The policy name is 'Cisco: Fan Critical [2034]' and the policy type is 'Dynamic Event'. The ticket description is empty. The description states: 'Cisco network device is reporting a "Critical" or "Shutdown" status with a cooling fan.' The probable cause includes: 'One or more fans are not operating.', 'The fans are operating too slowly.', and 'The power supply is not operating.' The resolution is: 'Manually check functioning of fan and replace if necessary.' At the bottom, there are fields for 'Correlation Reason' and 'Note', each with a 'Save' button.

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

- **Event ID.** Unique ID for the event, generated by SL1.
- **Event Message.** Message generated by the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit).
- **Severity.** Severity of the event. Choices are:

- *Critical*
 - *Major*
 - *Minor*
 - *Notice*
 - *Healthy*
- **For Element.** Name of the element associated with the event.
 - **First Occurrence.** Number of days and hours since the first occurrence of the event, and date and time of first occurrence of the event.
 - **Last Occurrence.** Number of days and hours since the last occurrence of the event, and date and time of last occurrence of the event.
 - **Occurrence Count.** Number of times this event has occurred on this entity.
 - **Acknowledged On.** Date and time the event was acknowledged.
 - **Acknowledged By.** Username of user who acknowledged the event.
 - **Policy Name/ID.** Name of the event policy, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit) and policy ID.
 - **Policy Type.** Source of the log message that triggers the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). Choices are:
 - *Syslog.* Event was generated from a system log generated by device.
 - *Internal.* Event was generated by SL1.
 - *Trap.* Event was generated by an SNMP trap.
 - *Dynamic.* Event was generated by a Dynamic Application collecting data from the device.
 - *Email.* Event was generated by an email from an external agent; for example, Microsoft Operations Manager (MOM).
 - *API.* Event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
 - **Ticket Description.** Description field from the associated ticket, if applicable.
 - **Probable Cause & Resolution Text.** This pane displays additional information about the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit).
 - **Correlation Reason.** This field displays the user-defined notes about event categories and event correlation. You can enter up to 256 characters in this field. To save your changes, select the **[Save Correlation Reason]** button.
 - **Note.** This field displays the user-defined note associated with the event. To add or edit a note, enter text in this field and then select the **[Save Note]** button.

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

- **Create a Ticket.** Leads to the **Ticket Editor** page, where you can define a new ticket based on the event.

- **Edit Aligned Ticket.** Leads to the **Ticket Editor** page, where you can edit an existing ticket that is based on the event.
- **Edit Aligned Event Policy.** Leads to the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit), where you can edit the properties of the event definition.
- **Edit Device Thresholds.** Leads to the **Device Thresholds** page, where you can define and edit storage and performance thresholds for a device.
- **Suppress Event for This Device.** Suppresses the current event on the current device. When you suppress an event, you are specifying that in the future, if this event occurs again on the same device, the event will not appear in the **Event Console** or the **Viewing Events** page.
- **Refresh This Page.** Updates the page with the latest information.
- **View Device Summary.** Leads to the **Device Summary** page for the device, where you can view overview information on the health of the device, a list of events and tickets associated with the device, a list of elements associated with the device, a list of monitoring policies for the device, and hardware and bandwidth usage for the device.

5. The **[Acknowledge]** button allows you to acknowledge the event.

6. The **[Clear]** button allows you to clear the event.

Customizing the Display in the Event Console

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

- The **Account Preferences** page. In this page, you can select the columns that display on the **Event Console** page.
- The **[Actions]** menu in the **Event Console** page. When you select the *Console Preferences* entry, SL1 displays the **Preferences** modal page, where you can define the appearance and behavior of the **Event Console** page.

Account Preferences

The **Account Preferences** page allows you to change your password and customize some of the behavior and appearance of SL1. The customizations that you choose will appear each time you log in to SL1. They will not affect how SL1 appears to other users.

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

NOTE: To access the **Account Preferences** page, accounts of type "user" must be granted one or more access keys that includes the following access hook: MyPreferences. Accounts of type "user" will then be able to view and edit the settings in the **Account Preferences** page. For more information on Access Keys, see the manual **Access Permissions**.

To access the **Account Preferences** page:

1. Go to the **Account Preferences** page (Preferences > Account > Preferences).

2. In the **Account Preferences** page, you can edit one or more of the fields described below.

The screenshot shows the Account Preferences page. At the top, there are three input fields: 'Existing Password', 'New Password', and 'Confirm New Password', followed by a 'Save' button. Below this is the 'Interface Settings' section, which is divided into three columns of options:

- Left Column (Interface Settings):** Includes 'Default Page' (set to Event Console), 'Theme' (ScienceLogic: White + Blue Tilebars), 'Page Refresh Rate' (5 Minutes), 'Page Result Count' (25), 'Table Row Height' (Small), 'Default Severity Filter' (Healthy), 'Preferred IF Label' (Interface Alias), 'Default Interface Graph Display' (% Utilization), 'Default Date Format' (22/05/2015), and 'Date Format String' (Y-m-d H:i:s).
- Middle Column (Checkboxes):** Includes 'Disable Navbar Auto-hide' (checked), 'View Assigned Tickets Only', 'Show Masked Events', 'Organizational Grouping Events', 'Collapse Organization Events', 'Show Severity Badges', 'Ticket Comment Reverse Sort', 'Disabled Ticket Comment Cloaking', 'Scale Percent Graphs to 100%', 'Code Highlighting', and 'Hide Empty Networks'.
- Right Column (Columns):** Lists columns for 'Event Console Columns', 'Ticket Console Columns', and 'Device Manager Columns'.

A 'Save' button is located at the bottom of the Interface Settings section.

3. The **Change Password** pane allows you to change your password. The following fields appear:

NOTE: Passwords must be between 7 and 64 characters in length.

- **Existing Password.** Type your current password.
- **New Password.** Type your new password.
- **Confirm Password.** Retype your new password.
- **[Save].** Select this button to save changes in the **Change Password** pane.

4. The **Interface Settings** pane allows you to define the appearance and behavior of some pages in SL1. The **Interface Settings** pane contains the following fields:


- **Default Page.** Select the page that automatically appears by default when you log in to SL1. Options include:
 - *None.* SL1 will display the ScienceLogic logo when you log in.
 - *Event Console.* SL1 will display the **Event Console** when you log in.
 - *Ticket Console.* SL1 will display the **Ticket Console** when you log in.
 - *Knowledge Base.* SL1 will display the **Knowledge Base Home** page when you log in.

CAUTION: Due to security vulnerabilities, ScienceLogic recommends that customers who installed SL1 prior to 8.9.2 disable the Knowledge Base. For details, see the release notes for version 8.9.2 of SL1.

- *Device Views*. SL1 will display the **Device Group Map** page (Classic Maps > Device Maps > Device Groups) when you log in.
- *Dashboard*. SL1 will display the selected Dashboard when you log in.
 - **Theme**. Select the backgrounds, colors, and graphics that appear when you log in. Theme entries are defined in the Settings > Themes page.
 - **Page Refresh Rate**. Select how often **Events**, **Tickets**, and **Views** pages in SL1 are refreshed. Options range from 10 seconds to 60 minutes.
 - **Page Result Count**. Select the number of results you want to display on each page that contains lists of entities. Options range from 25 to 500.
 - **Table Row Height**. Affects the row height of all pages that display a table in the main content pane. You can also change this setting in the [Event Console Preferences](#) page, the **Ticket Console Preferences** page, and the user **Account Preferences** page. Changing the setting for row height in the current page, the **Event Console Preferences** page, the **Ticket Console Preferences** page, or the user **Account Preferences** page affects the row height in all pages that display a table in the main content pane. Choices are:
 - *Small*. Sets row height to 17 px and font size to 11 px.
 - *Medium*. Sets row height to 27 px and font size to 12 px.
 - *Large*. Sets row height to 35 px and font size to 13 px.
 - **Default Severity Filter**. Select the minimum event severity that you want to display in the **Event Console** page. Only events of the selected severity and greater will appear in the page. Options include:
 - *Healthy*. Displays all events, including events with a severity of Healthy.
 - *Notice*. Displays all events with a severity of Notice, Major, Minor, and Critical.
 - *Minor*. Displays all events with a severity of Minor, Major, and Critical.
 - *Major*. Displays all events with a severity of Major and Critical.
 - *Critical*. Displays all events with a severity of Critical.
 - **Preferred IF Label**. Select how interfaces will be labeled in all pages and reports that reference network interfaces. Options include:
 - *Interface Alias*. Easy-to-remember, human-readable name for the network interface.
 - *Interface Name*. The name of the network interface.
 - **Default Interface Graph Display**. Select the default unit of measure for the Hourly Interface Usage graph in the **Device Summary** page. Options include:
 - *Interface Default*. The Hourly Interface Usage graph displays the amount of traffic in the unit of measure specified in the **Measurement** field in the **Interface Properties** page for the interface.
 - *% Utilization*. The Hourly Interface Usage graph displays utilization in percent.

- **Default Date Format.** Select the default date format for use throughout SL1.
- **Date Format String.** Select the date format for use throughout SL1. If defined, this date format overrides the default date format. You can use any date variables supported by the PHP date function in this field.

5. The **Checkboxes** pane allows you to configure features that are toggled on or off.

- **Disable NavBar Auto-hide.** If you select this checkbox, the NavBar pane persists after you select a link. This option is selected by default.
- **View Assigned Tickets Only.** If you select this checkbox, by default, only tickets assigned to you are displayed in the **Ticket Console** page.
- **Show Masked Events.** If you select this checkbox, all events that have been grouped together with a device's **Event Mask** setting will be displayed in the **Event Console** page. If you do not select this checkbox, these events are grouped together and rolled-up under the event with the highest severity and you can click on the magnifying-glass icon () to view the masked events.
- **Organizational Grouping Events.** If you select this checkbox, events will be grouped by organization in the **Event Console** page. The **filter-while-you-type** fields and the advanced filter tool will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single filter to events in multiple organizations.
- **Collapse Organization Events.** If you select this checkbox, all organizations with assigned events will be displayed but will be contracted; the **Event Console** page will display only a list of contracted organizations, which can be expanded by clicking on the plus sign (+). The default behavior of SL1 is to expand each organization and display the list of events for each organization.
- **Show Severity Badges.** If you select this checkbox:
 - The value in the **Severity** column will be displayed as a color-coded badge in the **Event Console** page and the **Ticket Console** page.
 - The value in the **Current State** column will be displayed as a color-coded badge in the **Device Manager** page.

If you do not select the **Show Severity Badges** checkbox:

- In the **Event Console** page, the value in the **Event Message** column and the value in the **Severity** column will be painted with the severity color.
- In the **Ticket Console** page, the value in the **Description** column and the **Severity** column will be painted with the severity color.
- In the **Device Manager** page, the value in the **Device Name** column and the value in the **Current State** column will be painted with the severity color.
- **Ticket Comment Reverse Sort.** If you select this checkbox, the *Notes* section of a ticket sorts the ticket's notes from newest to oldest. If you do not select this checkbox, ticket notes display from oldest to newest.
- **Disabled Ticket Comment Cloaking.** If you select this checkbox, then any comments you add to a ticket are viewable to all other users (i.e., not cloaked) by default.

- **Scale Percent Graphs to 100%**. If you select this checkbox, then any graphs that display percentage on the y-axis will display from 0% to 100%, regardless of the highest actual value. If you do not select this checkbox, then the y-axis will display from 0% to the highest actual value.
- **Code Highlighting**. If you select this checkbox, HTML, PHP, Python, and SQL code that displays in SL1 will be highlighted.. You can customize the highlight colors in the **Code Highlighting** page. If selected, syntax highlighting appears in:
 - The **Snippet Editor & Registry** page for Dynamic Applications of type "snippet" (System > Manage > Applications > create/edit > Snippets)
 - The **Dashboard Widget Editor** page (System > Customize > Dashboards > Widgets > create/edit)
 - The **Database Tool** page (System > Tools > DB Tool)
 - The **Action Policy Editor** page for actions of type "Snippet" and "SQL Query" (Registry > Run Book > Actions > create/edit)
 - The **Report Template Editor** page (Reports > Management > Report Manager > create/edit)
- **Hide Empty Networks**. If you select this checkbox, the IPv4 Networks page displays networks that do not include any devices or interfaces.

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

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

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

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

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

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

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

Event Console Preferences

The **Event Console Preferences** page allows you to customize the display and behavior of the **Event Console** page.

NOTE: To access the **Event Console Preferences** page, accounts of type "user" must be granted one or more access keys that includes the following access hook: Events/Event:View. Accounts of type "user" will then be able to view and edit settings in the **Event Console Preferences** page. For more information on Access Keys, see the manual **Access Permissions**.

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

1. Go to the **[Events]** tab.
2. In the **Event Console** page, select the **[Actions]** menu and choose *Console Preferences*.
3. The **Event Console Preferences** page appears.

Edit Event Console Preferences

Event Viewer Preferences Reset

Console Refresh Rate
[5 Minutes]

Default Severity Filter
[Healthy]

Table Row Height
[Small]

Group by Organization

Show Masked Events


Show Severity Badges

Collapse All Organizations
(Note: Enabling supersedes custom layout settings.)

Event Console Columns

- [Name / Link]
- [Type]
- [Acknowledged / User Name]
- [Ticket ID / Link]
- [Event Age / Elapse Time]
- [Last Detected / Date]
- [EID / Event ID]
- [Message Source]
- [Detection Count]
- [Severity]
- External Ticket / Link
- [Note]

Save

4. In the **Event Console Preferences** page, you can customize the following:
- **Console Refresh Rate.** Select how often the **Event Console** page is refreshed. Options range from 10 seconds to 60 minutes.
 - **Default Severity Filter.** Select the minimum event severity that you want to display in the **Event Console** page. Only events of the selected severity and greater will appear in the **Event Console** page. Options include:
 - *Healthy.* Displays all events, including events with a severity of Healthy.
 - *Notice.* Displays all events with a severity of Notice, Major, Minor, and Critical.
 - *Minor.* Displays all events with a severity of Minor, Major, and Critical.
 - *Major.* Displays all events with a severity of Major and Critical.
 - *Critical.* Displays all events with a severity of Critical.
 - **Table Row Height.** Affects the row height of all pages that display a table in the main content pane. You can also change this setting in the system [Account Preferences](#) page, the **Ticket Console Preferences** page, and the user **Account Preferences** page. Changing the setting for row height in the current page, the system **Account Preferences** page, the **Ticket Console Preferences** page, or the user **Account Preferences** page affects the row height in all pages that display a table in the main content pane. Choices are:
 - *Small.* Sets row height to 17 px and font size to 11 px.
 - *Medium.* Sets row height to 27 px and font size to 12 px.
 - *Large.* Sets row height to 35 px and font size to 13 px.
 - **Group by Organization.** If you select this checkbox, events will be grouped by organization. The *filter-while-you-type* fields and the Advanced Filter Tool will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single filter to events in multiple organizations.
 - **Show Masked Events.** If you select this checkbox, all events that have been grouped together with a device's **Event Mask** setting will be displayed in the **Event Console** page. If you do not select this checkbox, these events are grouped together and rolled-up under the event with the highest severity and you can click on the magnifying-glass icon () to view the masked events.
 - **Show Severity Badges.** If you select this checkbox:
 - The value in the **Severity** column will be displayed as a color-coded badge in the **Event Console** page and the **Ticket Console** page.
 - The value in the **Current State** column will be displayed as a color-coded badge in the **Device Manager** page.If you do not select the **Show Severity Badges** checkbox:
 - In the **Event Console** page, the value in the **Event Message** column and the value in the **Severity** column will be painted with the severity color.

- In the **Ticket Console** page, the value in the **Description** column and the **Severity** column will be painted with the severity color.
- In the **Device Manager** page, the value in the **Device Name** column and the value in the **Current State** column will be painted with the severity color.
- **Collapse All Organizations.** If you select this checkbox, all organizations with assigned events will be displayed but will be contracted; the **Event Console** page will display only a list of contracted organizations, which can be expanded by clicking on the plus sign (+). The default behavior of SL1 is to expand each organization and display the list of events for each organization.
- **Event Console Columns.** In this list, select the columns that you want to display by default in the **Event Console** page.

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

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

Hiding the Header Bar

You can also customize the display of the **Event Console** by hiding the header bar. To hide the header bar, click on the arrow in the top right of the **Event Console** (above the **[Guide]** button).


The screenshot displays the ScienceLogic Event Console interface. At the top, there are navigation tabs: Inbox, Dashboard, Views, Events, Tickets, Knowledge, Reports, Registry, System, and Preferences. The main area shows a list of events under the 'Event Console' header. The list includes columns for Organization, Name, Type, Event Message, Severity, Acknowledged, Note, Ticket, Age / Elapsed, Last Detected, EQ, Source, Count, and Notify. A legend at the bottom indicates severity levels: 0 Healthy (green), 1 Notice (yellow), 0 Minor (orange), 28 Major (red), and 12 Critical (dark red). A small arrow icon is located in the top right corner of the event list area, above the [Guide] button.

Event Masks in the Event Console

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

NOTE: For more information on the **Device Properties** page, see the chapter *Managing a Single Device with the Device Administration Panel* in the **Device Management** manual.

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

- By default, when events are masked, the **Event Console** displays all events that occur on the device within the specified timespan under a single event, the one with the highest severity. The magnifying-glass icon () appears to the left of the event. When you click on the magnifying-glass icon, the **Suppression Group** modal page appears. This page includes details about all events that are masked under the displayed event.
- If an event has **Occurrence Count** and **Occurrence Time** set in its **Event Policy Editor** page, SL1 will use the very first logged occurrence of the event to calculate the **Event Mask**, even if that first occurrence did not appear in the **Event Console** (due to the **Occurrence Count** and **Occurrence Time** fields).
 - For example, suppose an event, *event_x*, has an **Occurrence Count** of "3" and an **Occurrence Time** of "10 minutes." This means that the event must occur on the same device at least three times within 10 minutes before the event appears in the **Event Console**. Suppose the event, *event_X*, occurs on *device_A* at 15:51, 15:52, and 15:53. The event will appear in the **Event Console** with a time stamp of "15:53," an age of "2 minutes," and a count of "3."
 - Suppose *device_A* includes an **Event Mask** of "Group in blocks every 5 minutes." To calculate how to group *event_x*, the **Event Mask** will use the time stamp of the first occurrence, 15:51, even though the event did not appear in the **Event Console** at that time. The **Event Mask** will also use the time of the first occurrence, 15:51, to calculate the "Age/Elapsed" value for the event in the **Suppression Group** modal page.
- If you want masked events to appear in the **Event Console** by default, go the **Event Console Preferences** page (Events > Actions > Console Preferences), and enable the **Show Suppressed Events** field.

Chapter



3

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 the menu options, click the Advanced menu icon ()

For more information about infrastructure monitoring with advanced event suppression, watch the video at <https://sciencelogic.com/product/resources/feature-spotlight-infrastructure-monitoring-advanced-event-suppression>.

This chapter includes the following topics:

<i>Responding to Events</i>	55
<i>Selecting Multiple Events</i>	55
<i>Acknowledging and Clearing Events</i>	56
<i>Viewing and Editing Event Notes</i>	57
<i>Viewing the Event Policy</i>	57
<i>Suppressing and Unsuppressing an Event for a Device</i>	58
<i>Suppressing an Event</i>	58
<i>Suppressing an Event on Multiple Devices</i>	59
<i>Unsuppressing an Event</i>	61
<i>Unsuppressing All Instances of an Event</i>	62
<i>Enabling and Disabling Events</i>	62

Disabling Events	63
Enabling Events	63
Creating a Ticket from an Event	64
Responding to Events in the Event Console in the Classic SL1 User Interface	65
Adding a Note About an Event	66
Adding a Note to Multiple Events	67
Clearing One or More Events	68
Suppressing an Event on a Single Device	70
Suppressing an Event On Multiple Devices	71
Unsuppressing an Event	73
Unsuppressing All Instances of an Event	74
Disabling an Event	75
Enabling an Event	76

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 **Events** page and can be included in automation actions.
- **Clear.** Removes an instance of an event from the **Events** page. The cleared instance is no longer displayed.
- **Suppress.** Specifies that if the event occurs again on the same device, the event will not be displayed in the **Events** page.
- **Disable.** Specifies that if the event occurs on any device or is triggered by any application or policy, the event will not appear in the Event Console.

Selecting Multiple Events

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

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

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

Acknowledging and Clearing Events

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

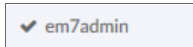
When you **clear** an event, you let other users know that this event has been addressed. Clearing an event removes a single instance of the event from the **Events** page. If the event occurs again on the same device, it will reappear in the **Events** page.

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.

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

To acknowledge and clear events:

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



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


2. To see when an event was acknowledged and who acknowledged it, hover your mouse over an acknowledged field.
3. If an event was acknowledged by another user and you have the relevant permissions, you can click the **[Reacknowledge]** button to acknowledge that event.
4. To clear an event, click the **[Clear]** button. The event is removed from the **Events** page.

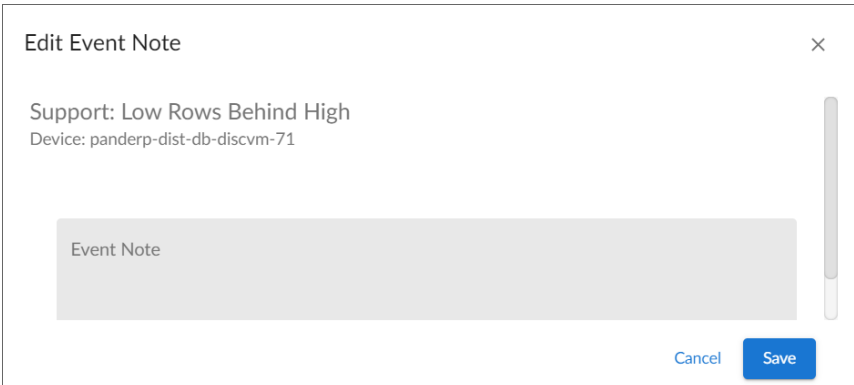
TIP: If you want to hide the **[Acknowledge]** or **[Clear]** buttons on the **Events** page, click the **Select Columns** icon (⚙️) and deselect those columns.

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:



The screenshot shows a modal window titled "Edit Event Note" with a close button (X) in the top right corner. The window contains the following text: "Support: Low Rows Behind High" and "Device: panderp-dist-db-discvm-71". Below this text is a large, empty text input field labeled "Event Note". At the bottom right of the window, there are two buttons: "Cancel" and "Save".

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.

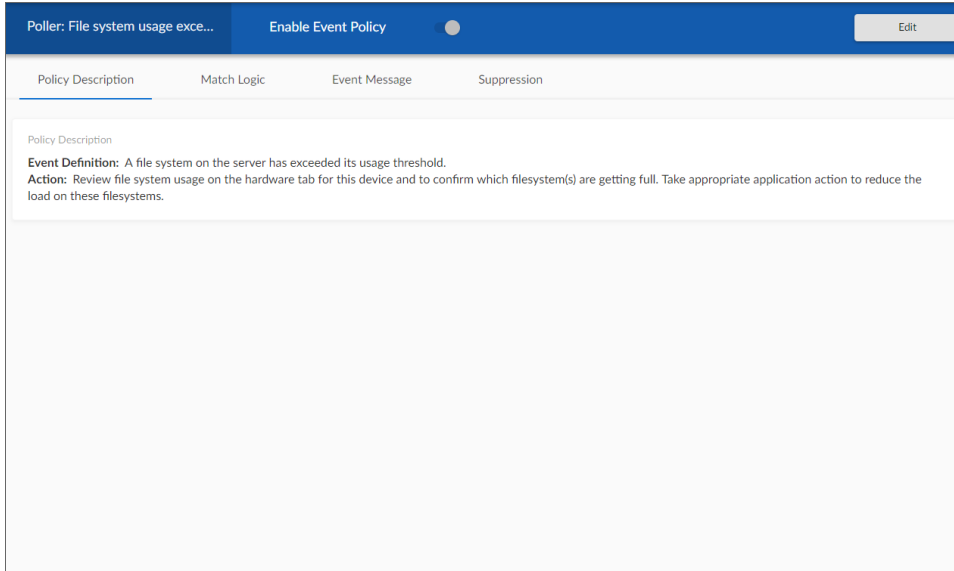
2. Type your additional text for the event note and then click **[Save]**. The event note is updated.

Viewing the Event Policy

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

To view an Event Policy from the **Events** page:

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



2. Click the **[Edit]** button to edit the Event Policy. For information about creating and editing an Event Policy, see the [Defining an Event Policy](#) section.

Suppressing and Unsuppressing an Event for a Device

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

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

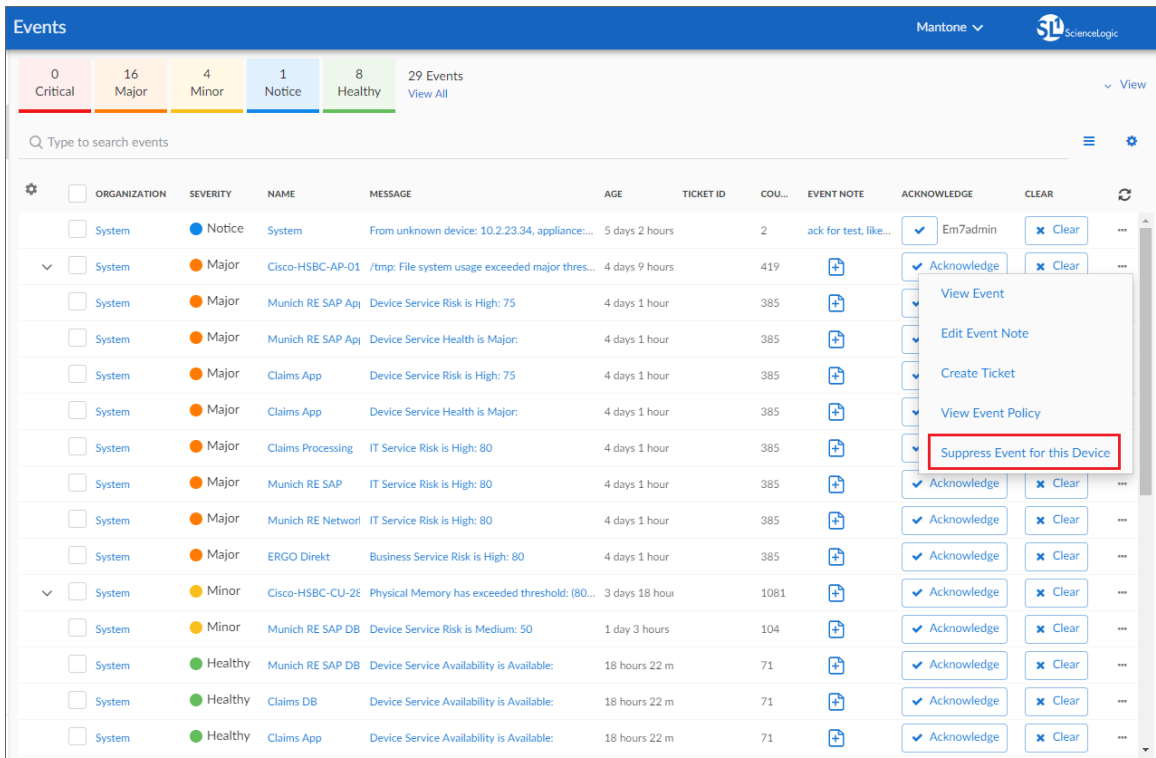
When you suppress an event, the current instance of the event still appears in the **Events**. To remove the current instance from the event console, clear the event (see the section [Clearing One or More Events](#)).

NOTE: To suppress an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Events/Event:View and Event:Clear. Accounts of type "user" will then be able to view and suppress events that belong to the same organization(s) as the user. For more information on access hooks, see the manuals [Access Permissions](#) and [Organizations and Users](#).

Suppressing an Event

To suppress an event:

1. Go to the **Events** page.
2. Click the **Actions** button (*******) for the event you want to suppress and select *Suppress Event for this Device*:



In the future, if this event occurs again on the same device, the event will not appear in the **Events** page.

NOTE: Users of type "user" can view only suppressed events that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all suppressed events.

Suppressing an Event on Multiple Devices

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

To suppress an event on multiple devices:

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

NAME	STATUS	TYPE	WEIGHT	SEVERITY
<input type="checkbox"/> % SASL Plain Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
<input type="checkbox"/> % Vtg Token Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
<input type="checkbox"/> AKCP: AC Voltage sensor detects no current	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: AC Voltage sensor now reporting Normal Status	Enabled	Syslog	0	Healthy
<input type="checkbox"/> AKCP: DC Voltage High Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: DC Voltage sensor High Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: DC Voltage sensor Low Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: DC Voltage sensor Low Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: DC Voltage sensor returned to Normal Status	Enabled	Syslog	0	Healthy
<input type="checkbox"/> AKCP: Dry Contact Sensor Low Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: Dry contact sensor now Normal	Enabled	Syslog	2	Healthy
<input type="checkbox"/> AKCP: Humidity High Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: Humidity Low Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: Smoke Detector Alert!	Enabled	Syslog	10	Critical
<input type="checkbox"/> AKCP: Smoke detector now Normal Status	Enabled	Syslog	4	Healthy
<input type="checkbox"/> AKCP: Water Sensor has detected water	Enabled	Syslog	0	Critical

- In the **Event Policies** page, select the Actions menu (**...**) of the event policy you want to edit and select *Edit*.
- The selected event policy is displayed in the **Event Policy Editor** page, where you can edit one or more properties of the event policy.
- Click the **[Suppression]** tab.

Policy Name: [] Enable Event Policy: Cancel Save

Policy Description Match Logic Event Message **Suppression**

Devices

No Devices Selected **No Device Groups Selected**

- On the **[Suppression]** tab, you can select the devices or device groups on which to suppress the event. To do so:

- Click **[Select Devices]** to select one or more devices on which to suppress the event. When you click **[Select Devices]**, the **Available Devices** modal page appears. Select the checkboxes of the devices you want to add to the suppression list, and then click **[Select]**.
- Click **[Select Device Groups]** to select one or more device groups on which to suppress the event. When you click **[Select Device Groups]**, the **Available Device Groups** modal page appears. Select the checkboxes of the device groups you want to add to the suppression list, and then click **[Select]**.

6. Click **[Save]**.

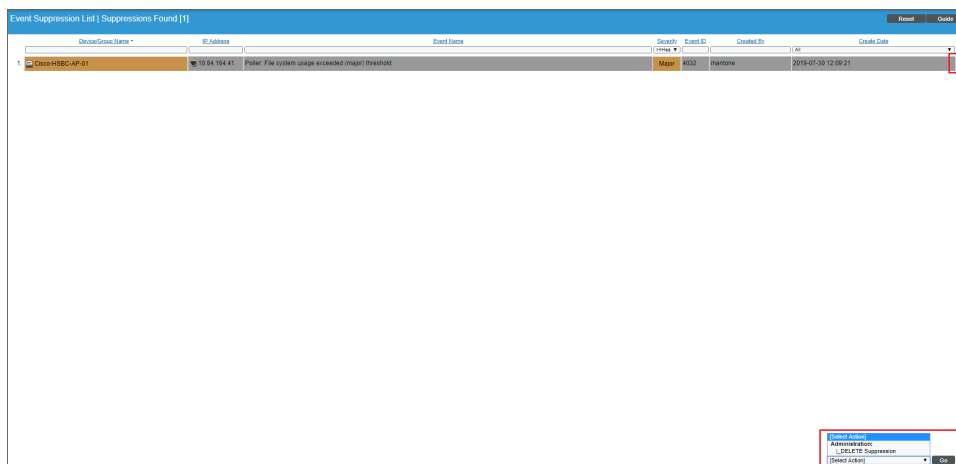
Unsuppressing an Event

You can view a list of all suppressed events in SL1 and choose to unsuppress one or more of those events. When you unsuppress an event, if this event occurs again on the same device, the event will appear in the **Events** page.

NOTE: To unsuppress an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Suppressions, and Event:Suppressions. Accounts of type "user" will then be able to view a list of suppressed events that belong to the same organization as the user. Accounts of type "user" will also be able to unsuppress one or more of these suppressed events. For more information on access hooks, see the manuals **Access Permissions** and **Organizations and Users**.

To unsuppress an event:

1. Go to the **Event Suppression List** page (Events > Suppressions).
2. Select the checkbox for each event you want to unsuppress.



3. In the **Select Action** drop-down menu, in the lower right, select **DELETE Suppression**.
4. Click **[Go]**. In the future, if the unsuppressed event occurs again on the same device, the event will appear in the **Events** page.

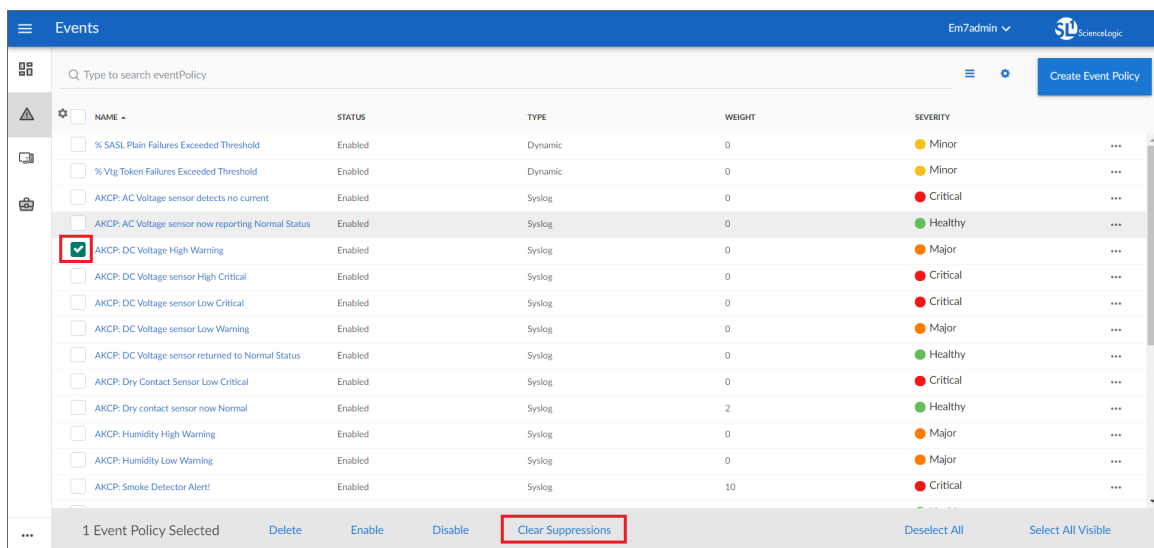
Unsuppressing All Instances of an Event

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

NOTE: To unsuppress an event on all devices, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Accounts of type "user" will then be able to access the **Event Policies** page and unsuppress one or more events on all devices. For more information on access hooks, see the manuals **Access Permissions** and **Organizations and Users**.

To unsuppress an event on all devices:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the checkbox for the event you want to unsuppress on all devices.



3. Click **[Clear Suppressions]**.

In the future, if the unsuppressed event occurs again on any device, it will appear in the **Events** page or in the **Viewing Events** page for the device.

Enabling and Disabling Events

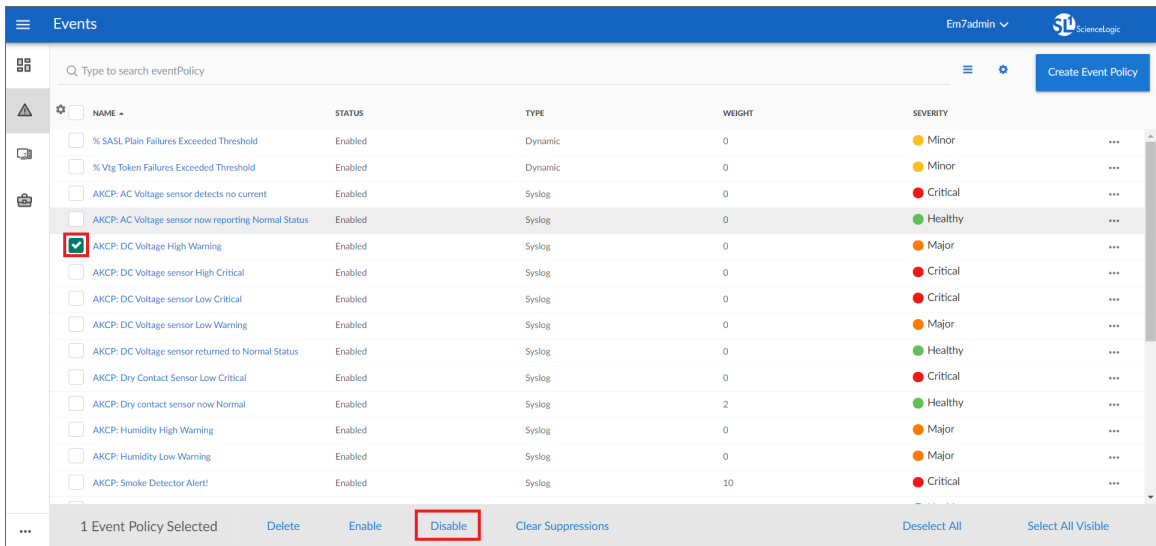
You can simultaneously disable one or more events on all devices. When an event is disabled, it will no longer appear in the **Events** page for any devices. You can also enable an event that has been disabled.

NOTE: To disable or enable an event on all devices, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Accounts of type "user" will then be able to access the **Event Policies** page and enable one or more events on all devices. For more information on access hooks, see the manuals *Access Permissions* and *Organizations and Users*.

Disabling Events

To disable one or more events:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the checkboxes for the events you want to disable.



NAME	STATUS	TYPE	WEIGHT	SEVERITY
<input type="checkbox"/> % SASL Plain Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
<input type="checkbox"/> % Vtg Token Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
<input type="checkbox"/> AKCP: AC Voltage sensor detects no current	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: AC Voltage sensor now reporting Normal Status	Enabled	Syslog	0	Healthy
<input checked="" type="checkbox"/> AKCP: DC Voltage High Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: DC Voltage sensor High Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: DC Voltage sensor Low Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: DC Voltage sensor Low Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: DC Voltage sensor returned to Normal Status	Enabled	Syslog	0	Healthy
<input type="checkbox"/> AKCP: Dry Contact Sensor Low Critical	Enabled	Syslog	0	Critical
<input type="checkbox"/> AKCP: Dry contact sensor now Normal	Enabled	Syslog	2	Healthy
<input type="checkbox"/> AKCP: Humidity High Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: Humidity Low Warning	Enabled	Syslog	0	Major
<input type="checkbox"/> AKCP: Smoke Detector Alert!	Enabled	Syslog	10	Critical

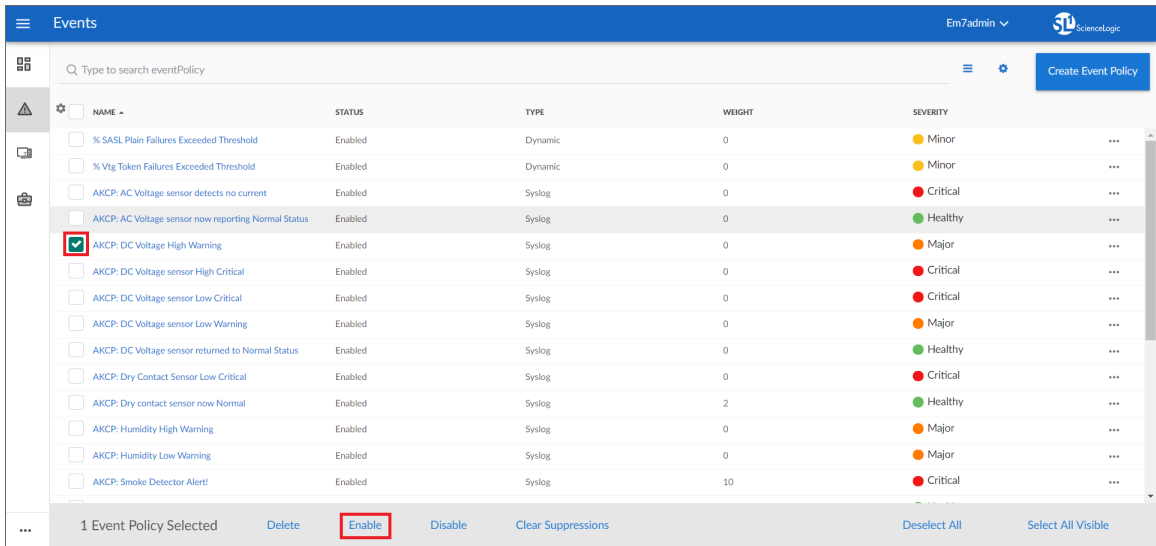
3. Click **[Disable]**.

The selected event(s) will no longer appear in SL1 for any device, application, or policy.

Enabling Events

To enable one or more events:

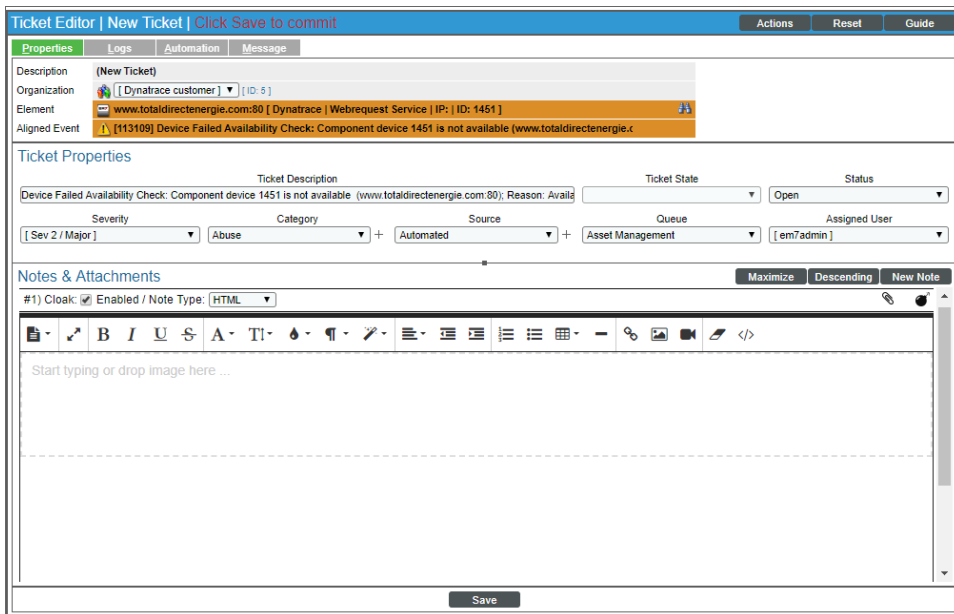
1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the checkboxes for the events you want to enable.



3. Click **[Enable]**. The selected event(s) will once again appear in SL1.

Creating a Ticket from an Event

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.



Responding to Events in the Event Console in the Classic SL1 User Interface

The **Event Console** page in the classic user interface allows you to acknowledge new events as they are detected by the system. Acknowledging an event lets other users know that you are aware of the event and working to resolve it.

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

NOTE: To acknowledge an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Events/Event:View and Event: Acknowledge. Accounts of type "user" will then be able to view and acknowledge events in the same organization(s) as the user. For more information on Access Keys, see the manual **Access Permissions**.

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

To acknowledge a single event:

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

Event ID	Source	Severity	Description	Time	Actions
7	WIN1-THYFO6RJR	Critical	File system usage exceeded critical threshold. Limit: 95.0%, Actual: 100.00%	2012-09-06 17:40:25	[Ack] [Go]
8	aus-rt-1	Major	Swap Memory has exceeded threshold: (60% currently) (100%)	2012-09-06 17:40:05	[Ack] [Go]
9	CTRS81	Major	BH server: Power Supply 2 Status is Error	2012-09-06 17:30:18	[Ack] [Go]
10	CMPLSESEV01	Major	DEL OMI: Chassis Status is Critical	2012-09-06 17:40:06	[Ack] [Go]
11	jeppad10	Major	jeppad10: File system usage exceeded major threshold. Limit: 85.0%, Actual: 89.57%	2012-09-06 17:40:25	[Ack] [Go]
12	iem7	Major	data local: File system usage exceeded major threshold. Limit: 85.0%, Actual: 89.00%	2012-09-06 17:40:25	[Ack] [Go]
13	iem7	Major	Swap memory utilization has exceeded threshold: (80% currently) (80%)	2012-09-06 17:40:13	[Ack] [Go]
14	iem7_db	Major	data local: File system usage exceeded major threshold. Limit: 85.0%, Actual: 88.00%	2012-09-06 17:40:25	[Ack] [Go]
15	afq-WZK3-JUMP01	Major	Swap Memory has exceeded threshold: (80% currently) (100%)	2012-09-06 17:40:05	[Ack] [Go]
16	HALSRV	Major	B1: File system usage exceeded major threshold. Limit: 85.0%, Actual: 89.88%	2012-09-06 17:40:25	[Ack] [Go]
17	afq-F591A1nframe	Major	File Status Critical	2012-09-06 17:31:05	[Ack] [Go]
18	afq-cucm7	Major	File system usage exceeded major threshold. Limit: 85.0%, Actual: 80.86%	2012-09-06 17:40:25	[Ack] [Go]
19	System	Major	Round alert rate critical: 10892 (Internal messages in 5 minutes)	2012-09-06 17:38:55	[Ack] [Go]
20	10.20.30.176	Minor	Printer Bypass paper tray empty. Bypass	2012-09-06 17:32:19	[Ack] [Go]
21	10.20.30.191	Minor	Printer Tray B paper tray empty. Tray B	2012-09-06 17:32:20	[Ack] [Go]
22	10.20.30.8	Minor	Printer Toner Cartridge OKI DATA CORP toner low, current level: 1% full	2012-09-06 17:32:22	[Ack] [Go]
23	10.4.6.11	Minor	System or agent has recently restarted	2012-09-06 17:40:10	[Ack] [Go]
24	10.4.1.77	Minor	Interface state changed to operationally down: 70. Name: S11, previous state was unknown (4)	2012-09-06 17:32:22	[Ack] [Go]
25	10.4.1.77	Minor	Interface state changed to operationally down: 1. Name: sc0, previous state was unknown (4)	2012-09-06 17:05:31	[Ack] [Go]
26	afqce 1016D	Minor	Printer Bypass Tray paper tray empty. Bypass Tray	2012-09-06 17:32:17	[Ack] [Go]
27	ev-8510-1-cisco.com	Minor	System or agent has recently restarted	2012-09-06 17:40:10	[Ack] [Go]
28	DELL2A72DA	Minor	Physical Memory has exceeded threshold: (80% currently) (100%)	2012-09-06 17:40:13	[Ack] [Go]
29	iem7	Minor	Physical Memory has exceeded threshold: (80% currently) (80%)	2012-09-06 17:40:13	[Ack] [Go]
30	iem7_db	Minor	Physical Memory has exceeded threshold: (80% currently) (82%)	2012-09-06 17:40:12	[Ack] [Go]
31	iem7_db	Minor	Physical Memory has exceeded threshold: (80% currently) (89%)	2012-09-06 17:40:11	[Ack] [Go]
32	iem7_db	Minor	Physical Memory has exceeded threshold: (80% currently) (90%)	2012-09-06 17:40:08	[Ack] [Go]
33	excrcat	Minor	Physical Memory has exceeded threshold: (80% currently) (86%)	2012-09-06 17:40:11	[Ack] [Go]
34	hp1.dmc.esri.com	Minor	Physical Memory has exceeded threshold: (80% currently) (99%)	2012-09-06 17:40:10	[Ack] [Go]
35	LAB-VENTER.ScienceLogic.local	Minor	Physical Memory has exceeded threshold: (80% currently) (92%)	2012-09-06 17:40:08	[Ack] [Go]
36	PCDM1	Minor	Physical Memory has exceeded threshold: (80% currently) (97%)	2012-09-06 17:40:05	[Ack] [Go]
37	PROD-SEN-POP.roadsvlab.com	Minor	Cisco Carrier Routing System SPA Interface Processor Card has exceeded threshold: (80% currently) (2534%)	2012-09-06 17:40:10	[Ack] [Go]
38	server-651	Minor	Printer HP Tray paper tray empty. HP Tray	2012-09-06 17:32:15	[Ack] [Go]
39	SAUR9214E	Minor	Physical Memory has exceeded threshold: (80% currently) (90%)	2012-09-06 17:40:05	[Ack] [Go]
40	TOSHIBA-e-STUD0451c	Minor	Printer Cassette1 paper tray empty. Cassette1	2012-09-06 17:32:20	[Ack] [Go]
41	inCom	Minor	Physical Memory has exceeded threshold: (80% currently) (100%)	2012-09-06 17:40:10	[Ack] [Go]
42	TULPTYS-ACCOUNTING	Minor	Printer Magneta Cartridge toner low, current level: 0% full	2012-09-06 17:32:16	[Ack] [Go]
43	WIN-RHA38609PO.ScienceLogic	Minor	Physical Memory has exceeded threshold: (80% currently) (80%)	2012-09-06 17:40:05	[Ack] [Go]
44	ibany-01	Notice	Interface state changed to admin up: 2. Name: ethernet0/1, previous state was down (2)	2012-09-06 17:34:57	[Ack] [Go]
45	ibany-01	Notice	Interface state changed to admin up: 1. Name: ethernet0/0, previous state was down (2)	2012-09-06 17:20:32	[Ack] [Go]
46	CMPLSESEV01	Healthy	Del Voltage Status is Normal	2012-09-06 17:32:21	[Ack] [Go]
47	iem7_cu	Healthy	Network Latency below threshold	2012-09-06 17:37:06	[Ack] [Go]
48	iem7_cu	Healthy	Network Latency below threshold	2012-09-06 17:32:38	[Ack] [Go]
49	iosdashed	Healthy	Temperature normal, now: 76	2012-09-06 17:40:11	[Ack] [Go]

To acknowledge multiple events:

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

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

Adding a Note About an Event

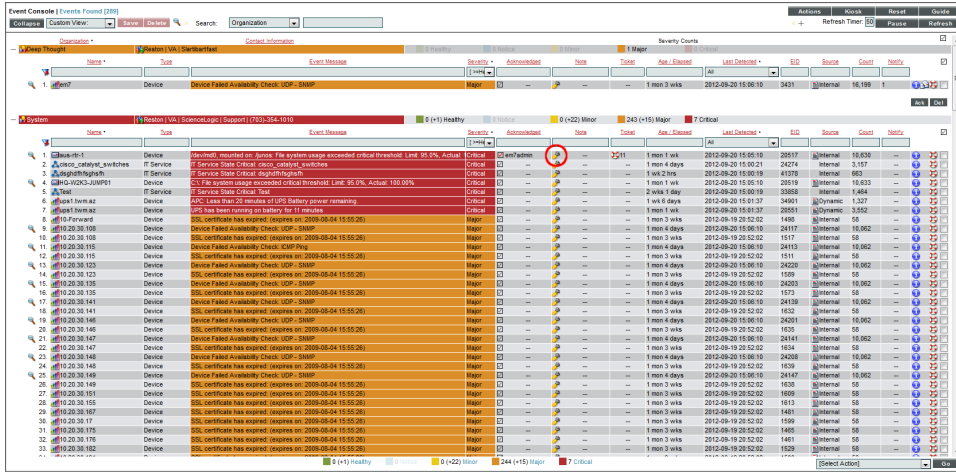
You can add brief notes to an event in the **Event Console** page. Each note will appear in the **Note** column for an event. SL1 does not keep a historical record of each note.

NOTE: A note can be included in an action policy by using the `%_user_note` variable. For details on creating automation policies and action policies, see the manual *Using Run Book Automation*.

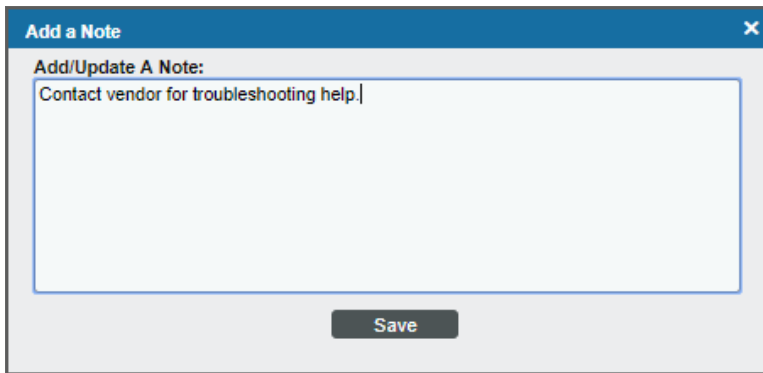
To create or edit a note for an event:

- In the **Event Console** page, find the event to which you want to add a note.

- In the **Note** column for that event, click on the wrench icon (🔧).



- In the **Add a Note** modal page, enter the note text. Click **[Save]** to save the note.



- The new or edited text appears in the **Note** column for the event.

Adding a Note to Multiple Events

You can add a brief note to multiple events simultaneously and/or overwrite existing notes for multiple events. The note will appear in the **Note** column for each event and in the **Note** field in the **Event Information** page for each event. SL1 does not keep a historical record of each note.

NOTE: A note can be included in an action policy by using the `%_user_note` variable. For details on creating automation policies and action policies, see the manual *Using Run Book Automation*.

To create or edit a note for multiple events:

- In the **Event Console** page, find the events for which you want to add a note and/or overwrite the existing note.

- For each event that you want to add and/or edit a note, select the checkbox in the last column.
- In the **Select Action** drop-down field, select **Add/Update Event Note**, then click the **[Go]** button.

Organization	Name	Type	Event Message	Severity	Acknowledged	Total	External Ticket	Age/Classed	Last Detected	EID	Source	Count	Notify
System	10.20.0.180	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	<input type="checkbox"/>	273458		1 mon 1 day	26/12/2013 12:30:14 pm	8227328	Dynamic	8,353	379
System	10.20.0.181	Device	Printer Tray B paper tray empty: Tray B	Minor	<input type="checkbox"/>	273454		1 mon 1 day	26/12/2013 12:31:25 pm	8226448	Dynamic	8,361	368
System	10.20.0.191	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	<input type="checkbox"/>	273707		1 mon 1 day	26/12/2013 12:30:37 pm	8220350	Dynamic	8,352	366
System	192.168.34.64	Device	App. 238, Snippet: 135 reported a collection problem (Explanation: (noSuchName) There is a	Minor	<input type="checkbox"/>	273421		1 mon 1 day	26/12/2013 12:31:08 pm	8225178	Internal	2,783	450
System	192.168.37.10	Device	Network latency exceeded threshold: No Response	Minor	<input type="checkbox"/>	273457		1 mon 1 day	26/12/2013 12:32:21 pm	8228142	Internal	20,877	20
System	Acro 10180	Device	Printer Bypass Tray paper tray empty: Bypass Tray	Minor	<input type="checkbox"/>	273541		1 mon 1 day	26/12/2013 12:31:25 pm	8220491	Internal	1,393	396
System	lan-brands-004	Device	Physical Memory has exceeded threshold: (80%) currently (84%)	Minor	<input type="checkbox"/>	273455		1 day 10 hrs	26/12/2013 12:30:12 pm	8536783	Dynamic	499	1
System	AVNCT018	Device	App. 238, Snippet: 135 reported a collection problem (Explanation: (noSuchName) There is a	Minor	<input type="checkbox"/>	273423		1 mon 1 day	26/12/2013 12:30:47 pm	8228189	Internal	2,784	400
System	BSM01090R002.008.dns	Device	CPU: 1 has exceeded threshold: (80%) currently (8499%)	Minor	<input type="checkbox"/>	273812		1 mon 1 day	26/12/2013 12:30:17 pm	8228220	Dynamic	8,345	17
System	SR1_C372CF	Device	Network latency exceeded threshold: No Response	Minor	<input type="checkbox"/>	273455		1 wk 21 hrs	26/12/2013 12:32:21 pm	8492599	Internal	5,677	1
System	AS5500-2	Device	CPU: 9 has exceeded threshold: (90%) currently (50000%)	Minor	<input type="checkbox"/>	273805		1 mon 1 day	26/12/2013 12:30:28 pm	8227930	Dynamic	8,353	19
System	CHWEB-01	Device	Physical Memory has exceeded threshold: (80%) currently (95%)	Minor	<input type="checkbox"/>	273455		1 wk 5 days	26/12/2013 12:30:05 pm	8421668	Dynamic	3,653	1
System	cisco-iosrtr1000-0	Device	Network latency exceeded threshold: No Response	Minor	<input type="checkbox"/>	273455		1 mon 1 day	26/12/2013 12:32:21 pm	8228140	Internal	20,877	26
System	isco_10.20.1.15	Device	CPU: 9 has exceeded threshold: (90%) currently (2489%)	Minor	<input type="checkbox"/>	273455		15 hrs 7 mins	26/12/2013 12:30:28 pm	8546685	Dynamic	101	1
System	isco_10.20.0.106	Device	PSUA: ECHO RTT 0 is above the minor threshold 999 999 ms, currently 683 ms	Minor	<input type="checkbox"/>	273455		52 mins 34 secs	26/12/2013 12:25:28 pm	8546673	Dynamic	4	1
System	isco_10.20.1.112	Device	CPU: 1 has exceeded threshold: (90%) currently (1050%)	Minor	<input type="checkbox"/>	273455		1 day 12 hrs	26/12/2013 12:30:09 pm	8536437	Dynamic	444	1
System	isco_10.20.0.129	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273388		1 mon 1 day	26/12/2013 12:30:04 pm	8220296	Internal	8,352	401
System	isco_10.20.1.4	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273380		1 mon 1 day	26/12/2013 12:30:05 pm	8228172	Internal	8,352	401
System	isco_10.20.1.9	Device	Printer Printer Cover: Simon cover open: Printer Cover Simon	Minor	<input type="checkbox"/>	273455		3 wks 1 day	26/12/2013 12:31:11 pm	8241686	Dynamic	1,959	1
System	isco_10.20.0.21	Device	CPU: 1 has exceeded threshold: (80%) currently (100%)	Minor	<input type="checkbox"/>	273455		17 mins 36 secs	26/12/2013 12:25:18 pm	8546680	Dynamic	3	1
System	isco_10.20.0.22	Device	CPU: 1 has exceeded threshold: (80%) currently (96%)	Minor	<input type="checkbox"/>	273455		21 mins 51 secs	26/12/2013 12:30:30 pm	8546885	Dynamic	4	1
System	isco_10.20.0.30	Device	CPU: 1 has exceeded threshold: (80%) currently (100%)	Minor	<input type="checkbox"/>	273455		17 mins 21 secs	26/12/2013 12:30:07 pm	8546608	Dynamic	4	1
System	Conference-Room	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273455		3 wks 2 hrs	26/12/2013 12:30:05 pm	8407086	Internal	3,706	1
System	as-0m	Device	App. 238, Snippet: 135 reported a collection problem (Explanation: Timeout)	Minor	<input type="checkbox"/>	273455		1 day 1 hr	26/12/2013 12:31:08 pm	8540520	Internal	78	1
System	as-0m	Device	App. 238, Snippet: 129 reported a collection problem (Explanation: Timeout)	Minor	<input type="checkbox"/>	273455		6 days 20 hrs	26/12/2013 12:30:28 pm	8481750	Internal	1,910	1
System	as-0m	Device	Physical Memory has exceeded threshold: (80%) currently (97%)	Minor	<input type="checkbox"/>	273455		2 days 14 hrs	26/12/2013 12:25:34 pm	8525317	Dynamic	403	1
System	as-0m	Device	Physical Memory has exceeded threshold: (80%) currently (97%)	Minor	<input type="checkbox"/>	273455		2 hrs 42 mins	26/12/2013 12:10:07 pm	8546973	Dynamic	13	1
System	isco-8510-1-cisco.com	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273388		1 mon 1 day	26/12/2013 12:30:04 pm	8220296	Internal	8,352	401
System	DEL0159101977F	Device	Printer HP Tray paper tray empty: HP Tray	Minor	<input type="checkbox"/>	273425		1 mon 1 day	26/12/2013 12:31:12 pm	8228229	Dynamic	1,392	400
System	DEL02472DA	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	<input type="checkbox"/>	273733		1 mon 1 day	26/12/2013 12:30:44 pm	8228283	Dynamic	8,343	366
System	ish_p2_ao	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273455		27 mins 36 secs	26/12/2013 12:10:06 pm	8546642	Internal	2	1
System	em7	Device	Physical Memory has exceeded threshold: (80%) currently (86%)	Minor	<input type="checkbox"/>	273455		1 wk 11 hrs	26/12/2013 12:30:16 pm	847268	Dynamic	1,953	1
System	em7	Device	Physical Memory has exceeded threshold: (80%) currently (84%)	Minor	<input type="checkbox"/>	273455		1 wk 52 hrs	26/12/2013 12:30:08 pm	847368	[Select Action]	1	1
System	em7	Device	Physical Memory has exceeded threshold: (80%) currently (81%)	Minor	<input type="checkbox"/>	273455		17 mins 36 secs	26/12/2013 12:30:08 pm	854900	[Administration: Clear]	1	1
System	em7	Device	Physical Memory has exceeded threshold: (80%) currently (95%)	Minor	<input type="checkbox"/>	273455		1 wk 12 hrs	26/12/2013 12:30:07 pm	847376	[Acknowledge]	1	1
System	em7	Device	Physical Memory has exceeded threshold: (80%) currently (94%)	Minor	<input type="checkbox"/>	273455		1 wk 12 hrs	26/12/2013 12:30:06 pm	847384	[Get External Ticket]	1	1
System	em7	Device	App. 238, Snippet: 129 reported a collection problem (Explanation: Timeout)	Minor	<input type="checkbox"/>	273455		52 mins 34 secs	26/12/2013 11:40:23 am	8546667	[Add]	1	1
System	em7pdufw	Device	Physical Memory has exceeded threshold: (80%) currently (82%)	Minor	<input type="checkbox"/>	273737		1 mon 1 day	26/12/2013 12:30:37 pm	8228289	[Add/Update Event Note]	1	1

- In the **Add a Note** modal page, enter the text for the note. Click the **[Save]** button.

- The new or edited text appears in the **Note** column for each selected event.

Clearing One or More Events

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

NOTE: To clear an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Events/Event:View and Event: Clear. Accounts of type "user" will then be able to view and clear events in the same organization(s) as the user. For more information on access hooks, see the manuals *Access Permissions* and *Organizations and Users*.

To clear an event:

1. Go to the **[Events]** tab.
2. In the **Event Console** page, select the checkbox for each event you want to clear. To select all events in an organization, click the checkmark icon above each organization's group of events.

The screenshot shows the Event Console interface with a table of events. The table has columns for Organization, Device, Event Name, Severity, Status, Time, and Actions. Several events are selected with checkboxes. A legend at the bottom indicates severity levels: 4 Healthy, 2 Notice, 24 Minor, 12 Major, and 7 Critical. A 'Select Action' dropdown menu is visible at the bottom right, with 'Clear' and 'Go' options highlighted.

Organization	Device	Event Name	Severity	Status	Time	Actions
WIN11HY0YOBUR	Device	File system usage exceeded critical threshold. Limit: 50.0%, Actual: 100.00%	Critical	...	58 mins 4 secs	[X] [Del] [Go]
user-tr-1	Device	Swap Memory has exceeded threshold. (80% currently (100%))	Major	...	1 hr 17 mins	[X] [Del] [Go]
CTRS81	Device	BM server: Power Supply 2 Status is Error	Major	...	1 hr 1 min	[X] [Del] [Go]
CHPLCSERV01	Device	BIU Off: Chassis Status is Critical	Major	...	1 hr 23 mins	[X] [Del] [Go]
ESOP010	Device	Backup: File system usage exceeded major threshold. Limit: 85.0%, Actual: 89.57%	Major	...	58 mins 4 secs	[X] [Del] [Go]
dem7	Device	Backup: File system usage exceeded major threshold. Limit: 85.0%, Actual: 89.00%	Major	...	58 mins 4 secs	[X] [Del] [Go]
dem7	Device	Swap Memory utilization has exceeded threshold. (80% currently (90%))	Major	...	50 mins 4 secs	[X] [Del] [Go]
dem7_db	Device	Backup: File system usage exceeded major threshold. Limit: 85.0%, Actual: 88.00%	Major	...	50 mins 4 secs	[X] [Del] [Go]
dem7	Device	Swap Memory has exceeded threshold. (80% currently (100%))	Major	...	1 hr 25 mins	[X] [Del] [Go]
dem7	Device	BIU: File system usage exceeded major threshold. Limit: 85.0%, Actual: 89.88%	Major	...	50 mins 4 secs	[X] [Del] [Go]
dem7	Device	File Status Critical	Major	...	1 hr 59 mins	[X] [Del] [Go]
dem7	Device	File system usage exceeded major threshold. Limit: 85.0%, Actual: 90.86%	Major	...	58 mins 4 secs	[X] [Del] [Go]
System	Organization	Round alert rate critical 10890 (Internal messages in 5 minutes)	Major	...	1 hr 9 mins	[X] [Del] [Go]
10.20.30.178	Device	Printer Bypass paper tray empty: Bypass	Minor	...	1 hr 30 mins	[X] [Del] [Go]
10.20.30.181	Device	Printer Tray 8 paper tray empty: Tray 8	Minor	...	1 hr 26 mins	[X] [Del] [Go]
10.4.1.11	Device	System or agent has recently restarted.	Minor	...	1 hr 23 mins	[X] [Del] [Go]
10.4.1.77	Device	Interface state changed to operationally down. 70: Name: S1, previous state was unknown (4)	Minor	...	9 mins 59 secs	[X] [Del] [Go]
10.4.1.77	Device	Interface state changed to operationally down. 1: Name: sc0, previous state was unknown (4)	Minor	...	37 mins 50 secs	[X] [Del] [Go]
10100	Device	Printer Bypass Tray paper tray empty: Bypass Tray	Minor	...	1 hr 20 mins	[X] [Del] [Go]
10.8610.1080.com	Device	System or agent has recently restarted.	Minor	...	1 hr 18 mins	[X] [Del] [Go]
DELL2A72DA	Device	Physical Memory has exceeded threshold. (80% currently (100%))	Minor	...	1 hr 24 mins	[X] [Del] [Go]
dem7	Device	Physical Memory has exceeded threshold. (80% currently (80%))	Minor	...	1 hr 7 mins	[X] [Del] [Go]
dem7_db	Device	Physical Memory has exceeded threshold. (80% currently (92%))	Minor	...	1 hr 48 mins	[X] [Del] [Go]
dem7_db	Device	Physical Memory has exceeded threshold. (80% currently (89%))	Minor	...	1 hr 58 mins	[X] [Del] [Go]
dem7_db	Device	Physical Memory has exceeded threshold. (80% currently (96%))	Minor	...	1 hr 34 mins	[X] [Del] [Go]
event4	Device	Physical Memory has exceeded threshold. (80% currently (99%))	Minor	...	50 mins 48 secs	[X] [Del] [Go]
hp1.dmc.asi.com	Device	Physical Memory has exceeded threshold. (80% currently (99%))	Minor	...	58 mins 7 secs	[X] [Del] [Go]
LAB-CENTER.ScienceLogic.local	Device	Physical Memory has exceeded threshold. (80% currently (97%))	Minor	...	1 hr 49 mins	[X] [Del] [Go]
PCDM1	Device	Physical Memory has exceeded threshold. (80% currently (97%))	Minor	...	1 hr 10 mins	[X] [Del] [Go]
ROS-DEN-POPprodsvlab.com	Device	Cisco Camer Routing System SPA Interface Processor Card has exceeded threshold. (80% currently (2534%))	Minor	...	1 hr 31 mins	[X] [Del] [Go]
server-651	Device	Printer MP Tray paper tray empty: MP Tray	Minor	...	1 hr 29 mins	[X] [Del] [Go]
SAPSRV2146	Device	Physical Memory has exceeded threshold. (80% currently (96%))	Minor	...	1 hr 20 mins	[X] [Del] [Go]
TOSHBA-STUD0451c	Device	Printer Cassette1 paper tray empty: Cassette1	Minor	...	1 hr 20 mins	[X] [Del] [Go]
TrnComm	Device	Physical Memory has exceeded threshold. (80% currently (100%))	Minor	...	1 hr 27 mins	[X] [Del] [Go]
TULLFTS-ACCOUNTING	Device	Printer Magenta Cartridge toner low, current level: 0% full	Minor	...	1 hr 27 mins	[X] [Del] [Go]
WINRMA2609PO.ScienceLogic	Device	Physical Memory has exceeded threshold. (80% currently (96%))	Minor	...	1 hr 44 mins	[X] [Del] [Go]
balbany-01	Device	Interface state changed to admin up-2. Name: ethernet0/1, previous state was down (2)	Notice	...	8 mins 24 secs	[X] [Del] [Go]
balbany-01	Device	Interface state changed to admin up-1. Name: ethernet0/0, previous state was down (2)	Notice	...	22 mins 49 secs	[X] [Del] [Go]
CHPLCSERV01	Device	Network Latency below threshold	Healthy	...	11 mins	[X] [Del] [Go]
dem7_cu	Device	Network Latency below threshold	Healthy	...	6 mins 15 secs	[X] [Del] [Go]
dem7_cu	Device	Network Latency below threshold	Healthy	...	11 mins 15 secs	[X] [Del] [Go]
unintended	Device	Temperature normal, now: 70	1 hr 16 mins	[X] [Del] [Go]

3. Clear the event(s) by doing one of the following:
 - Click the **[Del]** button.
 - In the **Select Action** drop-down list, select **Clear**, then click the **[Go]** button.
4. When you successfully clear an event, it will no longer appear in the **Event Console** page.

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

Suppressing an Event on a Single Device

When you suppress an event in the classic SL1 user interface, you are specifying that in the future, if this event occurs again on the same device, the event will not appear in the **Event Console** page or the **Viewing Events** page for a device.

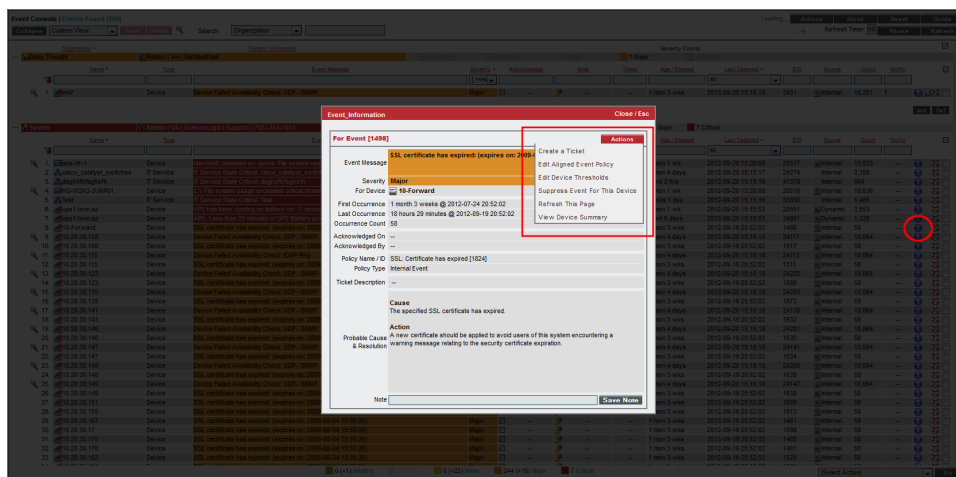
If a suppressed event occurs on a different device, it will appear in the **Event Console** page and on the **Viewing Events** page for that different device.

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

NOTE: To suppress an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Events/Event:View and Event:Clear. Accounts of type "user" will then be able to view and suppress events that belong to the same organization(s) as the user. For more information on access hooks, see the manuals [Access Permissions](#) and [Organizations and Users](#).

To suppress an event in the classic SL1 user interface:

1. Go to the **[Events]** tab.
2. In the **Event Console**, click the information icon (i) for the event you want to suppress.
3. In the **Event Information** page, click the **[Actions]** menu and select *Suppress Event for this Device*.




4. In the future, if this event occurs again on the same device, the event will not appear in the **Event Console** page.

NOTE: Users of type "user" can view only suppressed events that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all suppressed events.

Suppressing an Event On Multiple Devices

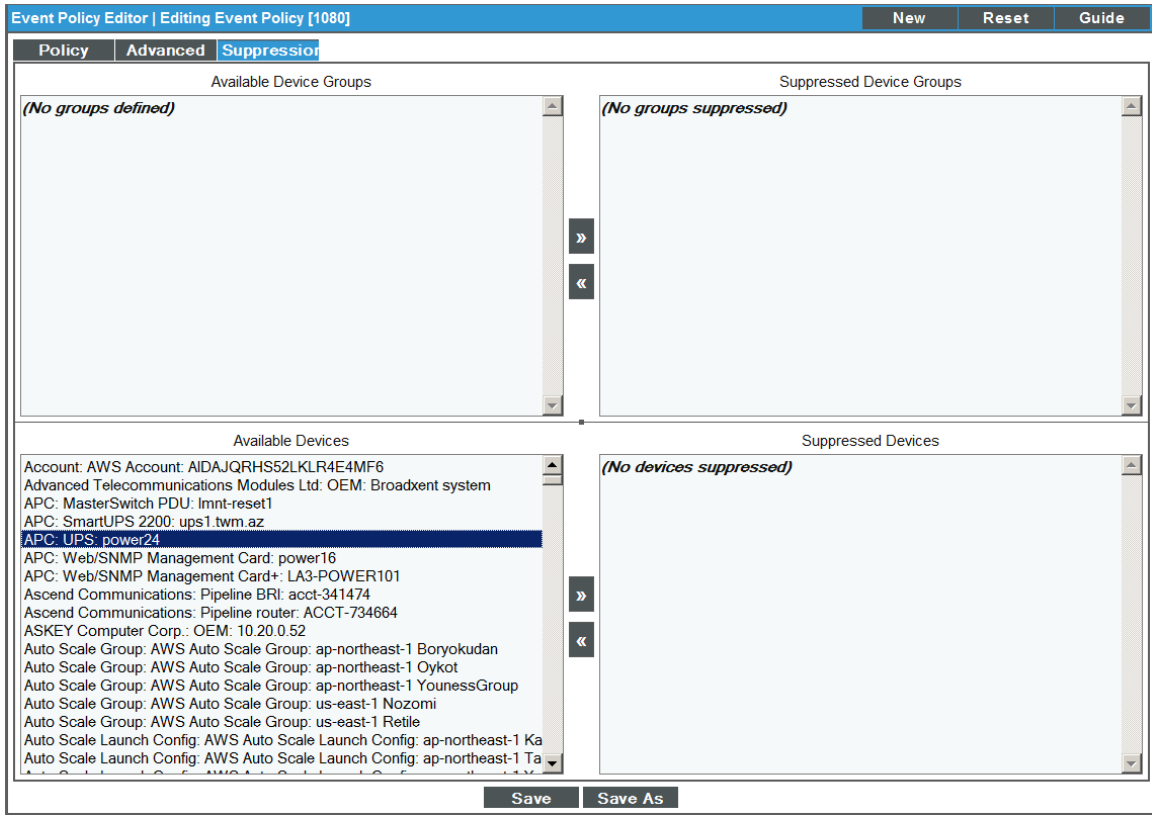
When you suppress an event on multiple devices, you are specifying that, in the future, if this event occurs again on any of those devices, the event will not appear in the **Event Console** page or in the **Viewing Events** page for any of those devices.

To suppress an event on multiple devices in the classic SL1 user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, select the page icon () of the event you want to suppress.

Event Policy Manager Policies Found [20]														Create	Reset	Guide
Event Policy Name	Type	State	P-Pack	Severity	Weight	ID	Expiry	Time	Thresh	Edited By	Last Edited	External ID	Category			
EM7											All					
1. Config: EM7 failed to initiate remote program execution	Internal	Enabled	Yes	Notice	0	1081	30 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
2. Config: EM7 initiated remote program execution on device	Internal	Enabled	Yes	Notice	0	1080	30 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
3. Config: EM7 reboot failed	Internal	Enabled	Yes	Minor	0	1075	60 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
4. Config: EM7 rebooting device	Internal	Enabled	Yes	Notice	0	1074	30 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
5. Config: EM7 service start request failed	Internal	Enabled	Yes	Minor	0	1079	60 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
6. Config: EM7 service stop request failed	Internal	Enabled	Yes	Minor	0	1078	60 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
7. Config: EM7 shutdown of device failed	Internal	Enabled	Yes	Minor	0	1077	60 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
8. Config: EM7 shutting down device	Internal	Enabled	Yes	Notice	0	1076	30 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
9. Config: Service started by EM7	Internal	Enabled	Yes	Notice	0	1072	30 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
10. Config: Service stopped by EM7	Internal	Enabled	Yes	Notice	0	1073	30 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
11. EM7: DRBD Diskless	Dynamic	Enabled	Yes	Critical	0	1015	0 Min.	0 Min.	0	em7/admin	2014-07-21 16:36:10	--	--			
12. EM7: DRBD DUnknown	Dynamic	Enabled	Yes	Major	0	1016	90 Min.	0 Min.	0	em7/admin	2014-07-21 16:36:10	--	--			
13. EM7: DRBD Inconsistent	Dynamic	Enabled	Yes	Minor	0	1017	60 Min.	0 Min.	0	em7/admin	2014-07-21 16:36:10	--	--			
14. EM7: DRBD Outdated	Dynamic	Enabled	Yes	Notice	0	1018	30 Min.	0 Min.	0	em7/admin	2014-07-21 16:36:10	--	--			
15. EM7: DRBD Up to Date	Dynamic	Enabled	Yes	Healthy	0	1019	15 Min.	0 Min.	0	em7/admin	2014-07-21 16:36:11	--	--			
16. Patcher: patch file checksum invalid or not valid EM7 patch file	Internal	Enabled	Yes	Minor	0	1135	60 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:24	--	--			
17. System: EM7 event	Internal	Enabled	Yes	Critical	0	1047	120 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
18. System: EM7 event	Internal	Enabled	Yes	Major	0	1106	90 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
19. System: EM7 event	Internal	Enabled	Yes	Minor	0	1107	60 Min.	0 Min.	0	em7/admin	2015-03-16 13:03:23	--	--			
20. VMware: vSphere Powerpack - Unable to access EM7 cache	API	Enabled	Yes	Minor	0	2520	60 Min.	0 Min.	0	em7/admin	2015-03-10 19:24:31	--	--			

3. The **Event Policy Editor** page appears, with the **Suppressions** tab selected.



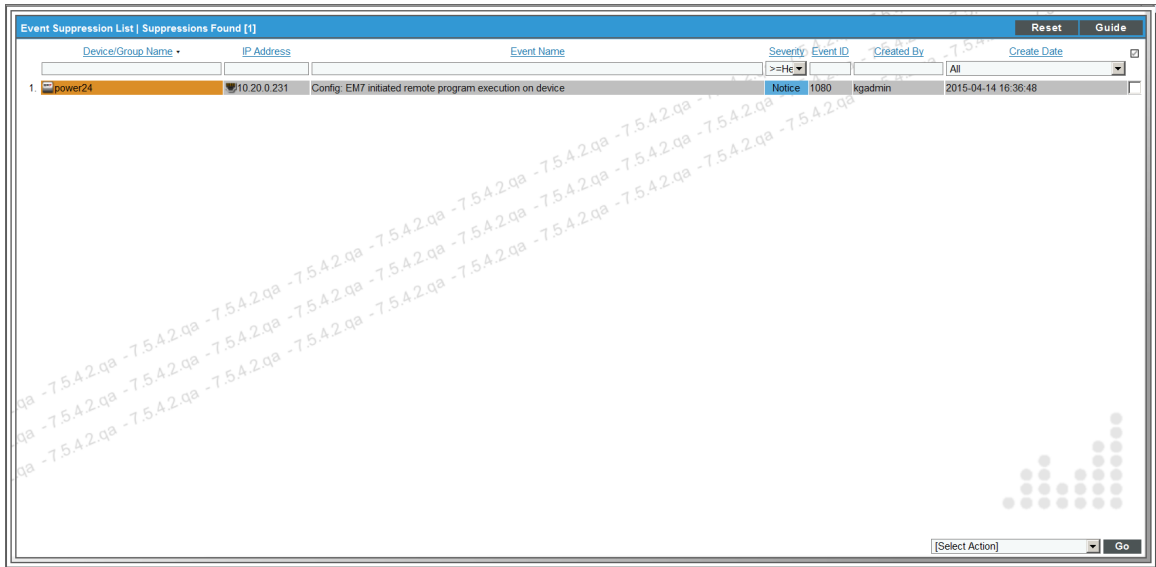
4. In the **Suppressions** tab, you can select the devices or device groups on which to suppress the event. To do so:

- Select one or more device groups in the **Available Device Groups** field and then click the right arrow button ([>>]) so those groups appear in the **Suppressed Device Groups** field.
- Select one or more devices in the **Available Devices** field and then click the right arrow button ([>>]) so those devices appear in the **Suppressed Devices** field.

5. Click **[Save]**.

In the future, if the event occurs on one of the selected devices, the event will not appear in the **Event Console** page or in the **Viewing Events** page for the device.

The suppressed event will appear in the **Event Suppression List** page (Registry > Events > Suppressions).



Device/Group Name	IP Address	Event Name	Severity	Event ID	Created By	Create Date
power24	10.20.0.231	Config: EM7 initiated remote program execution on device	Notice	1080	kgadmin	2015-04-14 16:36:48

Unsuppressing an Event

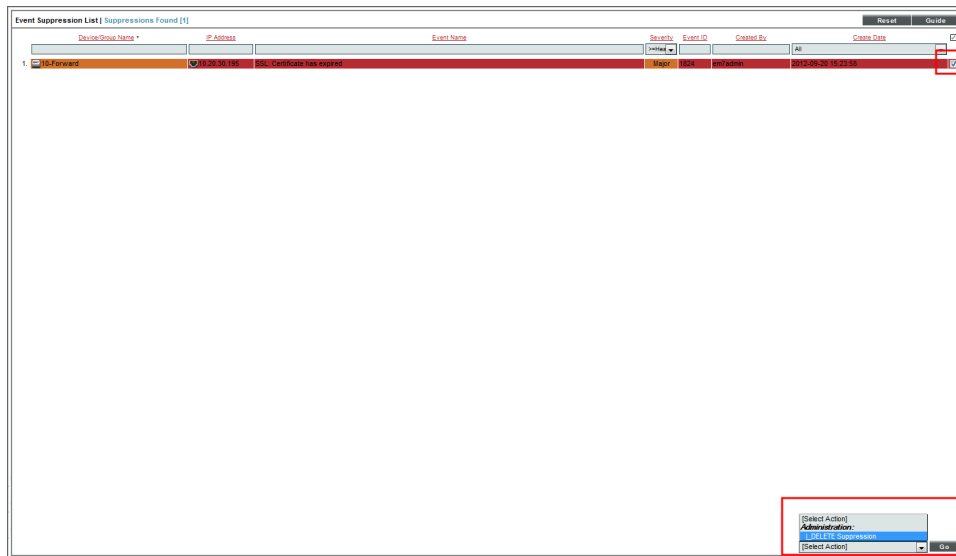
You can view a list of all suppressed events in SL1 and choose to unsuppress one or more of those events. When you unsuppress an event, if this event occurs again on the same device, the event will appear in the **Events** page (or the **Event Console** page in the classic SL1 user interface) .

NOTE: To unsuppress an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Suppressions, and Event:Suppressions. Accounts of type "user" will then be able to view a list of suppressed events that belong to the same organization as the user. Accounts of type "user" will also be able to unsuppress one or more of these suppressed events. For more information on access hooks, see the manuals **Access Permissions** and **Organizations and Users**.

To unsuppress an event:

1. Go to the **Event Suppression List** page (Registry > Events > Suppressions).

2. In the **Event Suppression List** page, select the checkbox for each event you want to unsuppress.



3. In the **Select Action** drop-down menu, in the lower right, select *DELETE Suppression*.
4. Click the **[Go]** button.
5. In the future, if the unsuppressed event occurs again on the same device, the event will appear in the **Events** page (or the **Event Console** page in the classic SL1 user interface) .

Unsuppressing All Instances of an Event

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

NOTE: To unsuppress an event on all devices, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Accounts of type "user" will then be able to access the **Event Policy Manager** page and unsuppress one or more events on all devices. For more information on access hooks, see the manuals *Access Permissions* and *Organizations and Users*.

To unsuppress an event on all devices in the classic SL1 user interface:

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

- In the **Event Policy Manager** page , select the checkbox for the event you want to unsuppress on all devices.

Event Policy Name	Date	State	Event	Severity	Alert	UI	Enable	Time	Threat	Schedule	Last State	Subscribed	Subscribed	Go
1. ADIC: Global Status Failed		Dynamic	Enabled	No	Major	0	900	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:14:30	--	--
2. ADIC: Global Status OK		Dynamic	Enabled	No	Healthy	0	902	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:14:31	--	--
3. ADIC: Tape Library Degraded		Dynamic	Enabled	No	Critical	0	898	60 Min.	0 Min.	0	em7Admin	2012-07-07 00:14:30	--	--
4. ADIC: Tape Library Degraded		Dynamic	Enabled	No	Minor	0	899	60 Min.	0 Min.	0	em7Admin	2012-07-07 00:14:30	--	--
5. AKCP: AC Voltage sensor detects no current		System	Enabled	Yes	Critical	0	1517	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
6. AKCP: AC Voltage sensor now reporting Normal Status		System	Enabled	Yes	Healthy	0	1523	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
7. AKCP: DC Voltage High Warning		System	Enabled	Yes	Major	0	1528	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
8. AKCP: DC Voltage sensor High Critical		System	Enabled	Yes	Critical	0	1528	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
9. AKCP: DC Voltage sensor Low Critical		System	Enabled	Yes	Critical	0	1527	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
10. AKCP: DC Voltage sensor Low Warning		System	Enabled	Yes	Major	0	1529	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
11. AKCP: DC Voltage sensor returned to Normal Status		System	Enabled	Yes	Healthy	0	1530	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
12. AKCP: Dry Contact Sensor Low Critical		System	Enabled	Yes	Critical	0	1516	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
13. AKCP: Dry Contact Sensor now Normal		System	Enabled	Yes	Healthy	2	1521	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
14. AKCP: Humidity High Warning		System	Enabled	Yes	Major	0	1524	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
15. AKCP: Humidity Low Warning		System	Enabled	Yes	Major	0	1525	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
16. AKCP: Smoke Detector Alert		System	Enabled	Yes	Critical	10	1522	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
17. AKCP: Smoke Detector now Normal Status		System	Enabled	Yes	Healthy	0	1518	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
18. AKCP: Water Sensor has detected water		System	Enabled	Yes	Critical	0	1520	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
19. AKCP: Water sensor now Normal		System	Enabled	Yes	Healthy	0	1519	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:00	--	--
20. ABeon: New Fan Created		Dynamic	Enabled	No	Healthy	0	1408	30 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:01	--	--
21. ABeon: Primary Power Supply Failure		Dynamic	Enabled	No	Major	0	1408	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:01	--	--
22. ABeon: Primary Power Supply Healthy		Dynamic	Enabled	No	Healthy	0	1409	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:01	--	--
23. ABeon: Redundant Power Supply Failure		Dynamic	Enabled	No	Major	0	1407	90 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:01	--	--
24. ABeon: Redundant Power Supply Healthy		Dynamic	Enabled	No	Healthy	0	1410	15 Min.	0 Min.	0	em7Admin	2012-07-07 00:15:01	--	--
25. ABeon: Batteries Do Not Need Replacement		Dynamic	Enabled	No	Healthy	0	946	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
26. ABeon: Battery Charge Normal		Dynamic	Enabled	No	Healthy	0	945	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
27. ABeon: Battery Run Time Remaining No Longer Critical		Dynamic	Enabled	No	Healthy	0	942	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
28. ABeon: Battery Status		Dynamic	Enabled	No	Major	0	941	90 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
29. ABeon: Calibration Test Completed		Dynamic	Enabled	No	Healthy	0	954	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
30. ABeon: Calibration Test Did Not Complete		Dynamic	Enabled	No	Minor	0	960	60 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:12	--	--
31. ABeon: Calibration Test Failed		Dynamic	Enabled	No	Minor	0	956	90 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
32. ABeon: Communication Status Okay		Dynamic	Enabled	No	Healthy	0	949	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
33. ABeon: Communication Status Stopped		Dynamic	Enabled	No	Major	0	951	90 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
34. ABeon: Diagnostic Test Failed		Dynamic	Enabled	No	Critical	0	957	90 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
35. ABeon: Diagnostic Test In Progress		Dynamic	Enabled	No	Notice	0	958	30 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:12	--	--
36. ABeon: Diagnostic Test Passed		Dynamic	Enabled	No	Healthy	0	953	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
37. ABeon: Diagnostic Test Stopped		Dynamic	Enabled	No	Minor	0	958	0 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:12	--	--
38. ABeon: Diagnostics Schedule Not Set		Dynamic	Enabled	No	Major	0	952	90 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
39. ABeon: Diagnostics Schedule Set		Dynamic	Enabled	No	Healthy	0	955	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
40. ABeon: Percent Battery Remaining No Longer Critical		Dynamic	Enabled	No	Healthy	0	944	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
41. ABeon: Temperature has exceeded threshold		Dynamic	Enabled	No	Minor	0	962	60 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
42. ABeon: Temperature has returned to normal		Dynamic	Enabled	No	Healthy	0	961	15 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
43. ABeon: UPS Battery Cleared		Dynamic	Enabled	No	Critical	0	938	90 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--
44. ABeon: UPS has Defective Battery Packs		Dynamic	Enabled	No	Major	0	936	90 Min.	0 Min.	0	em7Admin	2012-09-06 18:46:11	--	--

- In the **Select Action** drop-down menu select **CLEAR the Suppression List**.

- Click the **[Go]** button.

In the future, if the unsuppressed event occurs again on any device, it will appear in the **Event Console** page or in the **Viewing Events** page for the device.

Disabling an Event

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

NOTE: To disable an event on all devices, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry> Events>Event Manager, and Event:Add/Rem. Accounts of type "user" will then be able to access the **Event Policy Manager** page and disable one or more events on all devices. For more information on access hooks, see the manuals **Access Permissions** and **Organizations and Users**.

To disable one or more events in the classic SL1 user interface:

- Go to the **Event Policy Manager** page (Registry > Events > Event Manager).

2. In the **Event Policy Manager** page , select the checkbox for each event you want to disable.

Event Policy Name	Type	State	Enabled	Severity	Vendor	ID	Extra	Time	Thresh	Edited By	Last Edited	External ID	Category
1. Global Status Failed	Dynamic	Enabled	No	Major	0	900	90 Min.	0 Min.	0	em7admin	2012-07-27 00:14:30	--	--
2. Global Status OK	Dynamic	Enabled	No	Healthy	0	902	15 Min.	0 Min.	0	em7admin	2012-07-27 00:14:31	--	--
3. Web Services Status	Dynamic	Enabled	No	Warning	0	903	90 Min.	0 Min.	0	em7admin	2012-07-27 00:14:30	--	--
4. Web Services Library Occupied	Dynamic	Enabled	No	Minor	0	908	90 Min.	0 Min.	0	em7admin	2012-07-27 00:14:30	--	--
5. AACP: AC Voltage sensor detects no current	Syslog	Enabled	Yes	Critical	0	1517	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
6. AACP: AC Voltage sensor now reporting Normal Status	Syslog	Enabled	Yes	Healthy	0	1522	15 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
7. AACP: DC Voltage High Warning	Syslog	Enabled	Yes	Major	0	1528	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
8. AACP: DC Voltage sensor High Critical	Syslog	Enabled	Yes	Critical	0	1528	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
9. AACP: DC Voltage sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1527	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
10. AACP: DC Voltage sensor Low Warning	Syslog	Enabled	Yes	Major	0	1529	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
11. AACP: DC Voltage sensor returned to Normal Status	Syslog	Enabled	Yes	Healthy	0	1530	15 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
12. AACP: Dry Contact Sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1516	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
13. AACP: Dry Contact sensor now Normal	Syslog	Enabled	Yes	Healthy	2	1521	15 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
14. AACP: Humidity High Warning	Syslog	Enabled	Yes	Major	0	1524	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
15. AACP: Humidity Low Warning	Syslog	Enabled	Yes	Major	0	1525	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
16. AACP: Smoke Detector Alert	Syslog	Enabled	Yes	Critical	10	1522	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
17. AACP: Smoke detector now Normal Status	Syslog	Enabled	Yes	Healthy	4	1518	15 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
18. AACP: Water Sensor has detected water	Syslog	Enabled	Yes	Critical	0	1520	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
19. AACP: Water sensor now Normal	Syslog	Enabled	Yes	Healthy	0	1519	15 Min.	0 Min.	0	em7admin	2012-07-27 00:15:08	--	--
20. ABBon: New Trip Cleared	Dynamic	Enabled	No	Critical	0	1408	30 Min.	0 Min.	0	em7admin	2012-07-27 00:15:01	--	--
21. ABBon: Primary Power Supply Failure	Dynamic	Enabled	No	Major	0	1406	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:01	--	--
22. ABBon: Primary Power Supply Healthy	Dynamic	Enabled	No	Healthy	0	1409	15 Min.	0 Min.	0	em7admin	2012-07-27 00:15:01	--	--
23. ABBon: Redundant Power Supply Failure	Dynamic	Enabled	No	Major	0	1407	90 Min.	0 Min.	0	em7admin	2012-07-27 00:15:01	--	--
24. ABBon: Redundant Power Supply Healthy	Dynamic	Enabled	No	Healthy	0	1410	15 Min.	0 Min.	0	em7admin	2012-07-27 00:15:01	--	--
25. ABBon: Batteries Do Not Need Replacement	Dynamic	Enabled	No	Healthy	0	946	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
26. ABBon: Battery Charge Normal	Dynamic	Enabled	No	Healthy	0	945	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
27. ABBon: Battery Run Time Remaining No Longer Critical	Dynamic	Enabled	No	Healthy	0	942	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
28. ABBon: Battery Status	Dynamic	Enabled	No	Major	0	941	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
29. ABBon: Calibration Test Completed	Dynamic	Enabled	No	Healthy	0	964	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
30. ABBon: Calibration Test Did Not Complete	Dynamic	Enabled	No	Minor	0	960	60 Min.	0 Min.	0	em7admin	2012-09-26 18:48:12	--	--
31. ABBon: Calibration Test Failed	Dynamic	Enabled	No	Major	0	966	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
32. ABBon: Communication Status Okay	Dynamic	Enabled	No	Healthy	0	949	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
33. ABBon: Communication Status Stopped	Dynamic	Enabled	No	Major	0	951	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
34. ABBon: Diagnostic Test Failed	Dynamic	Enabled	No	Critical	0	957	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:12	--	--
35. ABBon: Diagnostic Test In Progress	Dynamic	Enabled	No	Warning	0	958	30 Min.	0 Min.	0	em7admin	2012-09-26 18:48:12	--	--
36. ABBon: Diagnostic Test Passed	Dynamic	Enabled	No	Healthy	0	953	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
37. ABBon: Diagnostic Test Skipped	Dynamic	Enabled	No	Major	0	959	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:12	--	--
38. ABBon: Diagnostics Schedule Not Set	Dynamic	Enabled	No	Major	0	952	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:12	--	--
39. ABBon: Diagnostics Schedule Set	Dynamic	Enabled	No	Healthy	0	955	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
40. ABBon: Percent Battery Remaining No Longer Critical	Dynamic	Enabled	No	Healthy	0	944	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
41. ABBon: Temperature has exceeded threshold	Dynamic	Enabled	No	Minor	0	962	60 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
42. ABBon: Temperature has returned to normal	Dynamic	Enabled	No	Healthy	0	961	15 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
43. ABBon: UPS Battery Capacity	Dynamic	Enabled	No	Critical	0	939	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--
44. ABBon: UPS has Detective Battery Packs	Dynamic	Enabled	No	Major	0	936	90 Min.	0 Min.	0	em7admin	2012-09-26 18:48:11	--	--

3. In the **Select Actions** drop-down list, select **DISABLE these Event Policies**.

4. Click the **[Go]** button.

The selected event(s) will no longer appear in SL1 for any device, application, or policy.

Enabling an Event

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

NOTE: To enable an event on all devices, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Accounts of type "user" will then be able to access the **Event Policy Manager** page and enable one or more events on all devices. For more information on access hooks, see the manuals **Access Permissions** and **Organizations and Users**.

To enable one or more events in the classic SL1 user interface:

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

- In the **Event Policy Manager** page , select the checkbox for each event you want to enable.

Event Policy Manager Policies Found [3496]													Create	Reset	Guide
Event Policy Name	Type	State	P-Pack	Severity	Weight	ID	Expiry	Time	Thresh	Edited By	Last Edited	External ID	Category	<input type="checkbox"/>	
1. ADIC Global Status Failed	Dynamic	Enabled	Yes	Major	0	2	90 Min	0 Min	0	em7admn	2014-06-04 14:33:31	--	--	<input checked="" type="checkbox"/>	
2. ADIC Global Status OK	Dynamic	Enabled	Yes	Healthy	0	4	15 Min	0 Min	0	em7admin	2014-06-04 14:33:31	--	--	<input type="checkbox"/>	
3. ADIC Global Status Unknown	Dynamic	Enabled	Yes	Notice	0	3	30 Min	0 Min	0	em7admin	2014-06-04 14:33:31	--	--	<input type="checkbox"/>	
4. ADIC Tape Library Degraded	Dynamic	Enabled	Yes	Minor	0	1	60 Min	0 Min	0	em7admin	2014-06-04 14:33:31	--	--	<input type="checkbox"/>	
5. AKCP: AC Voltage sensor detects no current	Syslog	Enabled	Yes	Critical	0	1222	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
6. AKCP: AC Voltage sensor now reporting Normal Status	Syslog	Enabled	Yes	Healthy	0	1228	15 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
7. AKCP: DC Voltage High Warning	Syslog	Enabled	Yes	Major	0	1233	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
8. AKCP: DC Voltage sensor High Critical	Syslog	Enabled	Yes	Critical	0	1231	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
9. AKCP: DC Voltage sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1232	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
10. AKCP: DC Voltage sensor Low Warning	Syslog	Enabled	Yes	Major	0	1234	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
11. AKCP: DC Voltage sensor returned to Normal Status	Syslog	Enabled	Yes	Healthy	0	1235	15 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
12. AKCP: Dry Contact Sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1221	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
13. AKCP: Dry Contact sensor now Normal	Syslog	Enabled	Yes	Healthy	2	1226	15 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
14. AKCP: Humidity High Warning	Syslog	Enabled	Yes	Major	0	1229	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
15. AKCP: Humidity Low Warning	Syslog	Enabled	Yes	Major	0	1230	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
16. AKCP: Smoke Detector Alert!	Syslog	Enabled	Yes	Critical	10	1227	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
17. AKCP: Smoke detector now Normal Status	Syslog	Enabled	Yes	Healthy	4	1223	15 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
18. AKCP: Water Sensor has detected water	Syslog	Enabled	Yes	Critical	0	1225	90 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
19. AKCP: Water sensor now Normal	Syslog	Enabled	Yes	Healthy	0	1224	15 Min	0 Min	0	em7admin	2014-06-04 14:35:03	--	--	<input type="checkbox"/>	
20. Ateon: New Flash Enabled	Dynamic	Enabled	Yes	Notice	0	36	30 Min	0 Min	0	em7admin	2014-06-04 14:33:33	--	--	<input type="checkbox"/>	
21. Ateon: Primary Power Supply Failure	Dynamic	Enabled	Yes	Major	0	32	90 Min	0 Min	0	em7admin	2014-06-04 14:33:33	--	--	<input type="checkbox"/>	
22. Ateon: Primary Power Supply Healthy	Dynamic	Enabled	Yes	Healthy	0	33	15 Min	0 Min	0	em7admin	2014-06-04 14:33:33	--	--	<input type="checkbox"/>	
23. Ateon: Redundant Power Supply Failure	Dynamic	Enabled	Yes	Major	0	34	90 Min	0 Min	0	em7admin	2014-06-04 14:33:33	--	--	<input type="checkbox"/>	
24. Ateon: Redundant Power Supply Healthy	Dynamic	Enabled	Yes	Healthy	0	35	15 Min	0 Min	0	em7admin	2014-06-04 14:33:33	--	--	<input type="checkbox"/>	
25. APC: Batteries Do Not Need Replacement	Dynamic	Enabled	Yes	Healthy	0	8	15 Min	0 Min	0	em7admin	2014-06-04 14:33:32	--	--	<input type="checkbox"/>	

[Select Action]

Administration

DELETE these Event Policies

ENABLE these Event Policies

DISABLE these Event Policies

CLEAR the Suppression List

[Select Action]

Viewing Page: 1

- In the **Select Actions** drop-down list, select *ENABLE these Event Policies*.
- Click the **[Go]** button. The selected event(s) will once again appear in SL1.

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 the menu options, click the Advanced menu icon ().

This chapter includes the following topics:


<i>Creating a Ticket from the List of Events</i>	79
<i>Event Ticket Behavior Settings</i>	82
<i>Integrating Events with External Tickets</i>	83
<i>External Tickets in the Events Page or Event Console</i>	83
<i>Using Run Book Automation to Populate the ScienceLogic Database with Values from External Tickets</i>	84
<i>Aligning an External Ticket with Multiple Events</i>	84
<i>Aligning an External Ticket with Multiple Events in the Classic User Interface</i>	85


Creating a Ticket from the List of Events

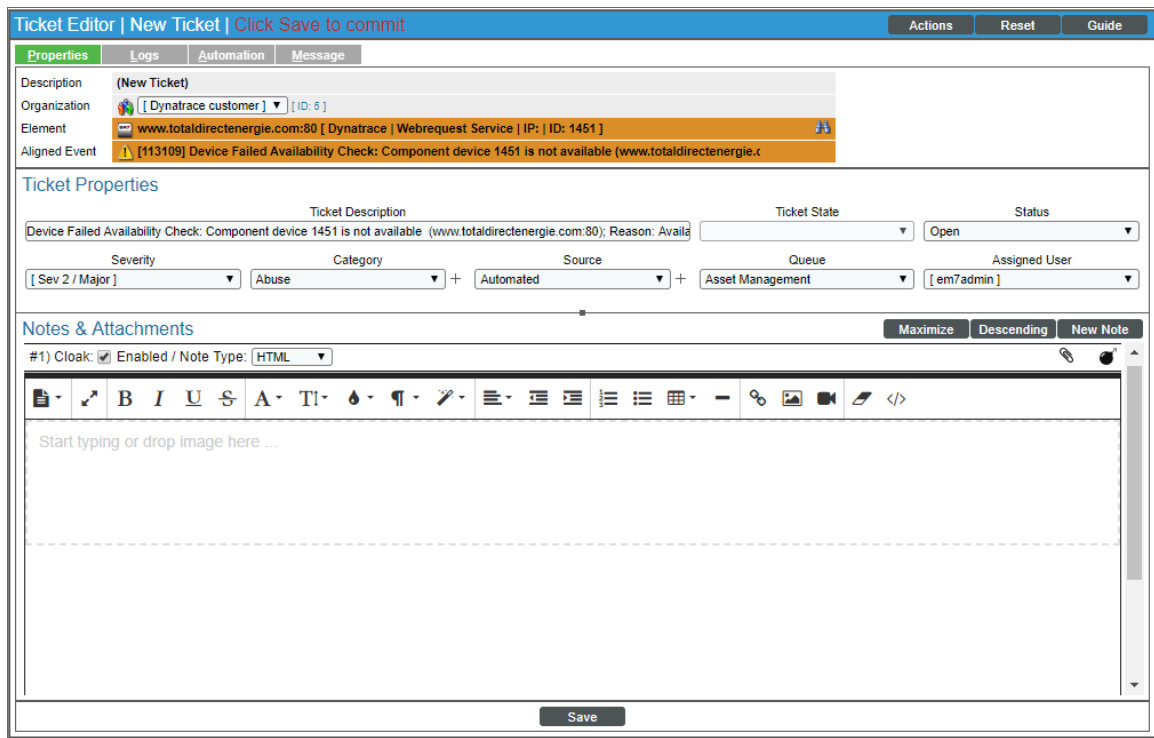
A **ticket** is a request for work that can be tracked in SL1. This request can be in response to a problem that needs to be fixed, for routine maintenance, or for any type of work required by your enterprise. A ticket can be created manually or created based on an event. For example, if an event occurs 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 (or the **Event Console** page in the classic SL1 user interface), 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 (or the **Event Console** page in the classic SL1 user interface). For more information on Access Keys, see the manual **Access Permissions**.

NOTE: Depending on the **Event Console Ticket Life Ring Button Behavior** setting in the **Behavior Settings** page (System > Settings > Behavior), clicking the life ring icon () in the **Event Console** will either create a ScienceLogic ticket or an external ticket. When viewing an event in the **Events** page (or the **Event Console** page in the classic SL1 user interface), you can create a ticket based on the selected event. Some of the ticket fields will be populated automatically with values from the event. To create a ticket based on an event:

1. On the **Events** page or the **Event Investigator** page for a specific event, click the **[Actions]** button (⋮) for the event and select *Create Ticket*. (Or, if you are using the classic SL1 user interface, on the **Event Console** page, click on the life ring icon () of the event for which you want to create a ticket.) The **Ticket Editor** page appears:




- 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.
- 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 (or the **Event Console** page in the classic SL1 user interface), 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 (or the **Event Console** page in the classic SL1 user interface), 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 (or the **Event Console** page in the classic SL1 user interface), 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 (or the life-ring icon ) in the **Event Console** in the classic SL1 user interface) is determined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface. To change this behavior:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Select from the following options in the **Event Console Ticket Life Ring Button Behavior** field:
 - *Create/View EM7 Ticket.* When you select the *Create Ticket* option or click the life-ring icon  for an event, 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 or click the life-ring icon  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 or click the life-ring icon  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](#).


Integrating Events with External Tickets

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

- If an external ticket is aligned with an event, then when you select the *Create Ticket* option (or click the life-ring icon ) for that event, SL1 spawns a new window and displays the external ticket.
- If an external ticket is not yet aligned with an event, when you select the *Create Ticket* option (or click the life-ring icon ) for that event, 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.

External Tickets in the Events Page or Event Console

The following two fields in the *master_events.events_active* database table in SL1 populate the values for external tickets in the **Events** page (or the **Event Console** page in the classic SL1 user interface):


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

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

For example, suppose the events in an off-site SL1 system are being integrated with the ScienceLogic Customer Care ticketing system, *em7.sciencelogic.com*. On the off-site system, for each event that has an open ticket, the **force_ticket_uri** and **ext_ticket_ref** values would be set to those of a ticket on the *em7.sciencelogic.com* system.

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

In the off-site SL1 system, we would define the following:

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

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


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

10000

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

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

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

- An automation policy that runs when events are created. Depending on your business needs, this automation policy might run when an event is acknowledged or when a user selects the *Create Ticket* option on the **Events** page (or the life-ring icon  in the **Event Console** in the classic SL1 user interface). This automation policy would execute the following actions:
 - One or more snippet actions that create a ticket in the external ticketing system. The ticket can be created using one or more of the available variables; for example, %M contains the message text for the event that triggered the automation policy. One of the snippet actions could pass the ticket ID for the ticket to SL1.
 - An SQL query action that updates the **ext_ticket_ref** and **force_ticket_uri** fields for the event. The value of **ext_ticket_ref** should be set to the value passed by the previous snippet action (accessed using the %_EM7_RESULT_% variable). The SQL query should use the %e variable (the event ID for the event that triggered the automation policy) to ensure that the query updates the correct event.
- An automation policy that runs when events are cleared. This automation policy would execute a snippet action that:
 - Performs an SQL query to retrieve the **ext_ticket_ref** value for the event that triggered the automation policy.
 - Resolves the appropriate ticket in the external ticketing system.

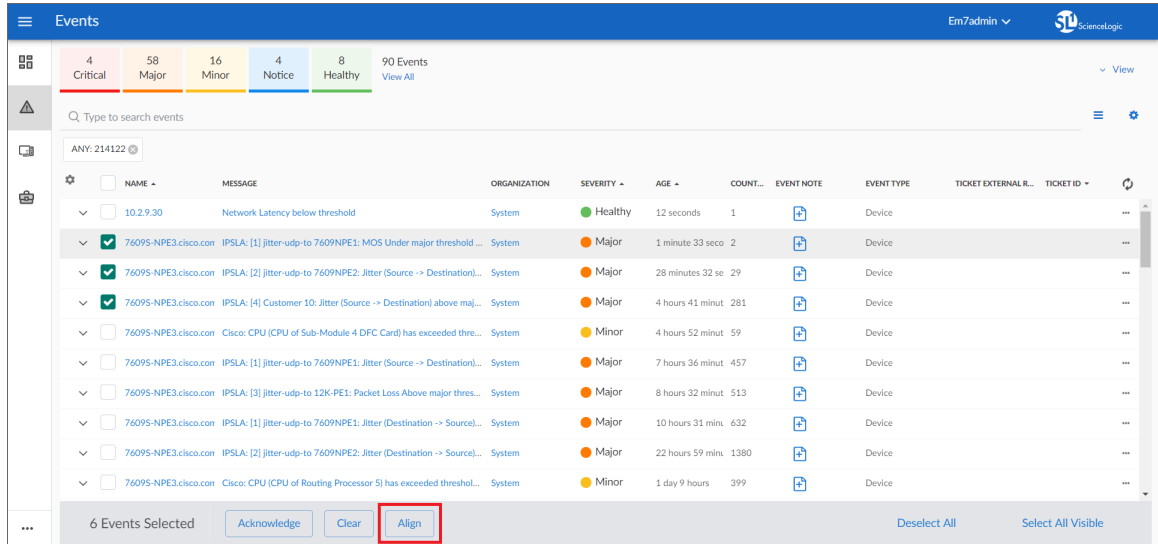
Aligning an External Ticket with Multiple Events

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

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

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

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



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

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

To copy the link to an external ticket to multiple, related events in the classic SL1 user interface:

1. In the **Event Console** page, select the checkbox for each event that you want to align with a single external ticket.
2. In the **Select Action** drop-down list, select *Set External Ticket* and then click the **[Go]** button.

Organization	Name	Type	Event/Message	Severity	Acknowledged	Time	External Ticket	Age_Closed	Last_Created	ECID	Source	Count	Tools
System	10.20.0.176	Device	Printer Tray2 paper tray empty: Tray2	Minor		2/27/2013 1:51:39 pm		1 mo 1 day	2012/2013 01/31/09 pm	8226484	Dynamic	1,395	386
System	10.20.0.176	Device	Printer Bypass tray empty: Bypass	Minor		2/27/2013 1:51:39 pm		1 mo 1 day	2012/2013 01/31/09 pm	8226484	Dynamic	1,396	386
System	10.20.0.198	Device	CPU has exceeded threshold: (80%) currently (103729221%)	Minor		2/27/2013 1:51:39 pm		1 mo 1 day	2012/2013 01/31/09 pm	8226484	Dynamic	1,396	378
System	10.20.0.191	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor		2/27/2013 1:51:39 pm		1 mo 1 day	2012/2013 01/31/09 pm	8226484	Dynamic	1,396	386
System	10.20.0.191	Device	Printer Tray B paper tray empty: Tray B	Minor		2/27/2013 1:51:39 pm		1 mo 1 day	2012/2013 01/31/09 pm	8226484	Dynamic	1,395	386
System	10.20.0.198	Device	Network latency exceeded threshold: No Response	Minor		2/27/2013 1:51:39 pm		1 mo 1 day	2012/2013 01/31/09 pm	8226484	Dynamic	1,395	386

3. The **Set External Ticket** modal appears. This page displays a list of external tickets that are currently aligned with active events. Select the external ticket that you want to align with the selected events. Click **[Save]**.

Set External Ticket
Close / Esc

Select An Aligned External Ticket:

None...

None...

https://workflow.sciencelogic.com/em7/index.em7?exec=ticket_editor&tid=15230

15230



4. The selected events now display the external ticket ID in the **External Ticket** column.

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 the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

Event Correlation	88
Defining Parent and Child Devices	89
<i>Device Categories that Don't Support Child Devices</i>	91
Defining Event Topology Masking and Suppression	91
<i>Defining Event Topology Suppression in the Classic SL1 User Interface</i>	92
Event Categories	95
<i>Assigning an Event Category to an Event</i>	96
<i>Assigning an Event Category to an Event in the Classic SL1 User Interface</i>	97
<i>Creating an Event Category</i>	98
<i>Editing an Event Category</i>	98
<i>Viewing the List of Event Categories</i>	99
<i>Deleting One or More Event Categories</i>	105

Event Correlation

In SL1, there are four types of events that might not appear on the **Events** page (or the **Event Console** page in the classic SL1 user interface):

- **Rolled-up events.** Multiple occurrences of the same event on the same device. When the same event occurs multiple times on a single device, SL1 does not display each occurrence on the **Events** page (or the **Event Console** page in the classic SL1 user interface). 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 (or the **Event Console** page in the classic SL1 user interface). For details on suppressing events for a single device, see the section on [Suppressing 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 (or the **Event Console** page in the classic SL1 user interface). 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 (or the **Event Console** page in the classic SL1 user interface). 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 (or the **Event Console** page in the classic SL1 user interface), masked events are displayed under a single event, the one with the highest severity. For details on events masks, see the section on [Event Masks](#).

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 (or the **Event Console** page in the classic SL1 user interface). For example, suppose a switch fails. Instead of seeing an event for the failed switch and seeing events about failed communication for each device connected to the switch, only a single event would appear on the **Events** page (or the **Event Console** page in the classic SL1 user interface). The single event would describe the switch failure. When you manually define a hierarchy between events, you can also include an event category. An event category allows 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

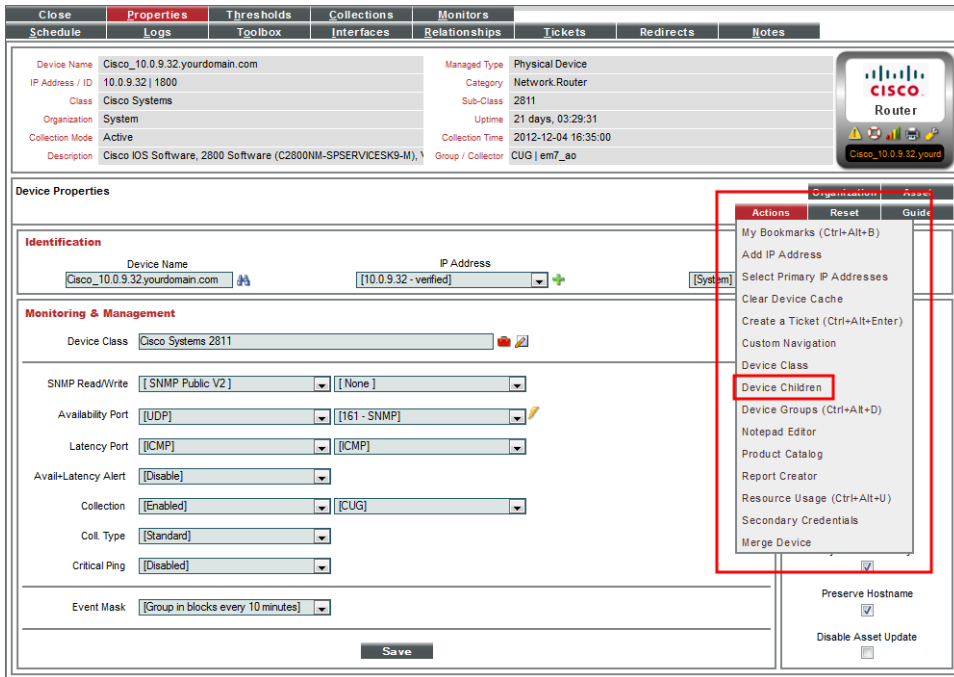
The **Device Children** modal page allows users to select one or more devices to become children of the currently selected device.

To add children to a device:

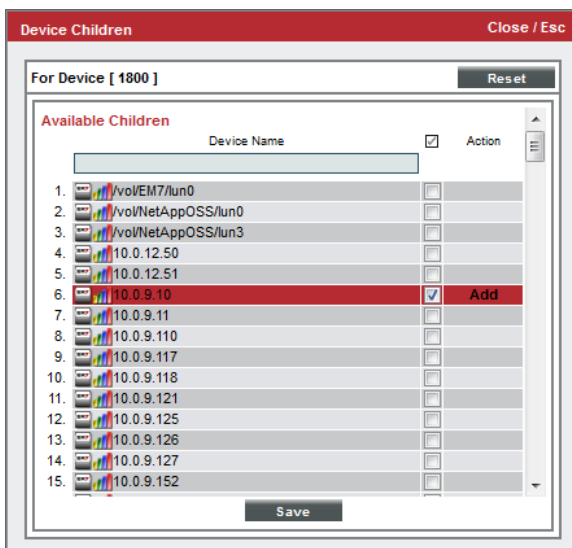
1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, select the wrench icon () for the device for which you want to add children devices.

- The **Device Properties** page appears:

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



- In the **Device Properties** page, in the **[Actions]** drop-down list, select *Device Children*.
- 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 Child 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 child devices:

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

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

Defining Event Topology Masking and Suppression

Topology masking, also referred to as **topology suppression**, is a setting that defines the rules that SL1 uses to determine **event correlation** and suppression 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 event policies must be defined: masking events and maskable events.

- **Masking events.** If this type of event occurs on a parent device, SL1 will search all related child devices for **maskable** events. On the child devices, all maskable events will be masked. Only the masking event will appear on the **Events** page; the maskable events will be nested under the parent event.
- **Maskable events.** This type of event is masked on a child device *only* when a masking event occurs on the parent device.

If you configure an event policy to be *both* masking and maskable, then if the event occurs on a parent device, it behaves as a masked event. If the event occurs on a child device, it behaves as a maskable event.

When a device uses the event masking setting, events that occur on a single device within a specified timespan are grouped together. On the **Events** page (or the **Event Console** page in the classic SL1 user interface), masked events are displayed under a single event, the one with the highest severity.

For more information about how to define an event as masking or maskable, see the section on [The Event Message Tab](#).


Defining Event Topology Suppression in the Classic SL1 User Interface

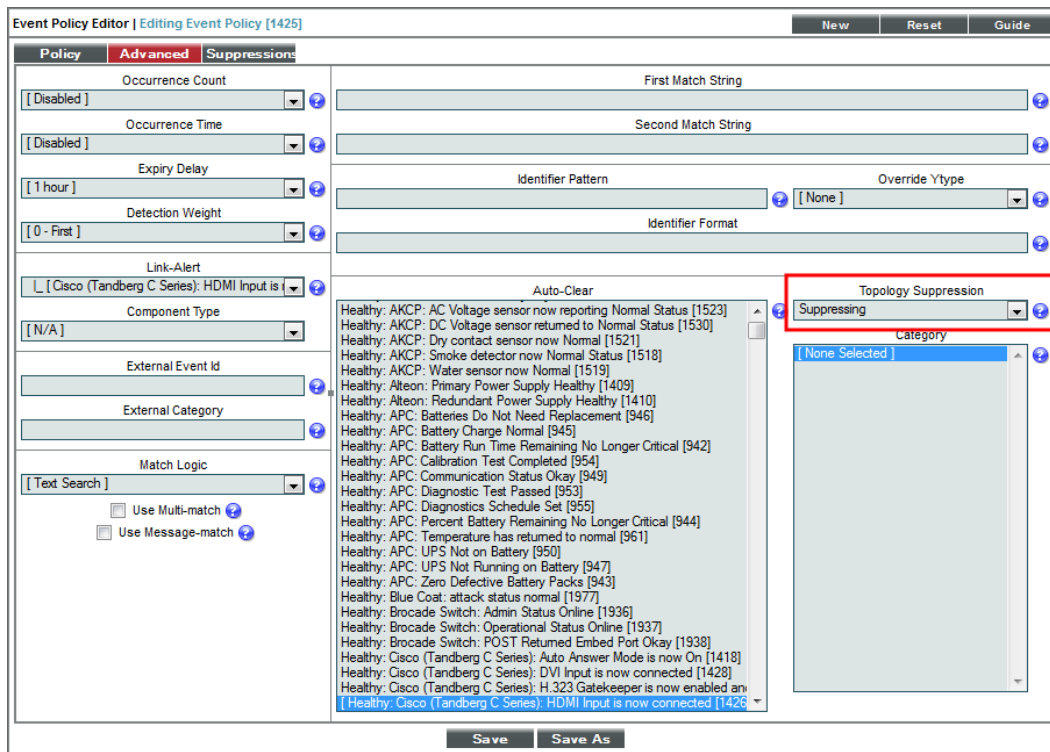
To manually configure event correlation in the classic SL1 user interface, you must define two types of events:

- **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 (or the **Event Console** page in the classic SL1 user interface) . The suppressible events will not appear in the **Events** page (or the **Event Console** page in the classic SL1 user interface) .
- **Suppressible events.** This type of event is suppressed on a child device only when a suppressing event occurs on the parent device.

NOTE: If you configure event categories, the suppressing and suppressible events must be associated with the same category for correlation to occur. If you do not configure event categories, each and every suppressing event that occurs on a parent device will cause SL1 to suppress **all suppressible** events on the associated children devices.

To define an event as a suppressing event on the **Event Policy Manager** page in the classic SL1 user interface):

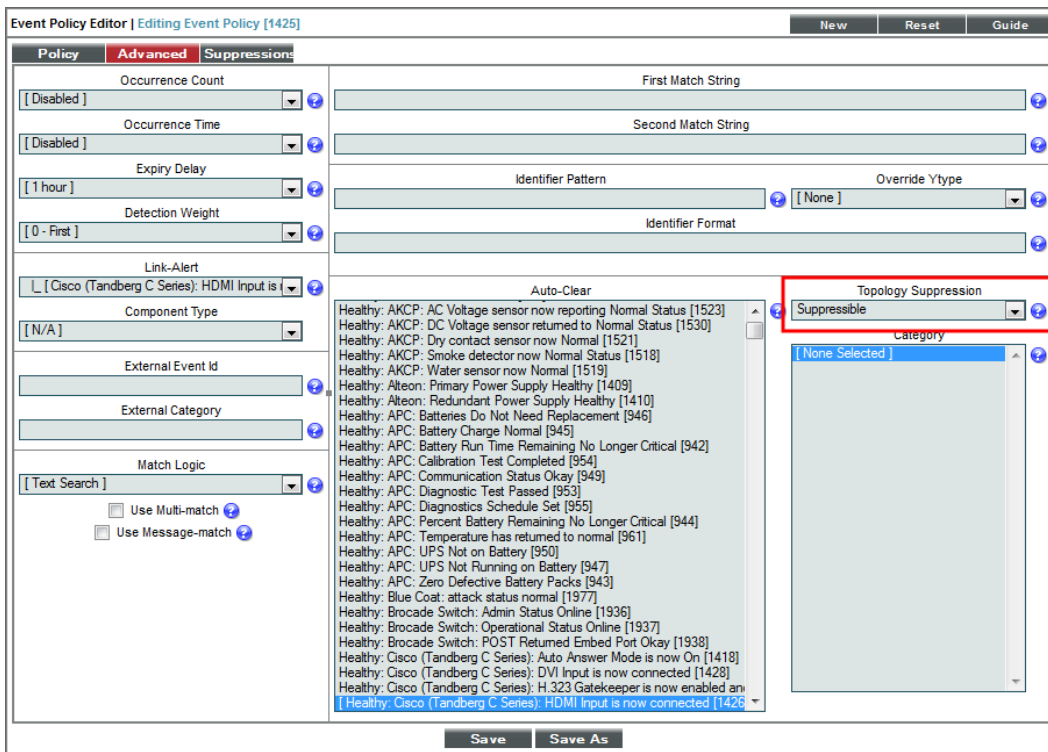
1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. On the **Event Policy Manager** page, click the wrench icon () of the event that you want to define as the **suppressing** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click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



4. In the **Topology Suppression** field, select *Suppressing*.
5. Click **[Save]**. In the future, when this event occurs on a device, 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 on the **Event Policy Manager** page in the classic SL1 user interface:

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



4. In the **Topology Suppression** field, select *Suppressible*.
5. Click **[Save]**. In the future, when this event occurs on a device, 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.

Example: Child Event Suppression

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

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

In this scenario, if an interface goes down on the switch *Boise-DMZ*, SL1 will not be able to communicate with the server, *HQ-W2K3-VC01*, attached to the switch.

With the above defined event topology suppression:

- The event "Poller: Interface operationally down" occurs on *Boise-DMZ*.
- The event "Poller: Device not responding" is suppressed on the server *HQ-W2K3-VC01*.

- On the **Events** page (or the **Event Console** page in the classic SL1 user interface), the only event that would appear in this scenario will be the event "Poller: Interface operationally down" on the device *Boise-DMZ*.

Event Categories

Event categories allow SL1 to more efficiently align masking or suppressing events. When you align an event category to a masking or maskable 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 masking event and the maskable event must both be aligned with a common event category.

NOTE: This section uses the terms "masking" and "maskable" for simplicity's sake, but these terms are interchangeable with "suppressing" and "suppressible". "Masking" and "maskable" are used in the unified SL1 user interface, while "suppressing" and "suppressible" are used in the classic SL1 user interface.

Before defining masking events and maskable events, you can define event categories to streamline event masking.

- If you do not define any event categories, then if a masking event occurs on a parent device, SL1 will search all related child devices for maskable events. On each child device, each occurrence of any event defined as maskable will be masked. Only the masking event and the parent device will appear on the **Events** page (or the **Event Console** page in the classic SL1 user interface). The maskable events will be nested under the masking 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 masking 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 maskable 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 masking event "Dynamic App Collection Problem" occurs.
 - SL1 will search for all child devices associated with the chassis and then search for all maskable events.
 - Suppose on the child device (the blade), two maskable events occur: "Temperature Critical" and "Availability Check Failed".
 - On the **Events** page (or the **Event Console** page in the classic SL1 user interface), SL1 will nest these two maskable events under the parent event, even though there is no relationship between the parent event and the child events.

- However, if you do define event categories and align those event categories to masking or maskable events, then those events will be correlated only with events that are aligned with the same event category. For example:
 - Suppose we define two event categories: "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 masking 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 maskable 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 masking or maskable, you align event categories like this:

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

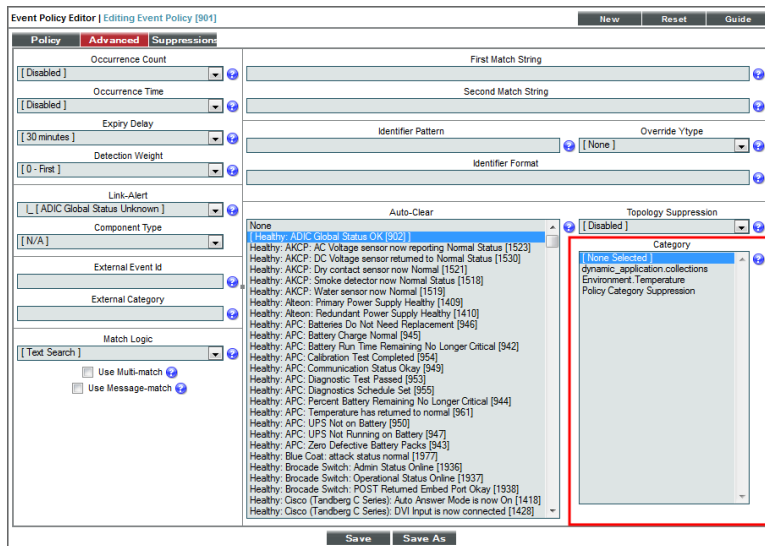
- Suppose on the parent device (the chassis) the masking event "Dynamic App Collection Problem" occurs.
 - SL1 will search for all child devices and then search for all maskable events that have the same event category, Dynamic Applications.Collection.
- Suppose on the child device (the blade) two maskable events occur: "Temperature Critical" and "Dynamic Application taking too long to collect".
 - On the **Events** page (or the **Event Console** page in the classic SL1 user interface), 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.
 - On the **Events** page (or the **Event Console** page in the classic SL1 user interface), SL1 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

For information about how to assign an event category to an event policy, see the section on [The Event Message Tab](#).

Assigning an Event Category to an Event in the Classic SL1 User Interface

In the classic SL1 user interface, 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.

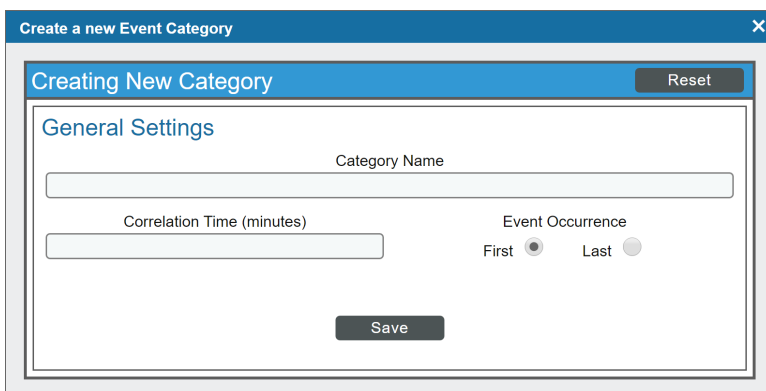
NOTE: If you assign an event category to an event that is neither suppressing nor suppressible, SL1 does not use the event category. The event category will have no effect.

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, click 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, click 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 (Events > Categories) displays the following about each event category:

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
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 let you 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:

NOTE: You can also use the "!" character in combination with the arithmetical 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:

"l?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.

Examples

- "!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".
- "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!*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXIXo" would match.
- "!"^s*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 "sXiXIXo" 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 that contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".

- "`^?n*$`". Matches text that begins with any single character, is followed by "n", and then zero or any number of any characters, and ends in "\$".

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 click the **[Go]** button.
4. Each selected event category is removed from SL1.

The screenshot shows the 'Event Category Manager' interface. The top navigation bar includes 'Inbox', 'Dashboards', 'Views', 'Events', 'Tickets', 'Knowledge', 'Reports', 'Registry', 'System', and 'Preferences'. The left sidebar lists various categories like 'Devices', 'Monitors', 'Networks', 'IT Services', 'Accounts', 'Assets', 'Business Services', 'Events', 'Run Book', 'Ticketing', and 'Web Proxies'. The main content area is titled 'Event Category Manager | Categories Found [5]' and contains 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 located to the right of the dropdown menu. The footer of the page reads: 'Copyright © 2003 - 2016 ScienceLogic, Inc. All rights reserved. 8.1.3.jenkins_EM7_G3_8.1.3 - build 127'.

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 the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

<i>How SL1 Generates Events</i>	107
<i>Viewing the List of Event Policies</i>	108
<i>Defining an Event Policy</i>	110
<i>The Match Logic Tab</i>	112
<i>The Event Message Tab</i>	115
<i>The Suppression Tab</i>	119
<i>Editing an Event Policy</i>	121
<i>Duplicating an Event Policy</i>	122
<i>Deleting an Event Policy</i>	122
<i>Selecting Multiple Event Policies</i>	122
<i>Using Event Policies in the Classic SL1 User Interface</i>	123
<i>Viewing the List of Event Policies in the Classic SL1 User Interface</i>	124
<i>Defining an Event Policy in the Classic SL1 User Interface</i>	131
<i>Editing an Event Policy in the Classic SL1 User Interface</i>	150

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 Policies** page (or the **Event Policy Manager** page in the classic SL1 user interface).

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 **Events** page (or the **Event Console** page in the classic SL1 user interface). 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 such as managers of managers (MoM). 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.
- **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.
- **Dynamic.** Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. SL1 examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, 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 Fahrenheit. If you do so, then if the chassis temperature exceeds 100 degrees at some point in the future, the alert evaluates to TRUE and the SL1 system inserts a message in the associated device's log files. The SL1 system matches that message with an existing event, and then triggers the event.
- **Email.** Message is generated by an email message sent to SL1.
- **API.** Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API.

- **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 Device Infrastructure Health* manual .

Viewing the List of Event Policies

From the **Event Policies** page (Events > Event Policies), you can view a list of all event policies in SL1 . To access the **Event Policies** page:

1. Go to Events > Event Policies. The **Event Policies** page appears:

NAME	STATUS	TYPE	WEIGHT	SEVERITY
% SASL Plain Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
% Vtg Token Failures Exceeded Threshold	Enabled	Dynamic	0	Minor
AKCP: AC Voltage sensor detects no current	Enabled	Syslog	0	Critical
AKCP: AC Voltage sensor now reporting Normal Status	Enabled	Syslog	0	Healthy
AKCP: DC Voltage High Warning	Enabled	Syslog	0	Major
AKCP: DC Voltage sensor High Critical	Enabled	Syslog	0	Critical
AKCP: DC Voltage sensor Low Critical	Enabled	Syslog	0	Critical
AKCP: DC Voltage sensor Low Warning	Enabled	Syslog	0	Major
AKCP: DC Voltage sensor returned to Normal Status	Enabled	Syslog	0	Healthy
AKCP: Dry Contact Sensor Low Critical	Enabled	Syslog	0	Critical
AKCP: Dry contact sensor now Normal	Enabled	Syslog	2	Healthy
AKCP: Humidity High Warning	Enabled	Syslog	0	Major
AKCP: Humidity Low Warning	Enabled	Syslog	0	Major
AKCP: Smoke Detector Alert!	Enabled	Syslog	10	Critical
AKCP: Smoke detector now Normal Status	Enabled	Syslog	4	Healthy
AKCP: Water Sensor has detected water	Enabled	Syslog	0	Critical

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

- **Name.** The name of the event policy.
- **Status.** Specifies whether the event policy is to be operational or not. Possible values are "Enabled" or "Disabled."
- **Type.** Specifies the source for the event policy. Possible values are:
 - *Syslog.* Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices such as managers of managers (MoM). A syslog is an unsolicited message from a device to 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.
 - *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.

- *Dynamic.* Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. SL1 examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, 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 Fahrenheit. If you do so, then if the chassis temperature exceeds 100 degrees at some point in the future, the alert evaluates to TRUE and the SL1 system inserts a message in the associated device's log files. The SL1 system matches that message with an existing event, and then triggers the event.
- *Email.* Message is generated by an email message sent to SL1.
- *API.* Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API.
- *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 Device Infrastructure Health** manual . *Monitoring*
- **Weight.** If two event definitions are very similar, the weight field specifies the order in which SL1 should match messages against each event definition. This field is most useful for event policies that use expression matching. The event definition with the lowest weight will be matched first.
- **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).
- **Edited By.** Name of the user who created or last edited the event.
- **Expiry.** If enabled, the time in which an active event will be cleared automatically if there is no re-occurrence of the event.
- **Ext. Category.** The category for the event. This is an optional field. If SL1 will be sending this event to an external system, this field defines the event category for use by the external system.
- **External ID.** The external event ID for the event. The external event ID is an optional field that can be used to correlate an event policy with an event ID on another network-monitoring system or on another SL1 system where the event has a different event ID.

- **Last Edited.** Date and time the event was created, imported into SL1, or last edited.
- **ID.** Unique numeric ID for the event policy, generated by SL1.
- **PowerPack.** Specifies whether the event is included in a PowerPack.
- **Threshold.** If enabled, the number of instances of an identical event from the identical source that must occur before creating a new event message in the **Events** page.
- **Time.** If enabled, the maximum amount of time to wait between multiple identical messages from the same source before creating a new event message in the Event Monitor. This allows related events to be rolled-up and posted together, under one event description.

TIP: To rearrange the columns in the List View, click and drag the column name to a new location. You can adjust the width of a column with by clicking and dragging the right edge of the column. You can click the **Select Columns** icon (⚙️) to add or remove columns, or to reset columns to their default settings.

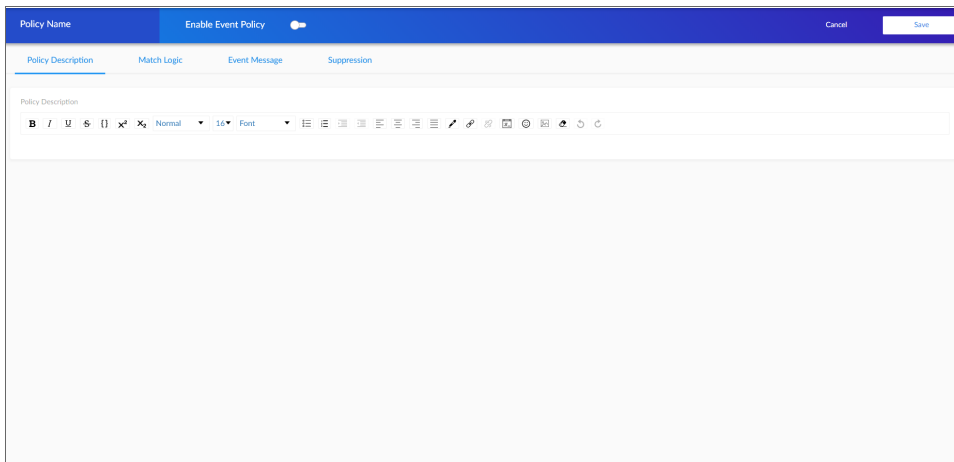
Defining an Event Policy

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 Policies** page (or the **Event Policy Manager** page in the classic SL1 user interface), you can define a new event. You can define custom events to meet your business requirements. You can also define events to be triggered by any custom Dynamic Application alerts you have created.

To create an event definition:

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



3. In the **Event Policy Editor** page and set of tabs, you can define a new event. The **Event Policy Editor** page contains the following fields and tabs:
 - **Policy Name**. Enter a name for the event policy.
 - **Enable Event Policy**. This toggle allows you to enable and disable the event policy.
 - **Policy Description**. Enter a description of the event policy.
 - **Match Logic**. Allows you to define pattern-matching for the event.
 - **Event Message**. Allows you to enter an event message and the severity of the event, as well as event masking.
 - **Suppression**. Allows you to suppress the event on selected devices and device groups.

The Match Logic Tab

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

The screenshot shows a web-based configuration interface for an event policy. At the top, there is a blue header bar with 'Policy Name' on the left, 'Enable Event Policy' with a toggle switch in the center, and 'Cancel' and 'Save' buttons on the right. Below the header, there are four tabs: 'Policy Description', 'Match Logic' (which is selected and highlighted in blue), 'Event Message', and 'Suppression'. The 'Match Logic' tab is divided into two main sections. The left section, titled 'MATCH CRITERIA', contains several fields: 'Event Source' (a dropdown menu with 'Syslog' selected), 'Syslog Facility' (a dropdown menu with 'Match Any' selected), 'Syslog Severity' (a dropdown menu with 'Match Any' selected), 'Syslog Application Name' (a text input field), 'Syslog Process ID' (a text input field), and 'Syslog Message ID' (a text input field). The right section contains a 'String' dropdown menu, a 'Match String' text input field, a 'Second Match String (Optional)' text input field, two toggle switches for 'Allow event to expire if it doesn't reoccur within a time frame' and 'Require multiple triggers within a time frame', a 'MATCHING' section with a 'Detection Weight' text input field set to '0', and two checkboxes: 'Multi Match' (with the subtext 'Allow other event policies to match this trigger') and 'Message Match' (with the subtext 'Create new event if entire message does not match').

- **Event Source.** Specifies the source for the event. The fields below this field will change based on your selection. Your options are:
 - *Syslog.* Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices such as managers of managers (MoM). A syslog is an unsolicited message from a device to 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. The following fields will appear:
 - **Syslog Facility.** Select the facility information used by syslog to match an event message.
 - **Syslog Severity.** Select the severity information used by syslog to match an event message.
 - **Syslog Application Name.** Type the application name used by syslog to match an event message.
 - **Syslog Process ID.** Type the Process ID used by syslog to match an event message.
 - **Syslog Message ID.** Type the 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>.

- *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. The following option will appear:

- **Select Link-Message.** Click this button to specify the message generated by SL1. The Link-Message window will appear with a list of messages to select from. Once you have selected a Message, click the **[Select]** button.

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

- **Trap.** Message is generated by an SNMP trap. SNMP traps can be sent by devices and proxy devices like 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. The following options will appear:
 - **Select Link-Trap.** Click this button to display a list of trap OIDs that are included in the MIB files that have been compiled in SL1. Select one of the listed trap OIDs to associate with the event. The **Link-Trap** window will appear with a list of traps to select from. After you have selected a trap, click the **[Select]** button.

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

- **Link-Trap.** Manually enter a custom trap OID as an alternative to selecting a Link-Trap using the **[Select Link-Trap]** button. You can use an asterisk (*) as a wildcard character at the end of the trap OID. If you add the wildcard character to the end of the trap OID, the event policy will match all trap OIDs that start with the specified OID string. This is useful for creating "catch all" event policies.
- **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.
- *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. SL1 examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, 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 Fahrenheit. If you do so, then if the chassis temperature exceeds 100 degrees at some point in the future, the alert evaluates to TRUE and the SL1 system inserts a message in the associated device's log files. The SL1 system matches that message with an existing event, and then triggers the event. The following option appears:
 - **[Select Link-Alert]**. Click this button to display a list of alerts defined in Dynamic Applications. A **Link-Alert** window displays a list of alerts. After you search for and select an alert, click **[Select]**. The alert is added to the **Link-Alert** field.
 - *Email*. Message is generated by an email message sent to SL1.
 - *API*. Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API.
 - *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 Device Infrastructure Health** manual. The following option appears:
 - **Log Policy**. Select the Log File Monitoring Policy the agent will use to collect the log message.

After selecting and defining your **Event Source**, enter values in the fields on the right side of the **Match Logic** tab:

- **String/Regular Expression**. Use this drop-down to select *String* or *Regular Expression*.
- **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 (Optional)**. A secondary string used to match against the originating log message. Can be up to 512 characters in length. Can be any combination of alpha-numeric and multi-byte characters. To match this event policy, the text of a log message or alert must match the value you enter in this field and the value you entered in the **Match String** field. This field is optional.
- **Allow event to expire if it doesn't reoccur within a time frame**. If toggled on, enter the time in which an active event will be cleared automatically if there is no reoccurrence of the event in the fields that appear. You can enter time in minutes or hours.

- **Require multiple triggers within a time frame.** If toggled on, enter the number of events and the time in which an event requires multiple triggers to occur in the fields that appear. You can enter time in minutes or 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).
- **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 **Multi Match** checkbox in all event policies 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.
- **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 **Message Match** checkbox, this behavior will occur only if the log messages or alerts contain the same message.

The Event Message Tab

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

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

Surround the regular expression with %R and %/R. For example:

%RFilename: .*? %/R

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

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

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

NOTE: If an event policy with a source of "Email" or "Trap" includes a poorly formed regular expression in the event message, SL1 will stop evaluating the event after 10 seconds and will generate a system event with a severity of Minor, alerting you to the issue.

- You can also use the following variables in this field:
 - %I (capital "eye"). Depending on the context, this variable contains one of the following:
 - For events with a source of "dynamic", this variable contains the index value from SNMP; this index value 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, in which case %I would return .1.1, .2.1, and .3.1, respectively:

```
1.3.6.1.4.1.999.3.2.1.1.1
1.3.6.1.4.1.999.3.2.1.2.1,
1.3.6.1.4.1.999.3.2.1.3.1.
```
 - For events with a source of "syslog" or "trap", this variable contains the value that matches the **Identifier Pattern** field in the **[Advanced]** tab.
 - For events with a source of "internal", this variable contains the "yName" (sub-entity name) value that matches the **Identifier Pattern** field in the **[Advanced]** tab.
 - %M. The full text of the log message that triggered the event 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*.
- **Correlate this event with external system.** Toggle this on if you want to correlate the event with an external system. Enter the *External ID* in the field that appears when this is turned on.
- **Categorize event for external system.** Toggle this on if you want to categorize this event for an external system. Enter the *External Category* in the field that appears when this is turned on.
- **Extract sub-entity using a regular expression.** Toggle this on if you want to extract a sub-entity using a regular expression. Enter values in the following fields that appear when this is turned on:
 - *Identifier pattern.* A regular expression used to extract the name of a sub-entity (like the name of a network interface) from within the log entry. By identifying the sub-entity, 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.
 - *Result order for multiple sub-entities.* If the **Identifier Pattern** field returns multiple results, users can specify which results to use and in which order. Each result is represented by a variable. This field is optional. For example, users could specify "%2:%1" for "Interface %2: Peer %1" where %1 is the first match with identifier pattern and %2 is the second match with identifier pattern.
 - *Y-type to override.* 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.

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**.

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

- **Autoclear.** If enabled, this field specifies whether an event can be cleared from the event list automatically. Click the **[Add Event Policy]** button to 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.

- **Topology Masking.**
 - *Mask events on child devices.* If this event occurs on a parent device, SL1 will search all related children devices for masked events.
 - If you have assigned a **Category** to this event, SL1 will search all the children devices and mask all events that have been defined as masked and are assigned to the same **Category**. For more details on event categories, see the section on [event correlation](#).
 - If you have not assigned a **Category** to this event, SL1 will search all children devices and mask all events that have been defined as masked and are not assigned to a **Category**. For more details on event categories, see the section on [event correlation](#).
 - The masked events will not appear on the **Events** page. They will be nested under the parent event.
 - *Maskable under a parent device's event.* This type of event is masked on a child device only when a maskable event occurs on the parent device.

- If you have assigned a **Category** to this event, SL1 will mask this event when it occurs on a child device and an event that has been defined as masked occurs on its parent device. The masked event must have the same **Category** as the maskable event. For more details on event categories, see the section on [event correlation](#).
- If you have not assigned a **Category** to this event, when a masked event that is not assigned to a **Category** occurs on the parent device SL1 will search all children devices and mask all events that have been defined as maskable and are not assigned to a **Category**. For more details on event categories, see the section on [event correlation](#).
- The maskable events will not appear on the **Events** page. They will be nested under the parent event.
- If both *Mask events on child devices* and *Maskable under a parent device's event* are selected, then if this event occurs on a parent device, it behaves as a masked event. If this event occurs on a child device, it behaves as a maskable event.
- **Add Category.** When you define a hierarchy between events, you can include a **Category**. A **Category** allows SL1 to more efficiently align masked events with maskable events. When you align an event category to a masked or maskable 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 masked event and the maskable event must both be aligned with a common category.

Click the **[Add Category]** button to open the **Available Categories** window and select the categories you want to add. For more details on event categories, see the section on [event correlation](#).

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

- If you have assigned a **Category** to a masked event, SL1 will search all the children devices and suppress all events that have been defined as maskable and are assigned to the same **Category**.
- If you have not assigned a **Category** to a masked event, when the event occurs on the parent device SL1 will search all children devices and suppress all events that have been defined as maskable and are not assigned to a **Category**.

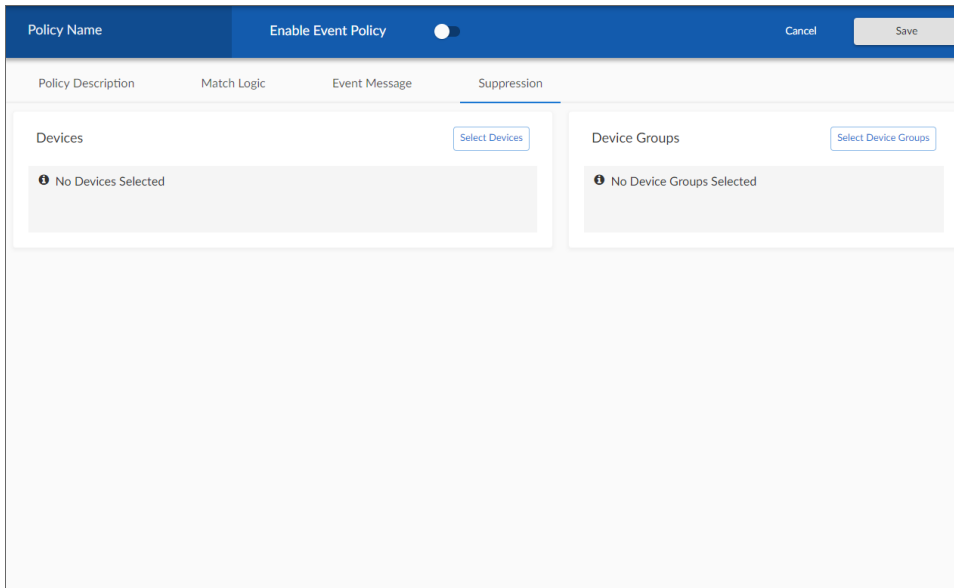
The Suppression Tab

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

A manually suppressed event is suppressed only for the selected devices and devices in the selected device groups. If the event occurs on another device, 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 **[Suppressions]** tab, you can define or edit the following:



- **Devices.** Devices on which you can suppress the current event. To suppress the current event on a device , click the **[Select Devices]** button and select one or more devices from the **Available Devices** window. The device(s) should now appear in a list under **Devices**. To remove a device from the list, click the **✕** icon next to the device name in the list.

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.

- **Device Groups.** Device groups on which you can suppress the current event. To suppress the current event on all devices in a device group, click the **[Select Device Groups]** button and select one or more device groups from the **Available Device Groups** window. The device group(s) should now appear in the list under **Device Groups**. To remove a device group from the list, click the **✕** icon next to the device group in the list. 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.

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

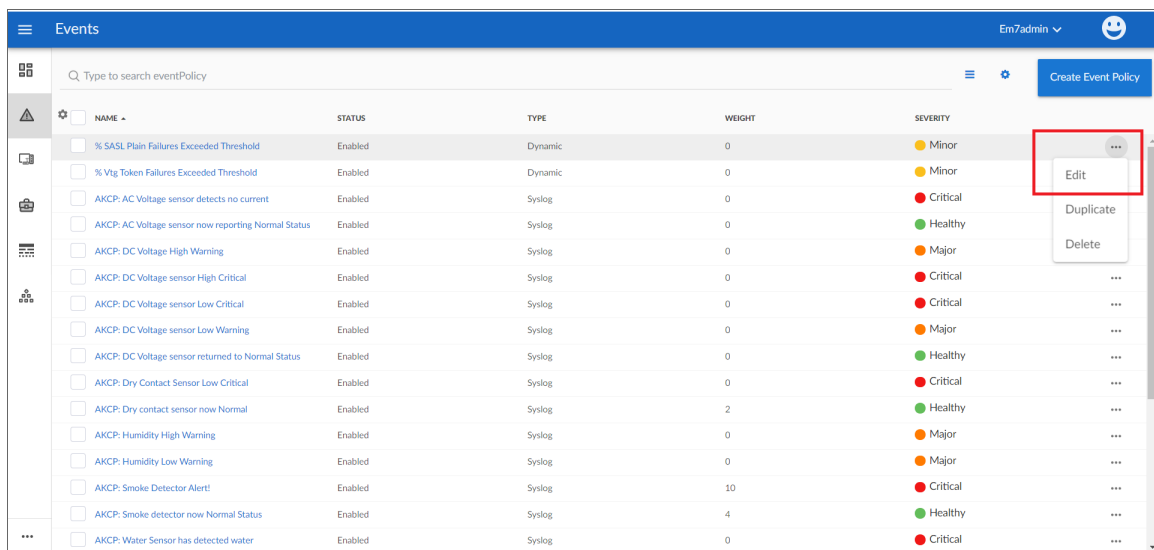
Editing an Event Policy

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

CAUTION: If you edit an event policy that was imported into your 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 Policies** page (Events > Event Policies).



2. In the **Event Policies** page, select the Actions menu (**...**) of the event policy you want to edit and select *Edit*.
3. The selected event policy is displayed in the **Event Policy Editor** page, where you can edit one or more properties of the event policy.
4. The **Event Policy Editor** page contains the following fields and tabs:
 - **Policy Name**. Edit the name for the event policy.
 - **Enable Event Policy**. This toggle allows you to enable and disable the event policy.
 - **Policy Description**. Edit the description of the event policy.


- **Match Logic.** Allows you to define pattern-matching for the event. This tab is described in the [Match Logic Tab](#) section.
- **Event Message.** Allows you to enter an event message and the severity of the event, as well as event masking. This tab is described in the [Event Message Tab](#) section.
- **Suppression.** Allows you to suppress the event on selected devices and device groups. This tab is described in the [Suppression Tab](#) section.

5. Click **[Save]** to save your changes to the event policy.

Duplicating an Event Policy

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

To duplicate an Event Policy:


1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the Actions menu () of the event policy you want to duplicate and select *Duplicate*.

A new Event Policy will appear in the list. It will have the same name as the Event Policy you duplicated, with the addition of "-Copy" at the end. For example, if you duplicated an Event Policy with the name "Temperature Critical", then the new Event Policy would be named "Temperature Critical-Copy".

3. Follow the instructions in the [Editing an Event Policy](#) section to edit the new Event Policy.

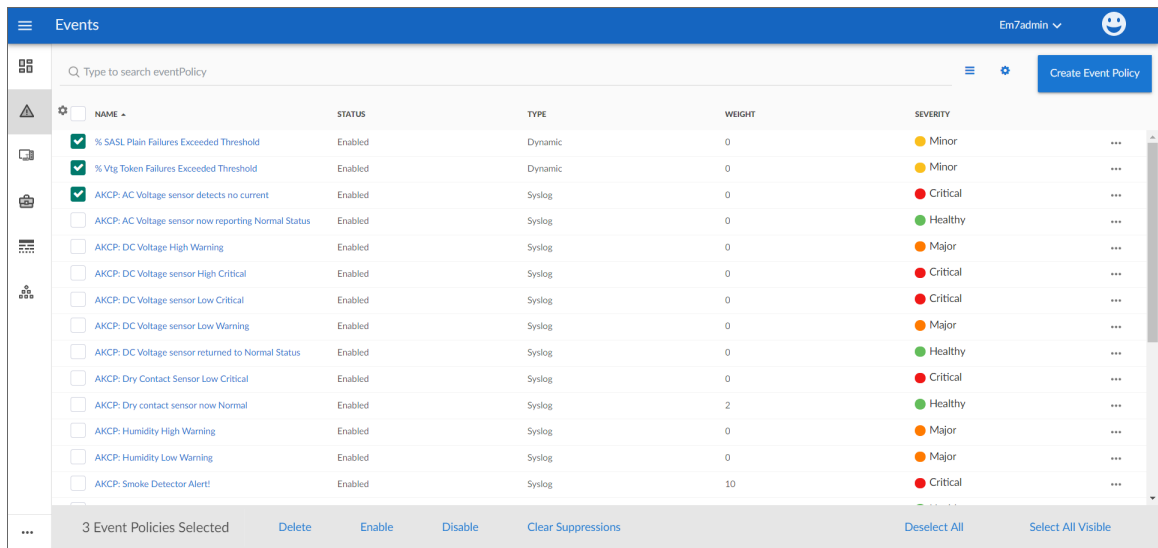
Deleting an Event Policy

To delete an Event Policy:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the Actions menu () of the event policy you want to duplicate and select *Delete*.

Selecting Multiple Event Policies

On the **Event Policies** page (Events > Event Policies), you can use the checkboxes to the left of the Event Policies to select more than one Event Policy at a time:



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

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

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

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

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

Using Event Policies in the Classic SL1 User Interface

This section describes how to view, define, and edit event policies using the **Event Policy Manager** in the classic SL1 user interface.

Viewing the List of Event Policies in the Classic SL1 User Interface

From the **Event Policy Manager** page of the classic user interface, 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	0	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. Alteon: New Flash Enabled	Dynamic	Enabled	Yes	Notice	0	36	30 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
21. Alteon: Primary Power Supply Failure	Dynamic	Enabled	Yes	Major	0	32	90 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
22. Alteon: Primary Power Supply Healthy	Dynamic	Enabled	Yes	Healthy	0	33	15 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
23. Alteon: Redundant Power Supply Failure	Dynamic	Enabled	Yes	Major	0	34	90 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
24. Alteon: 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 such as managers of managers (MoM). 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.
 - *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.
 - *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. SL1 examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, 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 Fahrenheit. If you do so, then if the chassis temperature exceeds 100 degrees at some point in the future, the alert evaluates to TRUE and the SL1 system inserts a message in the associated device's log files. The SL1 system matches that message with an existing event, and then triggers the event.
 - *Email*. Message is generated by an email message sent to SL1.
 - *API*. Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API.
 - *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 Device Infrastructure Health** 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 SL1 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 SL1.

- **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 SL1, 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 SL1 system where the event has a different event ID.
- **Category.** The category for the event. This is an optional field. If SL1 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 in the Classic SL1 User Interface

The Filter-While-You-Type fields appear as a row of blank fields at the top of the list. These fields let you 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:

NOTE: You can also use the "!" character in combination with the arithmetical 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.

Examples

- "!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".
- "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, O2, !aggr". Matches text that contains "silo" and also text that contains "O2" 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!*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXIo" would match.
- "!^s*i!*o\$". Matches all text that does not that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXIo" 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 in the Classic SL1 User Interface

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 Policies** page (or the **Event Policy Manager** page in the classic SL1 user interface), you can define a new event. You can define custom events to meet your business requirements. You can also define events to be triggered by any custom Dynamic Application alerts you have created.

To create an event definition:

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

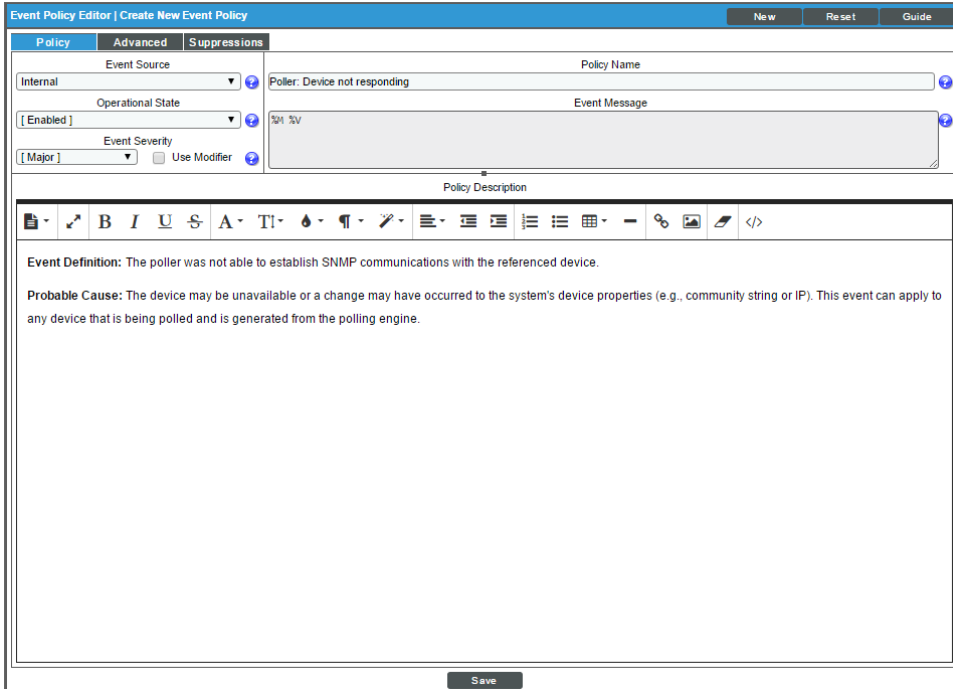
- In the **Event Policy Manager** page, click the **[Create]** button. The **Event Policy Editor** page appears:

The screenshot shows the 'Event Policy Editor' interface for creating a new policy. The 'Policy' tab is selected, showing configuration options for the event source, state, and severity. The 'Advanced' and 'Suppressions' tabs are also visible. The 'Policy Description' field is currently empty, with a rich text editor toolbar above it. A 'Save' button is located at the bottom of the form.

- 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. The 'Policy' tab is active, displaying the following fields:

- Event Source:** Internal
- Operational State:** [Enabled]
- Event Severity:** [Major]
- Use Modifier:**
- Policy Name:** Poller: Device not responding
- Event Message:** %M %V

The 'Policy Description' section 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 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 such as managers of managers (MoM). 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.
 - *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.

- *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell SL1 how to monitor applications and devices. You can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow you to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. SL1 examines each new message in the device log and determines if the message matches an event definition. If the message matches an event definition, 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 Fahrenheit. If you do so, then if the chassis temperature exceeds 100 degrees at some point in the future, the alert evaluates to TRUE and the SL1 system inserts a message in the associated device's log files. The SL1 system matches that message with an existing event, and then triggers the event.
- *Email*. Message is generated by an email message sent to SL1.
- *API*. Message is generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API.
- *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 Device Infrastructure Health** 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 regular expression syntax, see the documentation at <http://www.python.org>.

NOTE: If an event policy with a source of "Email" or "Trap" includes a poorly formed regular expression in the event message, SL1 will stop evaluating the event after 10 seconds and will generate a system event with a severity of Minor, alerting you to the issue.

- You can also use the following variables in this field:
 - `%I` ("eye"). Depending on the context, this variable contains one of the following:
 - For events with a source of "dynamic", this variable contains the index value from SNMP; this index value 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, in which case `%I` would return `.1.1`, `.2.1`, and `.3.1`, respectively:

```
1.3.6.1.4.1.999.3.2.1.1.1
1.3.6.1.4.1.999.3.2.1.2.1,
1.3.6.1.4.1.999.3.2.1.3.1.
```
 - For events with a source of "syslog" or "trap", this variable contains the value that matches the **Identifier Pattern** field in the **[Advanced]** tab.
 - For events with a source of "internal", this variable contains the "yName" (sub-entity name) value that matches the **Identifier Pattern** field in the **[Advanced]** tab.
 - `%M`. The full text of the log message that triggered the event 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 -7* 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:

The screenshot shows the 'Event Policy Editor | Editing Event Policy [3637]' window. The 'Advanced' tab is selected. On the left, there are settings for Occurrence Count (set to [Disabled]), Occurrence Time (set to [Disabled]), Expiry Delay (set to [1 hour]), and Detection Weight (set to [0 - First]). Below these are Link-Alert, External Event Id, External Category, and Match Logic (set to [Text Search]). The Match Logic section includes checkboxes for 'Use Multi-match' and 'Use Message-match'. The main area contains fields for First Match String, Second Match String, Identifier Pattern, Identifier Format, Auto-Clear, and Topology Suppression. The Auto-Clear and Topology Suppression sections have dropdown menus for selecting event categories. At the bottom, there are 'Save' and 'Save As' buttons.

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

NOTE: If you used the previous three fields to associate an event with an interface, then on the **Events** page, the link icon for this event 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**.

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

For example, given the following incoming message:

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

And given this **Identifier Pattern**:

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

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

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

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

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

- **Auto-Clear.** If enabled, this field specifies 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 section on [event correlation](#).

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

- *Disabled.* This event is neither a parent event nor a child event.
 - *Suppressing.* If this event occurs on a parent device, 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 section on [event correlation](#).
 - 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 section on [event correlation](#).
 - 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 section on [event correlation](#).
 - If you have not assigned a **Category** to this event, when a *Suppressing* event that is not assigned to a **Category** occurs on the parent device 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 section on [event correlation](#).
 - 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 section on [event correlation](#).

NOTE: You can use the field at the top of the **Category** field to filter the list of events. If you enter an 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**.

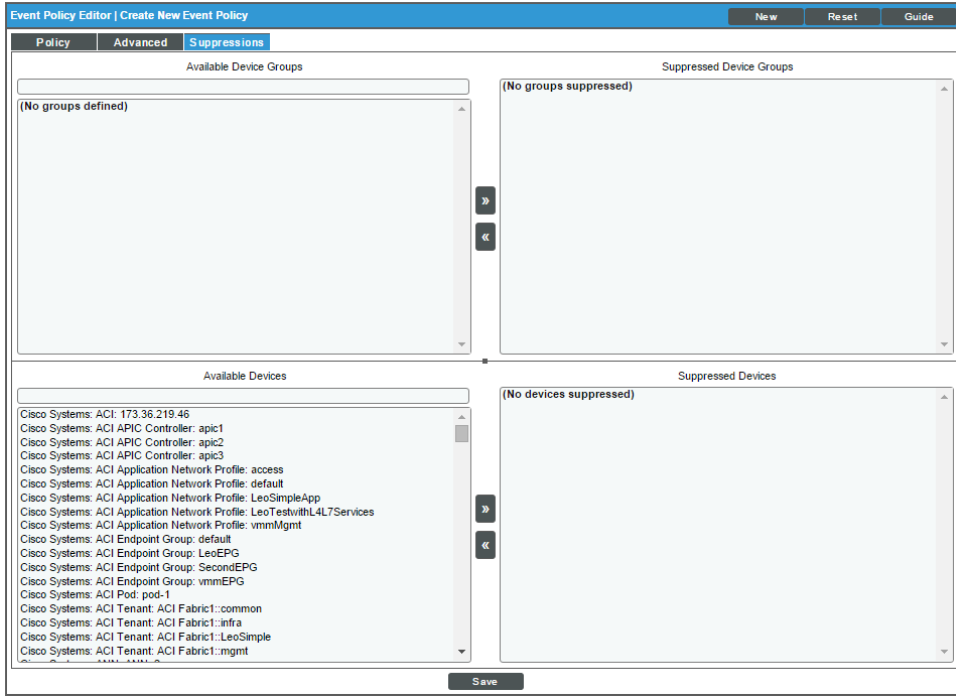
Defining EventSuppressions in the Suppressions Tab

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 **[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.

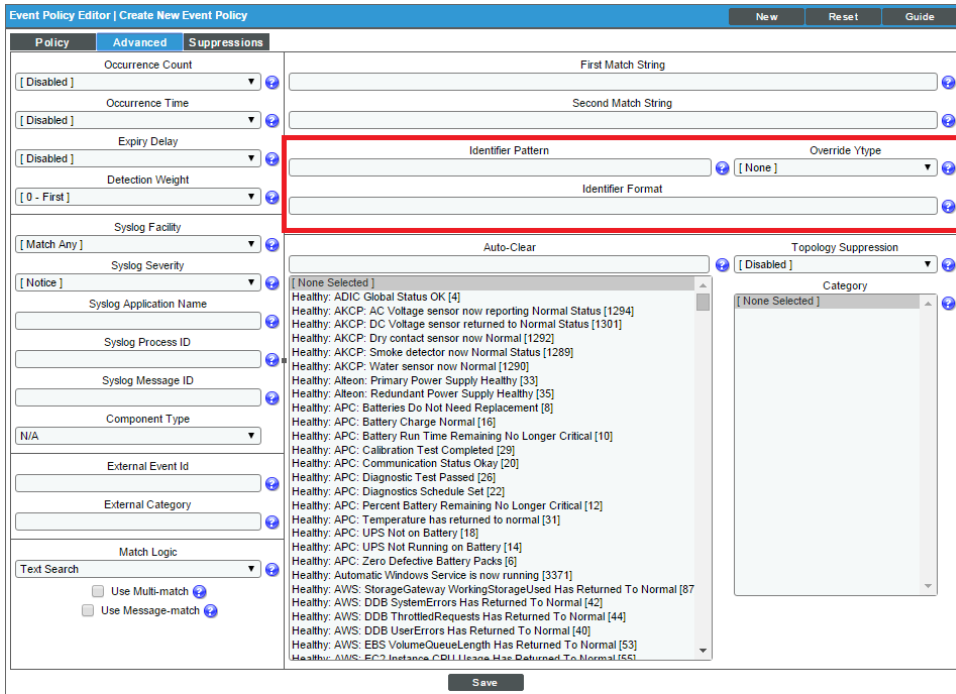
You can also include the interface name and SL1's unique interface ID in automation policies associated with the event.

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 regular expression syntax, see the documentation at <http://www.python.org>.

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

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

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

- **Override YType.** Specifies a yType for the interface (yType for interfaces is 7). If 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.

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

If these fields are used in an event:

- On the **Events** page, the link icon for this event 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 *Monitoring Network Interfaces* in the **Monitoring Device Infrastructure Health** 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.

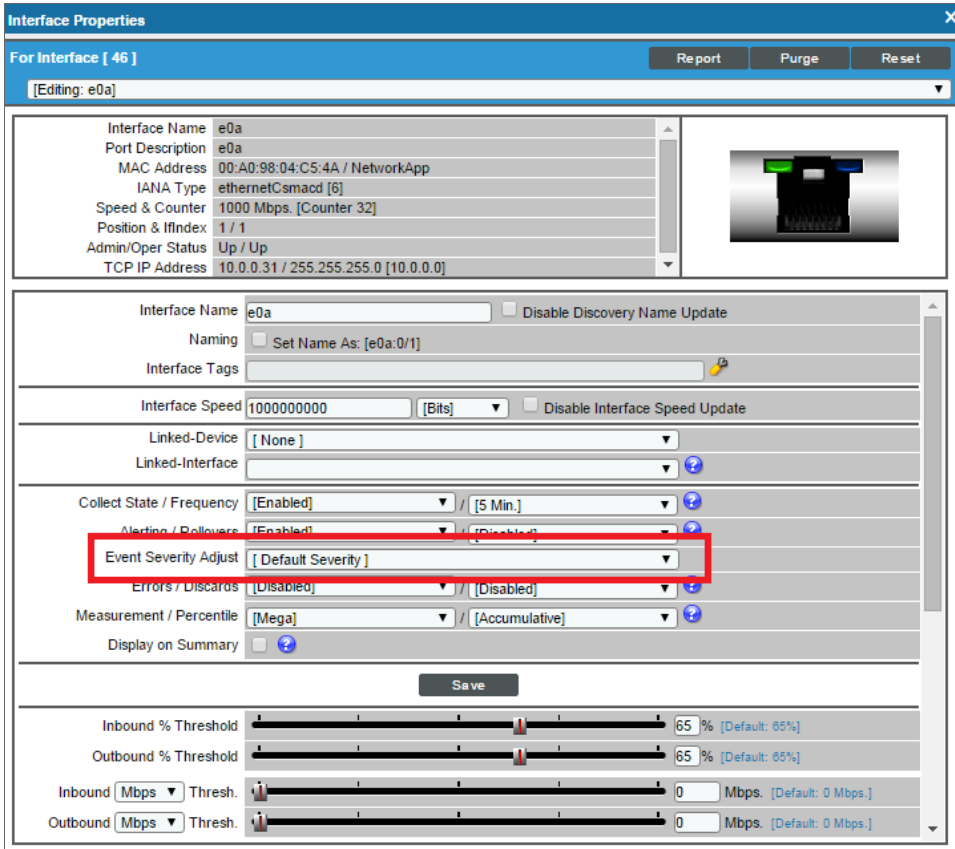
You could then edit the following events and tell them to use the custom severity for each interface that includes a custom severity:

- 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:

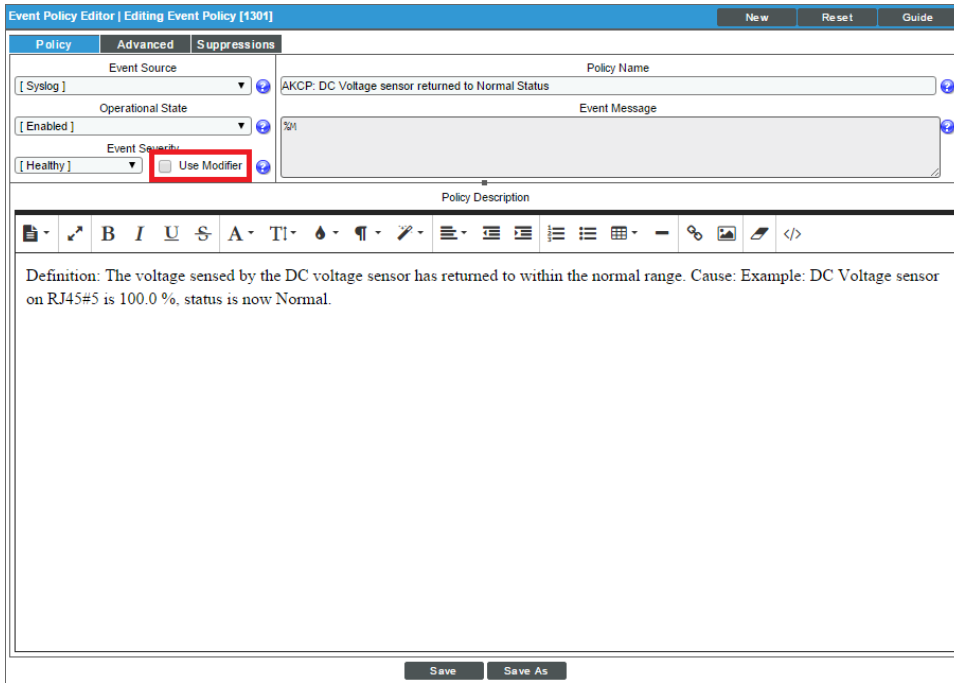
1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).
2. Select the wrench icon (🔧) for the interface for which you want to view the **Interface Properties** page.
3. Supply a value in the **Event Severity Adjust** field. Select the **[Save]** button.



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 in the Classic SL1 User Interface

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 of the classic user interface.

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	Thresh	Edited By	Last Colled	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	Major	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 the menu options, click the Advanced menu icon ().

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

Automation Policies	153
Action Policies	154

Automation Policies

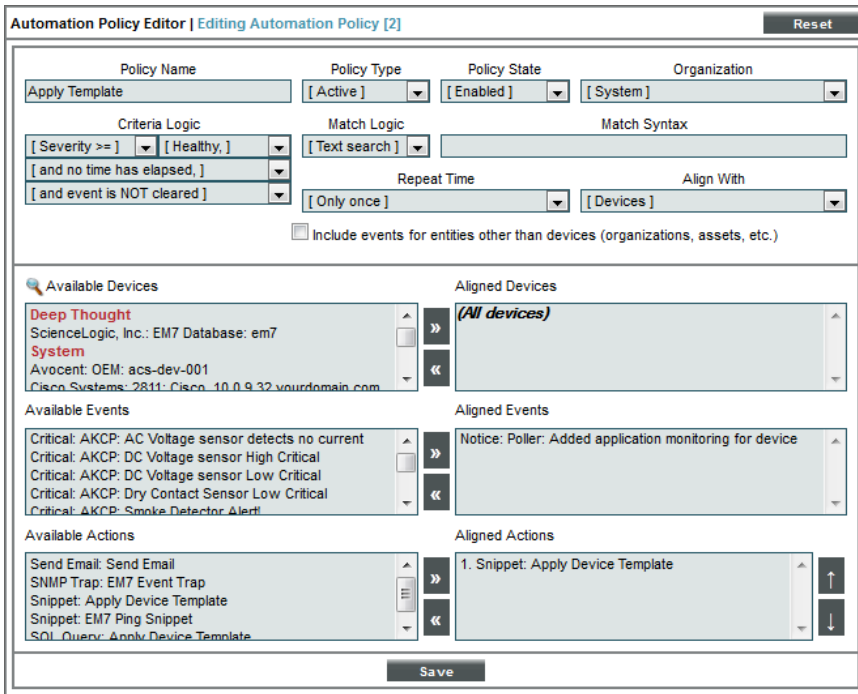
An automation policy allows you to define automatic actions that should be executed in response to events. An **automation policy** defines the event conditions that can trigger an automatic action.

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.



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).

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.

This chapter includes the following topics:

Configuring Events from Email	156
---	-----

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*.

Chapter

9



Reports for Events

Overview

SL1 provides the following types of reports on events:

- **Event Statistics report from the Event Console page in the classic SL1 user interface.** This report displays information about all active events on all devices in SL1.
- **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 the menu options, click the Advanced menu icon (.

The following sections describe each type of event report:

Event Statistics in the Event Console Page in the Classic SL1 User Interface	158
Event Statistics for a Single Device	162
Event Reports in the Reports Tab	164
Event Clear Map Report	164
Event Detections Report	167

<i>Unique Event Detections Report</i>	169
Event Overview Report	172
<i>Setting the Date for Reports</i>	172
<i>Number of Events by Severity</i>	172
<i>Most Common Event Types</i>	173
<i>Mean Time-to-Resolution</i>	173
Event Statistics	173
<i>Defining the Date Range</i>	174
<i>Fields</i>	174
<i>The Graph</i>	174

Event Statistics in the Event Console Page in the Classic SL1 User Interface

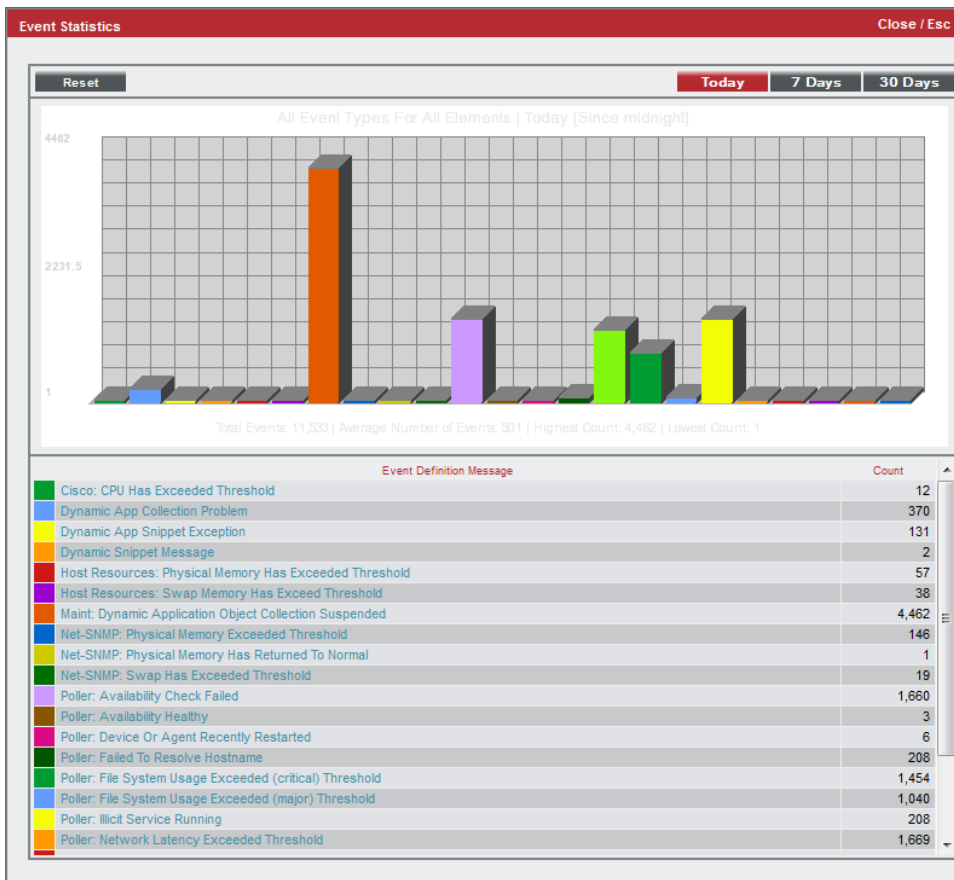
The **Event Statistics** modal page in the classic user interface displays a report on all events you are allowed to view. Users of type "Administrator" can view all events. Users of type "User" can view events that are aligned with the same organizations as their user account. For example, a user who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

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

To access and view the Event Statistics report:

1. Go to the **[Events]** tab.
2. In the **Event Console** page, in the **[Actions]** drop-down list, select **Event Statistics**. The Event Statistics report appears.
3. The Event Statistics report is displayed.

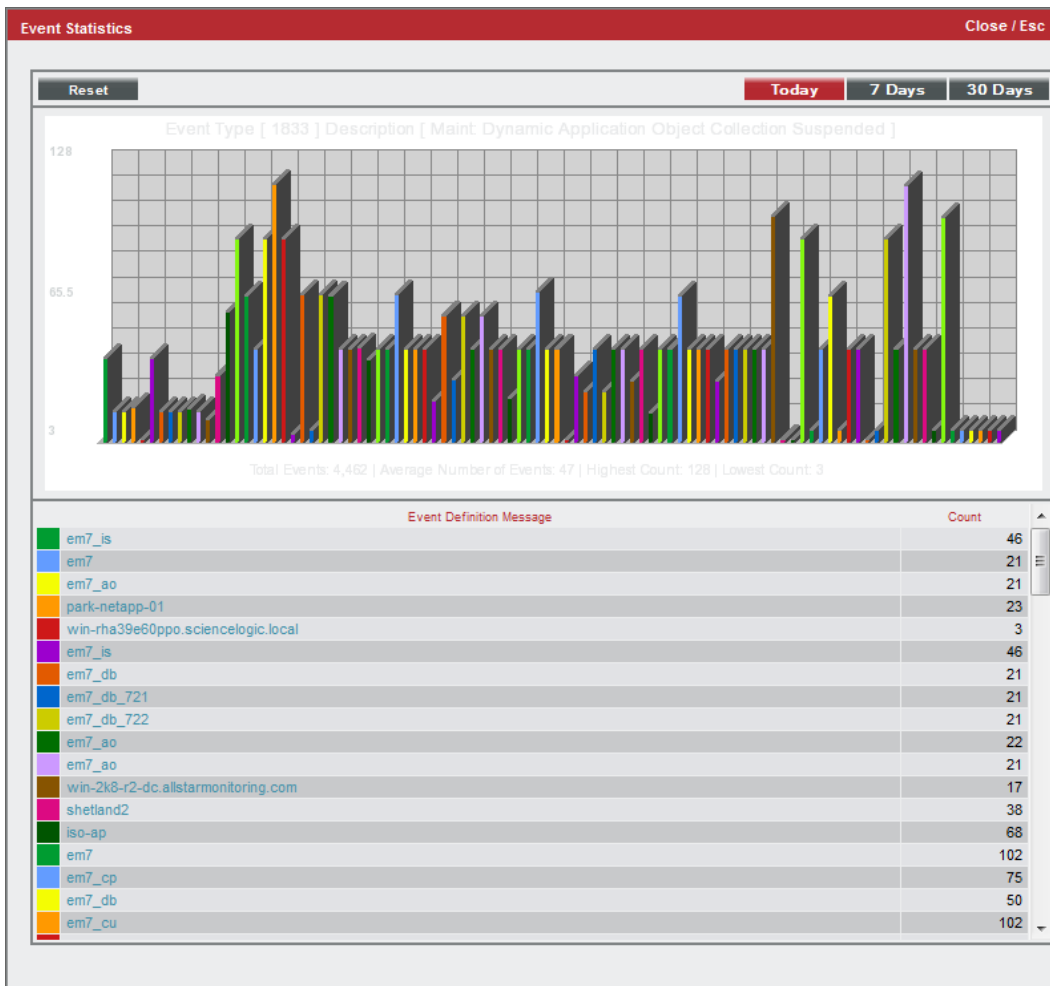
4. Initially, the **Event Statistics** page displays the bar graph "All Event Types for All Elements" for the past day.



5. The "All Event Types for All Elements" graph displays:

- All events that have occurred on all elements (that you are allowed to view) for the past day. You can select the **[7 Days]** button or the **[30 Days]** button to change the time period.
- Each event, represented by a colored bar. Mousing over a bar displays the name of the event and the number of occurrences.
- The event name on the x-axis.
- The number of occurrences on the y-axis.
- A table, listing each event and the number of occurrences.

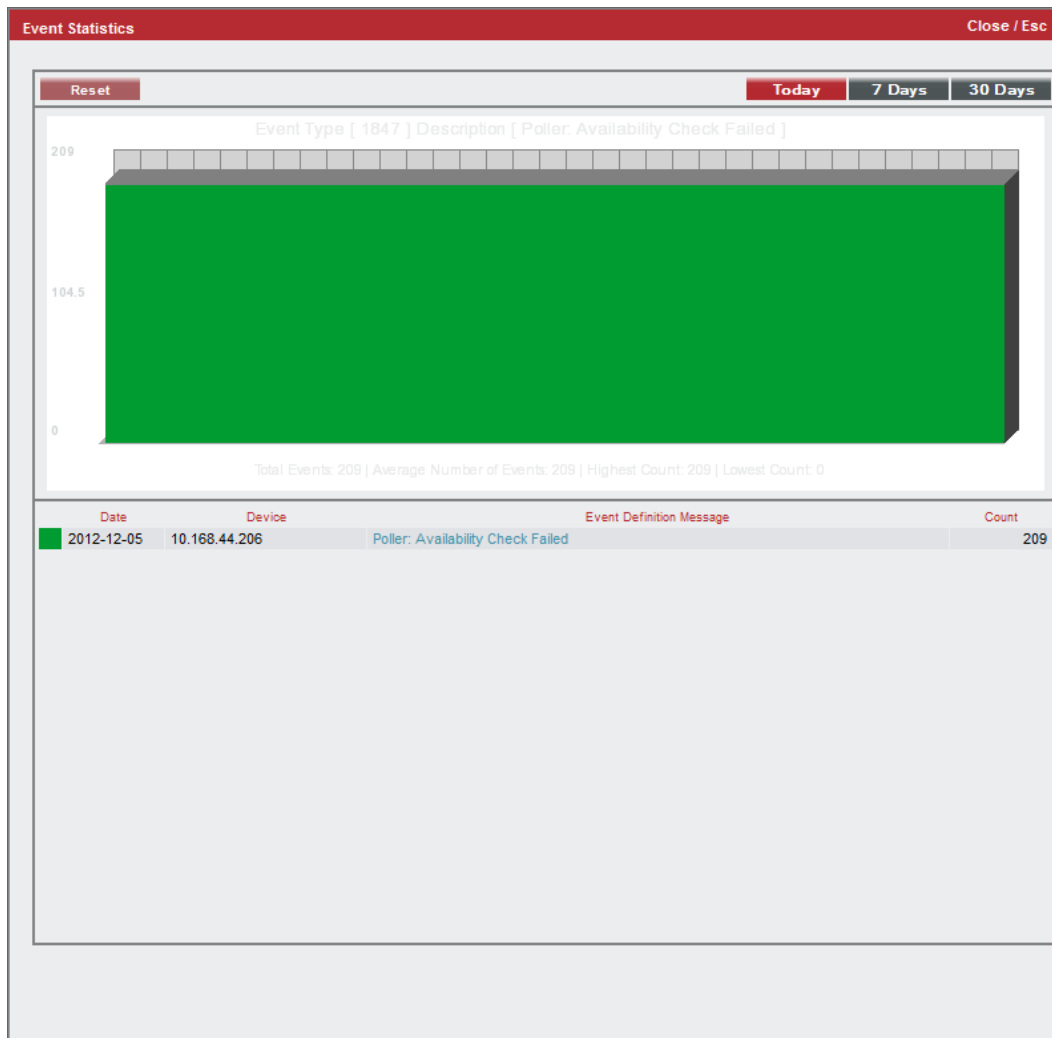
6. Clicking on a bar displays the "Single Event Type on All Elements" bar graph.



7. The "Single Event Type on All Elements" graph displays:

- Each occurrence of the selected event on all elements (that you are allowed to view) during the selected time period.
- Each element is represented by a colored bar. Mousing over a bar displays the name of the element and the number of occurrences.
- The element name on the x-axis.
- The number of occurrences on the y-axis.
- The graph also includes a table of each element where the event occurred and the number of occurrences.

8. Clicking on a bar displays the "Single Event Type For Selected Device" bar graph.



9. The "Single Event Type For Selected Device" graph displays:


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

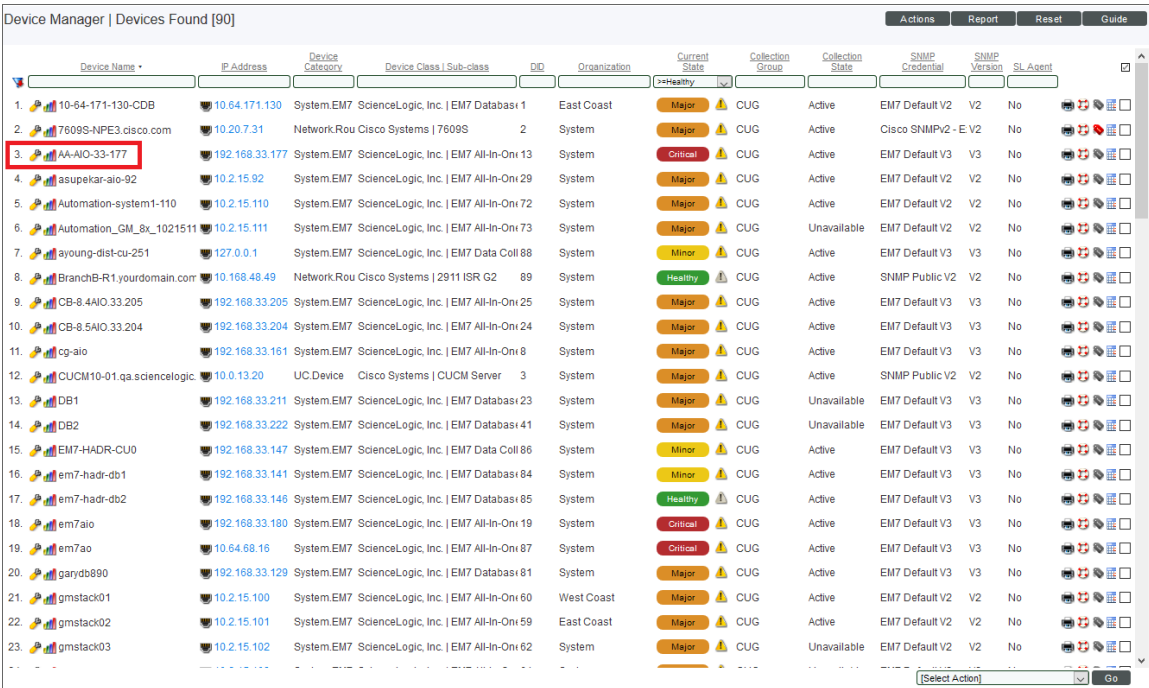
10. Clicking on the bar displays the [Events page for the device](#).

Event Statistics for a Single Device

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

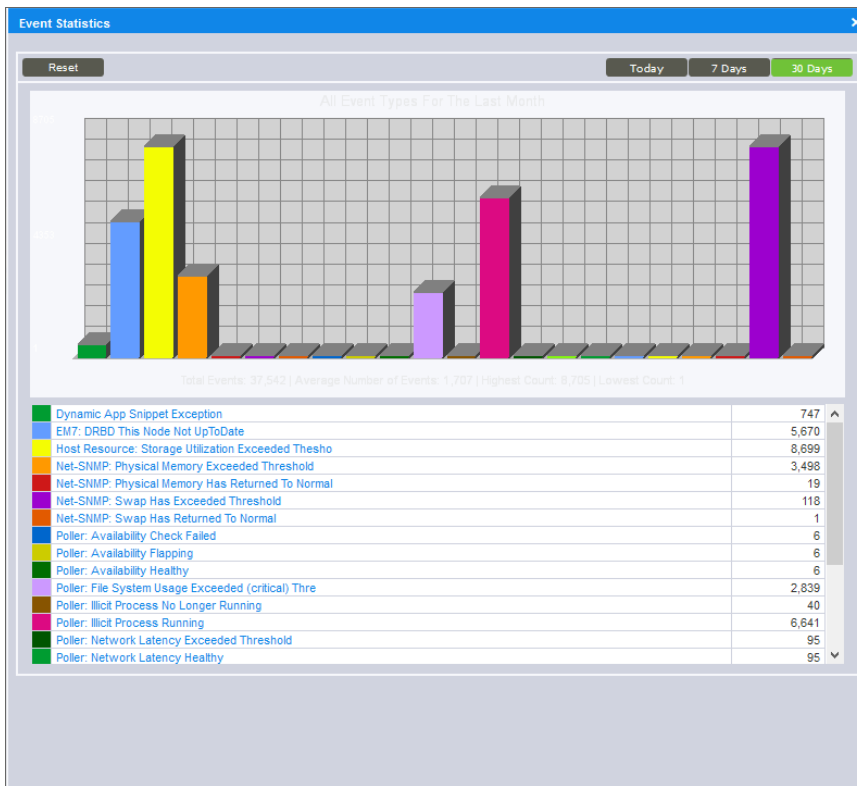
To view and access the Event Statistics report for a single device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. On the **Device Manager** page, select the bar graph icon () for the device for which you want to view Event Statistics.



Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	SL Agent
10-64-171-130-CDB	10.64.171.130	System.EM7	ScienceLogic, Inc. EM7 Databas	1	East Coast	Major	CUG	Active	EM7 Default V2	V2	No
17609S-NPE3.cisco.com	10.20.7.31	Network.Rou	Cisco Systems 7609S	2	System	Major	CUG	Active	Cisco SNMPv2 - E V2	No	No
AA-AIO-33-177	192.168.33.177	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	13	System	Critical	CUG	Active	EM7 Default V3	V3	No
asupekar-airo-92	10.2.15.92	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	29	System	Major	CUG	Active	EM7 Default V2	V2	No
Automation-system1-110	10.2.15.110	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	72	System	Major	CUG	Active	EM7 Default V2	V2	No
Automation_GM_8x_1021511	10.2.15.111	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	73	System	Major	CUG	Unavailable	EM7 Default V2	V2	No
ayoung-dist-cu-251	127.0.0.1	System.EM7	ScienceLogic, Inc. EM7 Data Coll	88	System	Minor	CUG	Active	EM7 Default V3	V3	No
BranchB-R1.yourdomain.com	10.168.48.49	Network.Rou	Cisco Systems 2911 ISR G2	89	System	Healthy	CUG	Active	SNMP Public V2	V2	No
CB-8.4AIO.33.205	192.168.33.205	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	25	System	Major	CUG	Active	EM7 Default V3	V3	No
CB-8.5AIO.33.204	192.168.33.204	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	24	System	Major	CUG	Active	EM7 Default V3	V3	No
cg-airo	192.168.33.161	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	8	System	Major	CUG	Active	EM7 Default V3	V3	No
CUCM10-01.qa.sciencelogic	10.0.13.20	UC.Device	Cisco Systems CUCM Server	3	System	Major	CUG	Active	SNMP Public V2	V2	No
DB1	192.168.33.211	System.EM7	ScienceLogic, Inc. EM7 Databas	23	System	Major	CUG	Unavailable	EM7 Default V3	V3	No
DB2	192.168.33.222	System.EM7	ScienceLogic, Inc. EM7 Databas	41	System	Major	CUG	Unavailable	EM7 Default V3	V3	No
EM7-HADR-CU0	192.168.33.147	System.EM7	ScienceLogic, Inc. EM7 Data Coll	86	System	Minor	CUG	Active	EM7 Default V3	V3	No
em7-hadr-db1	192.168.33.141	System.EM7	ScienceLogic, Inc. EM7 Databas	84	System	Minor	CUG	Active	EM7 Default V3	V3	No
em7-hadr-db2	192.168.33.146	System.EM7	ScienceLogic, Inc. EM7 Databas	85	System	Healthy	CUG	Active	EM7 Default V3	V3	No
em7aio	192.168.33.180	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	19	System	Critical	CUG	Active	EM7 Default V3	V3	No
em7ao	10.64.68.16	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	87	System	Critical	CUG	Active	EM7 Default V3	V3	No
qarydb890	192.168.33.129	System.EM7	ScienceLogic, Inc. EM7 Databas	81	System	Major	CUG	Active	EM7 Default V3	V3	No
gmstack01	10.2.15.100	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	60	West Coast	Major	CUG	Active	EM7 Default V2	V2	No
gmstack02	10.2.15.101	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	59	East Coast	Major	CUG	Active	EM7 Default V2	V2	No
gmstack03	10.2.15.102	System.EM7	ScienceLogic, Inc. EM7 All-In-Oni	62	System	Major	CUG	Unavailable	EM7 Default V2	V2	No

3. SL1 displays the **Device Reports** panel for the device. In the **Device Reports** panel for the device, click the **[Events]** tab.
4. On the **Viewing Events** page, click the **[Stats]** button. The **Event Statistics** modal page appears:



5. By default, the **Event Statistics** page displays the graph "All Event Types for the Last Month." This graph displays all events that have occurred on the device this month. This graph displays:

- All events that have occurred on the device in the last month. You can select the **[7 Days]** button to change the time period.
- Each event, represented by a colored bar. Mousing over a bar displays the name of the event and the number of occurrences.
- The event name on the x-axis.
- The number of occurrences on the y-axis.
- A table, listing each event and the number of occurrences.
- Additionally, clicking on a button displays all events that have occurred on the device during the selected time period.

6. Clicking on a bar displays the "Event Type" graph. This graph displays:
 - Each occurrence of the selected event on the element during the time period.
 - The name of the event, total number of occurrences, and date of the selected occurrence (when mousing over a bar).
 - The element name on the x-axis.
 - The number of occurrences on the y-axis.
 - A table, listing each occurrence of the event on the device, the date of the occurrence, and number of total occurrences.

Event Reports in the Reports Tab

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).

Run Quick Report: [Event Clear Map, version 1.4]

Edit Reset Guide

Sort By

- Severity
- Event Name
- Event ID

Show Events

- That are cleared
- Including non-cleared

Show At or Above

- Critical
- Major
- Minor
- Notice
- Healthy

Optional Columns

- Event Source
- Dynamic App Name
- Event Source Message
- Expiry Minutes

Output format: Web page (.html)

Generate

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 SL1 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).

The screenshot shows the 'Run Quick Report' interface for 'Event Detections, version 1.6'. The interface is divided into several sections:

- Organizations:** A list of organizations including 'Cisco' and multiple instances of 'East Coast Board Store'.
- Event Selection:** A search bar and a list of event types such as 'API Critical', 'API Major', 'Trap Example 1', 'Trap Example 2', 'ADIC Global Status Failed', 'ADIC Global Status OK', 'ADIC Global Status Unknown', and 'ADIC Tape Library Degraded'.
- Report Options:** A section with 'Show details' checked, 'Separated by' set to 'Event Name', and 'Optional Columns' including 'Device ID', 'Organization', 'Device Name', 'IP Address', 'Severity', 'Detection Count', 'First Occurrence', and 'Last Detected'.
- Report Span:** A section with 'Daily', 'Weekly', and 'Monthly' radio buttons, 'Monthly' selected, 'Starting' set to 'This month', a date range of '2015 / May / 1', and a 'Duration' of '1 month'.
- Output format:** A dropdown menu set to 'Web page (.html)'.
- Buttons:** 'Edit', 'Reset', 'Guide', and 'Generate' buttons are visible.

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.



Unique Event Detections

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

The screenshot shows the 'Run Quick Report' interface for 'Unique Event Detections, version 1.2'. The interface is divided into several sections:

- Device Selection:** Includes a checkbox for 'All devices' (checked), a list of organizations (AWS_temp_test, chris_org, em4583_org), a 'Select individual devices' checkbox, and a list of devices by organization.
- Separated by:** Includes checkboxes for 'Organization' (checked), 'Device group', and 'Device'.
- Report Span:** Includes radio buttons for 'Daily', 'Weekly', and 'Monthly' (selected). It also has a 'Starting' dropdown (This month), a date selector (2015 / May / 1), a 'Duration' dropdown (1 month), and a 'Timezone' dropdown (UTC).
- Device Group Selector:** Includes a checkbox for 'All Device Groups' (checked) and a list of device groups.
- Event Types:** Includes a checkbox for 'All events' (checked) and a list of event types (ADIC Global Status Failed, ADIC Global Status OK, ADIC Global Status Unknown, ADIC Tape Library Degraded).
- Report Sections:** Includes radio buttons for 'Both', 'Details Only', and 'Totals Only'.
- Output format:** A dropdown menu set to 'Web page (html)'. A 'Generate' button is located at the bottom right.

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

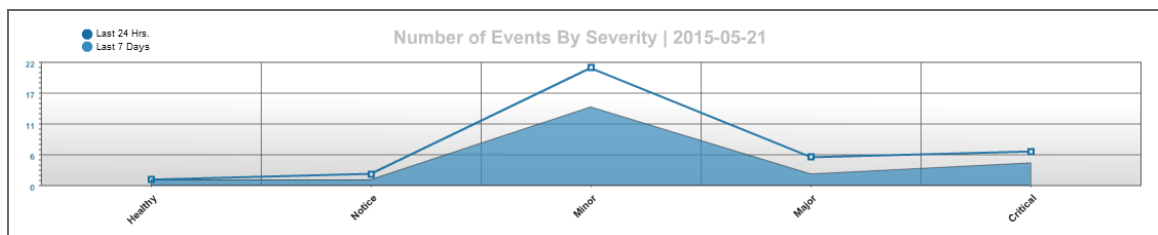
The **Event Overview** page includes a **Select Date** drop-down list in the upper right of the page. This drop-down allows you to define the date for the reports on this page.

- **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

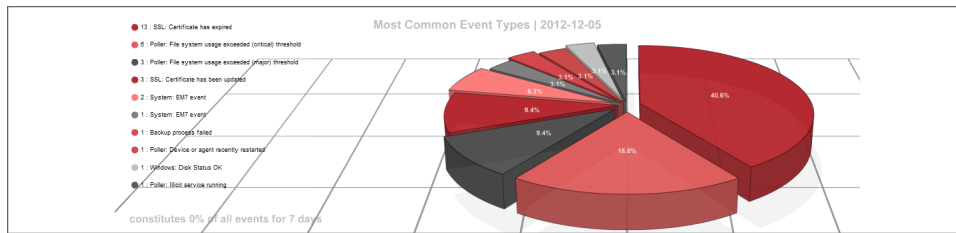
This graph displays event distribution by severity for the last 24 hours and for the last 7 days.



- 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

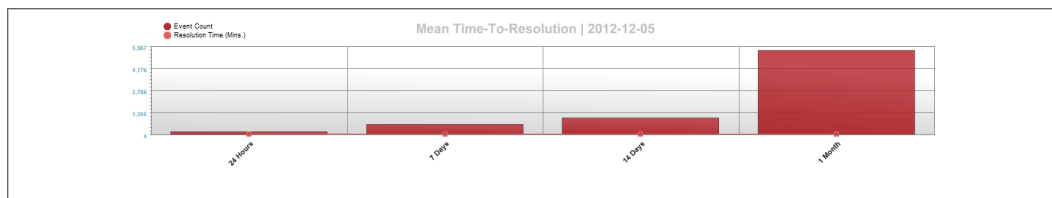
This pie graph displays the ten most frequently occurring events for the last seven days.



- 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.

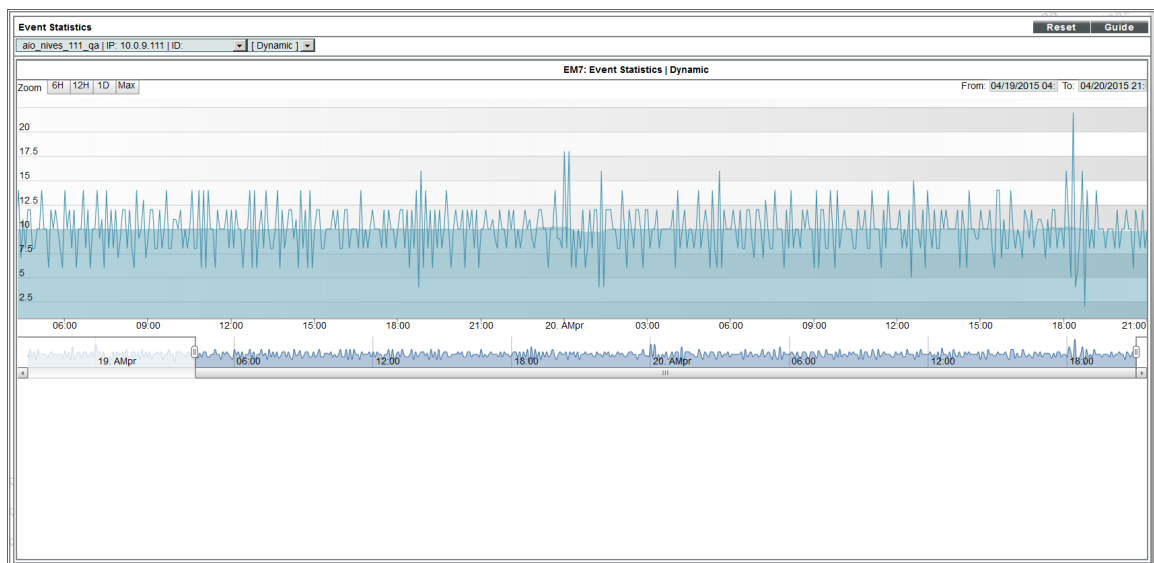
Fields

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.

Chapter



10

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 the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

Data Retention Settings that Affect Events	176
System Settings that Affect Events	177
System Settings that Affect Event Tickets	178

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:

Section	Setting	Value	Current
System Data Retention	Audit Logs	3 months*	Current: 3 months*
	Event Logs	3 months*	Current: 3 months*
	Access Logs	12 months*	Current: 12 months*
	System Logs	31 days	Current: 31 days
	Collector Unit Data Buffer	2 days	Current: 2 days
Collection Data Retention	Raw Performance Data	7 days	Current: 7 days
	Hourly Rollup Performance Data	120 days	Current: 120 days
	Daily Rollup Performance Data	24 months*	Current: 24 months*
	Configuration Data	7 days	Current: 7 days
	Journal Data	60 days	Current: 60 days
	Bandwidth Data	31 days	Current: 31 days
	Hourly Rollup Bandwidth Data	120 days	Current: 120 days
	Daily Rollup Bandwidth Data	24 months*	Current: 24 months*
	Bandwidth Billing Data	24 months*	Current: 24 months*
	Device Logs Age	90 days	Current: 90 days
	Device Logs Max	10000 records	Current: 10000 records
	Raw ITSM Data	31 days	Current: 31 days
	ITSM Service Metrics Data	30 days	Current: 30 days
	Hourly Rollup ITSM Service Metrics Data	120 days	Current: 120 days
	Daily Rollup ITSM Service Metrics Data	12 months*	Current: 12 months*
	ITSM Key Metrics Data	120 days	Current: 120 days
	Hourly Rollup ITSM Key Metrics Data	365 days	Current: 365 days
Daily Rollup ITSM Key Metrics Data	24 months*	Current: 24 months*	
Subscription Data Retention	Subscriber Device Configuration Data	6 months*	Current: 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' configuration page. On the right side, under the 'Event Clearing Mode' dropdown menu, the option 'Clear All in Group' is selected and highlighted with a red rectangular box. Other settings include 'Event Console Ticket Life Ring Button Behavior' set to 'Create / View EM7 Ticket' and 'Automatic Ticketing Emails' set to 'Enabled'.

- **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 (or the **Event Console** page in the classic SL1 user interface).

System Settings that Affect Event Tickets

The behavior of the *Create Ticket* option on the **Events** page (or the life-ring icon (🔔) in the **Event Console** in the classic SL1 user interface) is determined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface. To change this behavior:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Select from the following options in the **Event Console Ticket Life Ring Button Behavior** field:
 - *Create/View EM7 Ticket.* When you select the *Create Ticket* option or click the life-ring icon (🔔) for an event, 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 or click the life-ring icon (🚨) 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 or click the life-ring icon (🚨) 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](#).

© 2003 - 2022, 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