



---

# Events

SL1 version 8.10.0

---

# Table of Contents

<b>What is an Event?</b> .....	<b>1</b>
What is an Event? .....	1
How Are Events Triggered? .....	1
Viewing Events .....	3
Event Correlation .....	3
Defining Events .....	4
Event States .....	4
<b>Viewing Events</b> .....	<b>6</b>
Overview .....	6
Viewing All Events from the Event Console .....	7
Events that Are Not Displayed in the Event Console .....	9
Information About Each Displayed Event .....	10
Searching and Filtering the List of Events .....	12
Global Search Field .....	12
Filter While You Type .....	14
Advanced Filter .....	16
Special Characters .....	19
Custom View .....	22
Event Throttling .....	23
Viewing Events for a Single Device .....	24
Viewing Events for a Single Organization .....	25
Viewing Event Details .....	28
Customizing the Display in the Event Console .....	31
Account Preferences .....	31
Event Console Preferences .....	36
Hiding the Header Bar .....	39
Event Masks .....	40
<b>Responding to Events</b> .....	<b>41</b>
Overview .....	41
Acknowledging One or More Events .....	42
Adding a Note About an Event .....	43
Adding a Note to Multiple Events .....	44
Clearing One or More Events .....	46
Suppressing an Event on a Single Device .....	47
Suppressing an Event On Multiple Devices .....	48
Unsuppressing an Event .....	50
Unsuppressing All Instances of an Event .....	51
Disabling an Event .....	52
Enabling an Event .....	53
<b>Events and Tickets</b> .....	<b>55</b>
Overview .....	55
Creating a Ticket from the Event Console .....	56
Event Ticket Behavior Settings .....	58
Integrating Events with External Tickets .....	59
External Tickets in the Event Console .....	59
Using Run Book Automation to Populate the ScienceLogic Database with Values from External Tickets .....	60
Aligning an External Ticket with Multiple Events .....	61
<b>Event Correlation and Parent and Child Events</b> .....	<b>63</b>
Overview .....	63
Event Correlation .....	64

Defining Parent and Child Devices .....	64
Device Categories that Don't Support Children Devices .....	66
Defining Suppressing and Suppressible Events .....	66
Event Categories .....	69
Assigning an Event Category to an Event .....	71
Creating an Event Category .....	72
Editing an Event Category .....	72
Viewing the List of Event Categories .....	74
Filtering the List of Event Categories .....	75
Special Characters .....	76
Deleting One or More Event Categories .....	79
<b>Defining and Editing Event Policies .....</b>	<b>81</b>
Overview .....	81
Viewing the List of Event Policies .....	83
Filtering the List of Event Policies .....	85
Special Characters .....	87
Defining an Event Policy .....	91
Defining Basic Event Parameters in the Policy Tab .....	92
Defining Pattern Matching and Advanced Behavior in the Advanced Tab .....	95
Defining Event Suppressions in the Suppressions Tab .....	103
Defining an Event Policy for a Specific Interface .....	104
Defining Custom Severity for an Interface .....	106
Editing an Event Policy .....	108
Best Practices for Event Definitions .....	110
<b>Event Notification and Event Automation .....</b>	<b>112</b>
Overview .....	112
Automation Policies .....	112
Action Policies .....	113
Creating Automation Policies and Action Policies .....	114
<b>Events from Email .....</b>	<b>115</b>
Overview .....	115
Configuring Events from Email .....	115
<b>RSS Feeds and Events .....</b>	<b>116</b>
Overview .....	116
Viewing Events with an RSS Feed .....	116
Defining a Custom RSS Feed .....	116
Editing a Custom RSS Feed .....	119
Viewing a Custom RSS Feed .....	120
Defining an External RSS Feed to Trigger Events .....	121
Viewing the List of Monitored RSS Feeds .....	122
Defining an RSS Feed to Monitor .....	122
Editing a Monitored RSS Feed .....	123
Viewing Articles from an RSS Feed .....	124
Performing Administrative Tasks on One or More Monitored RSS Feeds .....	126
<b>Reports for Events .....</b>	<b>128</b>
Overview .....	128
Event Statistics in the Event Console page .....	128
Event Statistics for a Single Device .....	132
Event Reports in the Reports tab .....	135
Event Clear Map Report .....	136
Event Detections Report .....	138
Unique Event Detections Report .....	140

Event Overview Report .....	143
Setting the Date for Reports .....	143
Number of Events by Severity .....	143
Most Common Event Types .....	144
Mean Time-to-Resolution .....	144
Event Statistics .....	144
Defining the Date Range .....	145
Fields .....	145
The Graph .....	145
<b>Settings that Affect Events .....</b>	<b>147</b>
Overview .....	147
Data Retention Settings that Affect Events .....	147
System Settings that Affect Events .....	148
System Settings that Affect Event Tickets .....	150

## What is an Event?

---

### 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 **Event Console** page, under the **[Events]** tab.

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

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

The ScienceLogic platform includes pre-defined events for the most commonly encountered conditions on the most common platforms. 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?

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

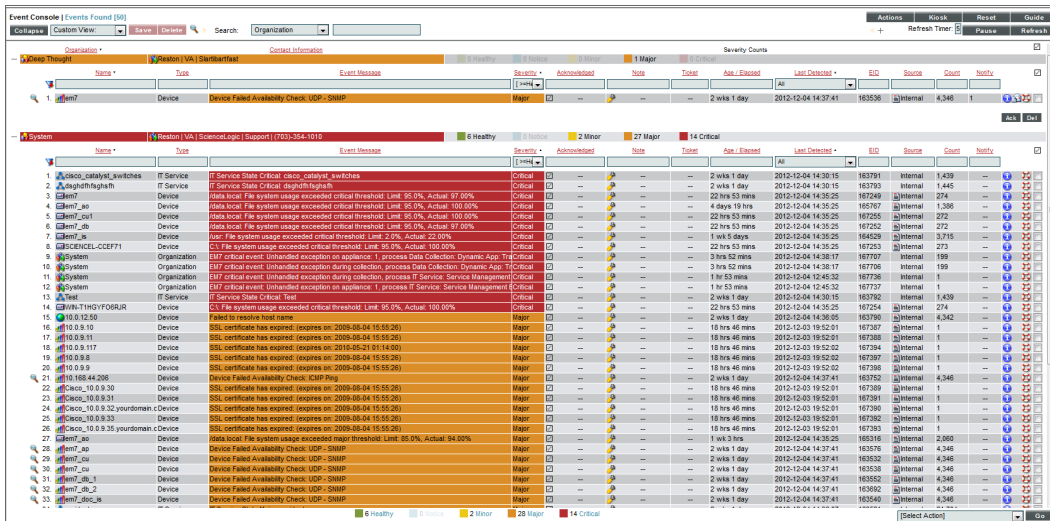
The ScienceLogic platform includes logic that correlates and groups (rolls-up) related logs and messages into a single event. The platform includes pre-defined events for many syslog, internal, trap, and dynamic messages.

The ScienceLogic platform generates events by collecting log messages from the following sources:

- **Syslog**. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices like MoMs. A syslog is an unsolicited message from a device to the ScienceLogic platform. Syslog is a standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools. For more information on sylogs, see the manual **Syslogs and Traps**.
- **Internal**. Message is generated by a ScienceLogic process. The message is about the ScienceLogic system itself, instead of the devices that the ScienceLogic 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 the ScienceLogic platform. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device. For more information on traps, see the manual **Syslogs and Traps**.
- **Dynamic**. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell the ScienceLogic platform how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. The ScienceLogic platform examines each new message in the device log and determines if the message matches an event definition. If it does, the platform generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the ScienceLogic system inserts a message in the associated device's log files, and the ScienceLogic system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
- **Email**. Message is generated by an email message sent to the platform. For more information on generating events with email messages, see the [Events from Email](#) chapter.
- **API**. Message was generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the manual **Run Book Automation**. For more information on snippet Dynamic Applications, see the manual **Snippet Dynamic Application Development**. For more information on the ScienceLogic API, see the manual **Using the ScienceLogic API**.

# Viewing Events

The **Event Console** page 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. You can also create a ticket based upon an event.



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.

You can use the **Organizational Administration** panel and the **Organizational Events** page to view a list of events for a single organization. The events are displayed in a page that is similar to the **Event Console** page, but displays only events that occurred on entities in the selected organization.

For details on viewing events (in the **Event Console** page and for a single device), see the chapter on [viewing events](#). For details on viewing events for an organization, see the manual [Organizations and Users](#).

# Event Correlation

In the ScienceLogic platform, 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 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. In addition to creating parent-child relationships between devices and between events, you can define event categories that allow the ScienceLogic platform to more efficiently align events.

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

## Defining Events

The **Event Policy Manager** page displays a list of all event policies in the ScienceLogic platform. This page also allows you to define new event definitions and edit existing event definitions.

Event Policy Name	Type	State	B-Flag	Severity	Weight	ID	Enable	Time	Threshold	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	Major	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	1284	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
7. AKCP: DC Voltage High Warning	Syslog	Enabled	Yes	Major	0	1289	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
8. AKCP: DC Voltage sensor High Critical	Syslog	Enabled	Yes	Critical	0	1287	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
9. AKCP: DC Voltage sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1286	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	1282	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
14. AKCP: Humidity High Warning	Syslog	Enabled	Yes	Major	0	1285	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
15. AKCP: Humidity Low Warning	Syslog	Enabled	Yes	Major	0	1286	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
16. AKCP: Smoke Detector Alert	Syslog	Enabled	Yes	Critical	10	1283	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	1288	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
20. ABeon: New Flash Enabled	Dynamic	Enabled	Yes	Notice	0	36	30 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
21. ABeon: Primary Power Supply Failure	Dynamic	Enabled	Yes	Major	0	32	90 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
22. ABeon: Primary Power Supply Healthy	Dynamic	Enabled	Yes	Healthy	0	33	15 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
23. ABeon: Redundant Power Supply Failure	Dynamic	Enabled	Yes	Major	0	34	90 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
24. ABeon: 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	Major	0	27	60 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--

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

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

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

## Event States

Although not displayed in the **Event Console** page or the the user interface, events have four distinct states:

- **Active**. The ScienceLogic platform has created an event record. The event might appear in the **Event Console** page or it might be masked or nested as a topology event, and therefore not appear in the **Event Console** page.
- **Masked**. The event record is Active and appears in the **Event Console** page as a masked event. In the **Event Console** 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 **Event Console** page. 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.
- **Prepending**. An alert triggered the event, but additional criteria must be met before the ScienceLogic platform creates an event record.

---

# Chapter

# 2

## Viewing Events

2

---

### Overview

You can view a list of all events in the ScienceLogic platform or view a list of events for a single device. This chapter describes how to perform both tasks.

This chapter also describes how to customize the display in the **Event Console** page.

# Viewing All Events from the Event Console

To view a list of all active events, select 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**.

The screenshot displays the Event Console interface with the following data:

Name	Type	Event Message	Severity	Acknowledged	Note	Ticket	Age / Elapsed	Last Detected	EID	Source	Count	Notify
1. iam7	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163556	Internal	4,346	1
1. System	System	System	6 Healthy	2 Minor	27 Major	14 Critical						
1. cliop_cahygl_Lwatches	IT Service	IT Service Status Critical: cliop_cahygl_Lwatches	Critical	☐	---	---	2 wks 1 day	2012-12-04 14:30:15	163793	Internal	1,439	1
2. cliop_cahygl_spath	IT Service	IT Service Status Critical: cliop_cahygl_spath	Critical	☐	---	---	2 wks 1 day	2012-12-04 14:30:15	163793	Internal	1,445	1
3. cliop7_ao	Device	Data local File system usage exceeded critical threshold: Limit: 95.0%, Actual: 97.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167249	Internal	274	1
4. cliop7_ao	Device	Data local File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	4 days 19 hrs	2012-12-04 14:35:25	167677	Internal	1,396	1
5. cliop7_ao1	Device	Data local File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167256	Internal	272	1
6. cliop7_ao	Device	Data local File system usage exceeded critical threshold: Limit: 95.0%, Actual: 97.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167252	Internal	272	1
7. cliop7_ao	Device	Java: File system usage exceeded critical threshold: Limit: 2.0%, Actual: 22.00%	Critical	☐	---	---	1 wk 5 days	2012-12-04 14:35:25	164529	Internal	3,715	1
8. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167253	Internal	273	1
9. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167253	Internal	273	1
9. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167254	Internal	274	1
10. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167254	Internal	274	1
11. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167254	Internal	274	1
12. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167254	Internal	274	1
13. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167254	Internal	274	1
14. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167254	Internal	274	1
15. cliop7_ao	Device	File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☐	---	---	22 hrs 53 mins	2012-12-04 14:35:25	167254	Internal	274	1
16. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:01	167387	Internal	1	1
17. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:01	167388	Internal	1	1
18. cliop7_ao	Device	SSL certificate has expired: (expires on: 2010-05-21 01:14:00)	Major	☐	---	---	19 hrs 46 mins	2012-12-03 19:52:02	167384	Internal	1	1
19. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:02	167387	Internal	1	1
20. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:02	167388	Internal	1	1
21. cliop7_ao	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163552	Internal	4,346	1
22. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:01	167389	Internal	1	1
23. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:01	167391	Internal	1	1
24. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:01	167390	Internal	1	1
25. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:01	167392	Internal	1	1
26. cliop7_ao	Device	SSL certificate has expired: (expires on: 2009-08-04 15:55:26)	Major	☐	---	---	18 hrs 46 mins	2012-12-03 19:52:01	167393	Internal	1	1
27. cliop7_ao	Device	Data local File system usage exceeded major threshold: Limit: 95.0%, Actual: 94.00%	Major	☐	---	---	1 wk 3 hrs	2012-12-04 14:35:25	165516	Internal	2,060	1
28. cliop7_ao	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163552	Internal	4,346	1
29. cliop7_ao	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163552	Internal	4,346	1
30. cliop7_ao	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163553	Internal	4,346	1
31. cliop7_ao	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163552	Internal	4,346	1
32. cliop7_ao	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163682	Internal	4,346	1
33. cliop7_ao	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	---	---	2 wks 1 day	2012-12-04 14:37:41	163540	Internal	4,346	1

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 does not affect service but about which users should be aware.
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. For more details on the **Account Preferences** page and the **Event Console Preferences** page, see the section on [Customizing the Display in the Event Console](#).

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 the ScienceLogic platform, 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, the platform does not display each occurrence in the **Event Console**. Instead, the platform 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 chapter on [Responding to Events](#).

- **Topology Events.** In the ScienceLogic platform, [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 chapter 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 in this chapter 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 the ScienceLogic platform). 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 last 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 the ScienceLogic platform.
- **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 the ScienceLogic platform.
  - *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.
  - *ScienceLogic agent.* Message is generated by log file messages collected by the ScienceLogic agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the **Monitoring Using the ScienceLogic agent** 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 ScienceLogic 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**), the ScienceLogic platform 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, the ScienceLogic platform 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.

## Searching and Filtering the List of Events

The **Event Console** page 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 the ScienceLogic platform (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.

## 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. The ScienceLogic platform 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 the platform).
  - *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 the ScienceLogic platform.
  - *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. The ScienceLogic platform 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. The ScienceLogic platform 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. The ScienceLogic platform 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 columns 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.

## 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, the ScienceLogic platform 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, the ScienceLogic platform will not match a substring unless you use a special character.

### String and Numeric

- , (comma). Specifies an "OR" operation. Works for string and numeric values. For example:  
"dell, micro" matches all values that contain the string "dell" OR the string "micro".
- & (ampersand). Specifies an "AND" operation. Works for string and numeric values. For example:  
"dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.
- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:  
"!dell" matches all values that do not contain the string "dell".  
"! ^ micro" would match all values that do not start with "micro".  
"!fer\$" would match all values that do not end with "fer".  
"! ^ \$" would match all values that are not null.  
"! ^" would match null values.  
"! \$" would match null values.  
"!\*" would match null values.  
"happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

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

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

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

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

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

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

"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.

## Additional Examples

- "aio\$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo\$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!O\$". Matches only text that does not end with "O".
- "!^silo\$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!. Matches null values, typically represented as "--" in most pages.
- "!. Matches null values, typically represented as "--" in most pages.

- `!^$`. Matches all text that is not null.
- `silolaggr`. Matches text that contains the characters "silo" and also text that does not contain "aggr".
- `silol02laggr`. Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- `silol02laggr!01`. Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- `^s*i!*o$`. Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would match.
- `!^s*i!*o$`. Matches all text that does not that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would not match.
- `!vol&!silo`. Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- `!vol&02`. Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol" and it does contain "02".
- `aggr,lvol&02`. Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- `aggr,lvol&!infra`. Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- `**`. Matches all text.
- `!*`. Matches null values, typically represented as "--" in most pages.
- `silol`. Matches text that contains "silo".
- `!silol`. Matches text that does not contain "silo".
- `!^silol$`. 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".

## 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.

---

## Event Throttling

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

When the ScienceLogic platform 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 the ScienceLogic platform throttles messages, the platform also triggers events:

- **Event with a Severity of Critical and the message "Inbound Message Flood"**. This event is triggered when a single IP exceeds the threshold of syslog messages or trap messages at least once per minute for the last ten minutes. The default threshold is 100 messages per second.
- **Event with a Severity of Notice and the message "Inbound Message Spikes"**. This event is triggered when a single IP exceeds the threshold of syslog messages or trap message. The default threshold is 100 messages per second.

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

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

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

**NOTE:** The ScienceLogic platform does not support message throttling on IPv6 devices monitored by CentOS5 Data Collectors.

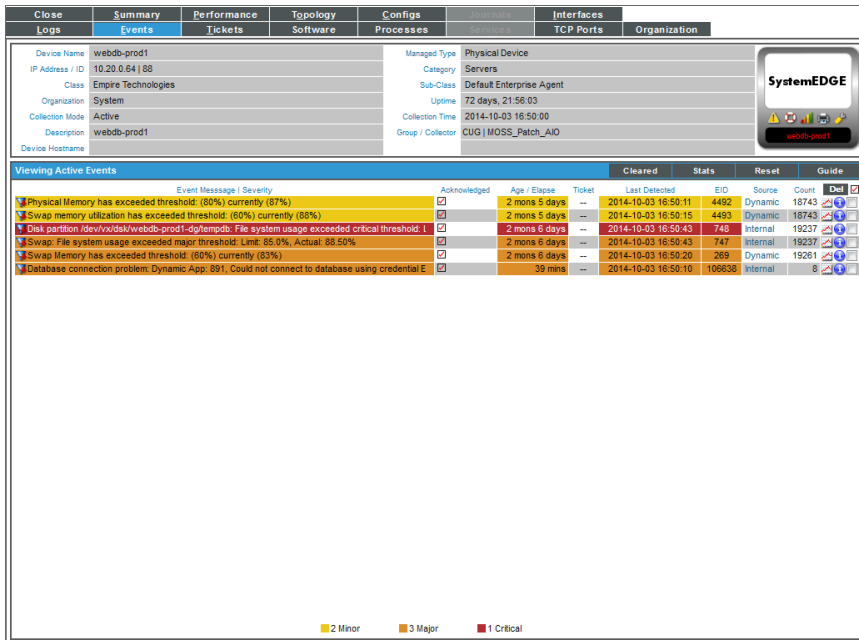
# Viewing Events for a Single Device

To view a list of events for a single device, 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 last 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 the ScienceLogic platform.
- **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 the ScienceLogic platform.
  - *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 the ScienceLogic platform is associated with an organization. Each occurrence of an event is grouped by organization (the organization associated with the device where the event occurred or the organization associated with the policy that generated the event).

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

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

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization with associated events that you want to view.

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	em7admin	2012-03-15 18:18:48	
2. PDC - Servers	Washington	DC		--	--	1	11	--	4	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	rskint@super.com	1	--	--	5	em7admin	2012-03-13 19:54:52	
5. PHOC	Reston	VA	Mill, Griffin	704-354-1111	gmill@super.com	1	--	--	4	em7admin	2012-03-13 19:52:57	
6. QA	Reston	--	--	--	--	1	2	--	1	em7admin	2012-02-22 22:39:54	
7. System	Reston	VA	Support, ScienceLogic	(703)-354-1010	support@sciencelogic.com	5	27	3	0	em7admin	2007-12-01 15:51:17	




3. If a value appears in the *Events* column, click the event icon (⚠).

4. The **Organizational Events** page appears for the organization.

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%	<input checked="" type="checkbox"/>	2012-05-01 18:40:08	--	--	2012-05-02 11:55:07	Internal	208	
10.100.100.8	backup_complete	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	2012-04-20 18:22:13	--	--	2012-05-02 11:52:13	Internal	3391	
LAB-2010-SPLAB	Device Failed Availability Check: UDP - SNMP	<input checked="" type="checkbox"/>	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)	<input checked="" type="checkbox"/>	2012-02-22 20:25:30	--	--	2012-02-27 16:35:25	Dynamic	1385	
10.100.100.28	Network latency exceeded threshold: No Response	<input checked="" type="checkbox"/>	2012-04-20 18:22:13	--	--	2012-05-02 11:52:13	Internal	3391	
10.2.2.18	System or agent has recently restarted	<input checked="" type="checkbox"/>	2012-04-20 18:20:17	--	--	2012-05-02 11:55:15	Internal	3367	
10.2.2.27	System or agent has recently restarted	<input checked="" type="checkbox"/>	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)	<input checked="" type="checkbox"/>	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)	<input checked="" type="checkbox"/>	2012-04-23 09:30:51	--	--	2012-05-02 11:55:40	Dynamic	2544	
10.100.100.28	Drive \\.\PHYSICALDRIVE0 now OK	<input checked="" type="checkbox"/>	2012-03-30 11:11:27	--	--	2012-03-30 11:11:27	Dynamic	1	

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 last 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 the ScienceLogic platform.

- **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 the ScienceLogic platform.
  - *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

You can view details about an event, suppress an event, and access the event policy from the **Event Information** page.

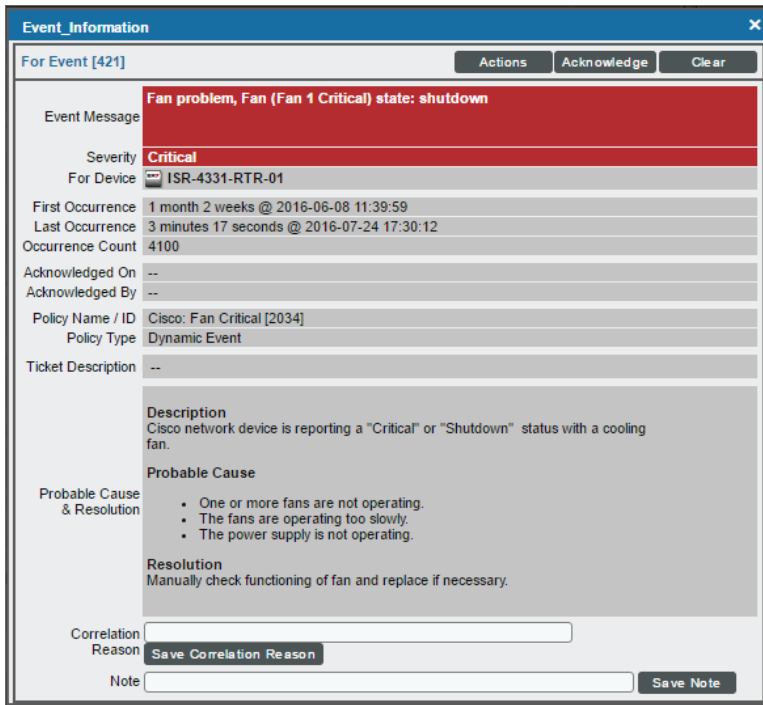
**NOTE:** To view the **Event Information** page, accounts of type "user" must be granted one or more access keys that includes the following access hook: Events/Event:View. Accounts of type "user" will then be able to view details for all events in the same organization as the user.

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

- **Event ID.** Unique ID for the event, generated by the ScienceLogic platform.
- **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 the ScienceLogic platform.
  - *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 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, the ScienceLogic platform 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 the ScienceLogic platform. The customizations that you choose will appear each time you log in to the platform. They will not affect how the platform 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):** Contains dropdown menus for 'Default Page' (set to 'Event Console'), 'Theme' (set to 'ScienceLogic: White + Blue Tilebars'), 'Page Refresh Rate' (set to '5 Minutes'), 'Page Result Count' (set to '25'), 'Table Row Height' (set to 'Small'), 'Default Severity Filter' (set to 'Healthy'), 'Preferred IF Label' (set to 'Interface Alias'), 'Default Interface Graph Display' (set to '% Utilization'), 'Default Date Format' (set to '22/05/2015'), and 'Date Format String' (set to 'Y-m-d H:i:s').
- Middle Column (Checkboxes):** Contains several options with 'Check = Enabled' status: '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 (Column Selection):** Contains three lists of columns for different consoles: 'Event Console Columns', 'Ticket Console Columns', and 'Device Manager Columns'. Each list has a scrollable selection area.

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 the platform. The **Interface Settings** pane contains the following fields:
- **Default Page.** Select the page that automatically appears by default when you log in to the ScienceLogic platform. Options include:
    - *None.* The platform will display the ScienceLogic logo when you log in.
    - *Inbox.* The platform will display the **[Inbox]** tab when you log in.
    - *Event Console.* The platform will display the **Event Console** when you log in.
    - *Ticket Console.* The platform will display the **Ticket Console** when you log in.
    - *Knowledge Base.* The platform will display the **Knowledge Base Home** page when you log in.

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

- *Device Views*. The platform will display the **Device Group Map** page (Views > Device Maps > Device Groups) when you log in.
- *Dashboard*. The platform 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 Systems > Customize > Themes page.
- **Page Refresh Rate**. Select how often **Events**, **Tickets**, and **Views** pages in the ScienceLogic platform 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 the ScienceLogic platform.
- **Date Format String.** Select the date format for use throughout the ScienceLogic platform. 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 the ScienceLogic platform 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 the ScienceLogic platform 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.

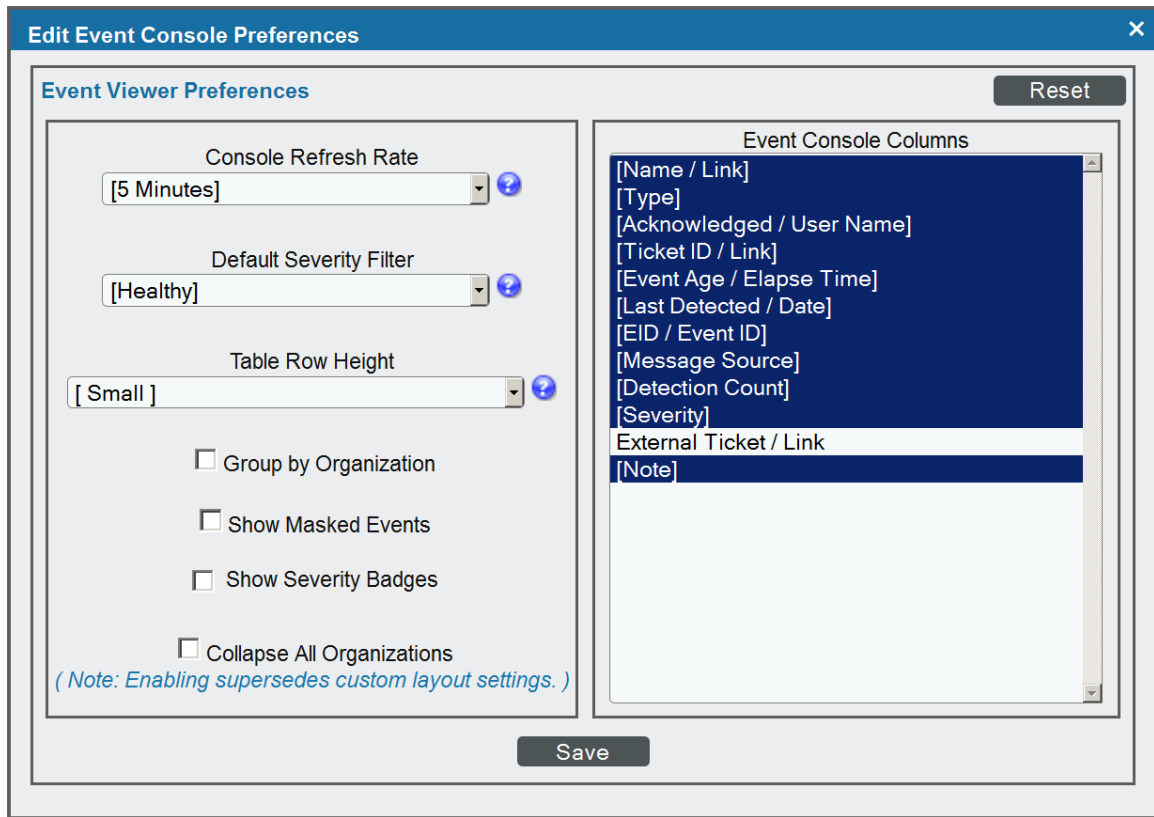
**NOTE:** To access the **Event Console Preferences** page, accounts of type "user" must be granted one or more access keys that includes the following access hook: Events/Event:View. Accounts of type "user" will then be able to view and edit settings in the **Event Console Preferences** page. For more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



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 the ScienceLogic platform 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's a navigation bar with tabs for Inboxes, Dashboards, Views, Events, Tickets, Knowledge, Reports, Registry, System, and Preferences. The 'Events' tab is active. Below the navigation bar, there's a search and filter section. The main area shows a list of events with columns: Name, Type, Event Message, Severity, Acknowledged, Note, Ticket, Age, Elapsed, Last Detected, SID, Source, Count, and Notify. A red box highlights a small arrow icon in the top right corner of the event list area, which is used to hide the header bar.

Name	Type	Event Message	Severity	Acknowledged	Note	Ticket	Age	Elapsed	Last Detected	SID	Source	Count	Notify
1. fem7	Device	Device Failed Availability Check: UDP - SNMP	Major				2 wks 1 day		2012-12-04 16:12:42	163538	Internal	4,365	1
1. Cisco_Catalyst_Switches	IT Service	Service State Critical: cisco_catalyst_switches	Critical				2 wks 1 day		2012-12-04 16:15:12	163791	Internal	1,446	
2. dghdfhfgsh	IT Service	Service State Critical: dghdfhfgsh	Critical				2 wks 1 day		2012-12-04 16:15:12	163793	Internal	1,452	
3. fem7	Device	Data local: File system usage exceeded critical threshold: Limit: 95.0%, Actual: 97.00%	Critical				1 day 32 mins		2012-12-04 16:15:40	167249	Internal	294	
4. fem7_ao	Device	Data local: File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical				4 days 21 hrs		2012-12-04 16:15:40	165767	Internal	1,406	
5. fem7_cvt	Device	Data local: File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical				1 day 32 mins		2012-12-04 16:15:40	167255	Internal	292	
6. fem7_db	Device	Data local: File system usage exceeded critical threshold: Limit: 95.0%, Actual: 97.00%	Critical				1 day 32 mins		2012-12-04 16:15:40	167252	Internal	292	
7. fem7_eh	Device	Data local: File system usage exceeded critical threshold: Limit: 2.0%, Actual: 22.00%	Critical				1 wk 5 days		2012-12-04 16:15:40	164828	Internal	3,735	
8. SCENKEL_CCEFT1	Device	C:\ File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical				1 day 32 mins		2012-12-04 16:15:40	167253	Internal	293	
9. System	Organization	EMT critical event: Unhandled exception on appliance: 1. process Data Collection: Dynamic App: Tr	Critical				5 hrs 30 mins		2012-12-04 16:17:08	167707	Internal	288	
10. System	Organization	EMT critical event: Unhandled exception during collection: process Data Collection: Dynamic App	Critical				5 hrs 30 mins		2012-12-04 16:17:08	167706	Internal	288	
11. Test	IT Service	IT Service State Critical: Test	Critical				2 wks 1 day		2012-12-04 16:15:12	163792	Internal	1,446	
12. WNI-THGYFOBJR	Device	C:\ File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical				1 day 32 mins		2012-12-04 16:15:40	167254	Internal	294	
13. 10.0.0.20	Device	Failed to resolve host name	Major				2 wks 1 day		2012-12-04 16:16:07	163790	Internal	4,362	
14. 10.0.0.10	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:01	167387	Internal	1	
15. 10.0.0.11	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:01	167388	Internal	1	
16. 10.0.0.117	Device	SSL certificate has expired: (expires on 2010-05-21 01:14:00)	Major				20 hrs 25 mins		2012-12-03 19:52:02	167394	Internal	1	
17. 10.0.0.8	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:02	167387	Internal	1	
18. 10.0.0.9	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:02	167388	Internal	1	
19. 10.188.44.206	Device	Device Failed Availability Check: ICMP Ping	Major				2 wks 1 day		2012-12-04 16:12:42	163532	Internal	4,365	
20. Cisco_10.0.9.30	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:01	167389	Internal	1	
21. Cisco_10.0.9.31	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:01	167391	Internal	1	
22. Cisco_10.0.9.32.yourdomain	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:01	167390	Internal	1	
23. Cisco_10.0.9.33	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:01	167392	Internal	1	
24. Cisco_10.0.9.35.yourdomain	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:01	167393	Internal	1	
25. fem7_ao	Device	Data local: File system usage exceeded major threshold: Limit: 85.0%, Actual: 94.00%	Major				1 wk 5 hrs		2012-12-04 16:15:40	165916	Internal	2,080	
26. fem7_ap	Device	Device Failed Availability Check: UDP - SNMP	Major				2 wks 1 day		2012-12-04 16:12:42	163537	Internal	4,365	
27. fem7_cu	Device	Device Failed Availability Check: UDP - SNMP	Major				2 wks 1 day		2012-12-04 16:12:42	163532	Internal	4,365	
28. fem7_db_1	Device	Device Failed Availability Check: UDP - SNMP	Major				2 wks 1 day		2012-12-04 16:12:42	163552	Internal	4,365	
29. fem7_db_2	Device	Device Failed Availability Check: UDP - SNMP	Major				2 wks 1 day		2012-12-04 16:12:42	163552	Internal	4,365	
30. fem7_db_3	Device	Device Failed Availability Check: UDP - SNMP	Major				2 wks 1 day		2012-12-04 16:12:42	163552	Internal	4,365	
31. fem7_db_4	Device	Device Failed Availability Check: UDP - SNMP	Major				2 wks 1 day		2012-12-04 16:12:42	163540	Internal	4,365	
32. esri-test	IT Service	IT Service State Major: esri-test	Major				2 wks 1 day		2012-12-04 16:17:08	163321	Internal	21,003	
33. Juniper_10.0.9.43	Device	SSL certificate has expired: (expires on 2009-08-04 15:55:26)	Major				20 hrs 25 mins		2012-12-03 19:52:02	167396	Internal	1	

---


## Event Masks

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.

2

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, the platform 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

3

---

### Overview

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

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

This chapter describes all of these possible responses to events.

# Acknowledging One or More Events

The ScienceLogic platform 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**.

To acknowledge a single event:

1. Go to the [Events] tab.
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 Name	Device	Description	Acknowledged	Details
1. @HUB-1770R0R0R	Device	File system usage exceeded major threshold. Limit: 90.0%, Actual: 100.0%	☑ jdoe	10/25/2012 10:08:56 1598 Internal 12
2. @HUB-1770R0R0R	Device	File system usage exceeded threshold. (90%) currently (100%)	☐	10/25/2012 10:08:56 1598 Internal 12
3. @HUB-1770R0R0R	Device	File system usage exceeded major threshold. Limit: 90.0%, Actual: 90.0%	☐	10/25/2012 10:08:56 1598 Internal 12
4. @HUB-1770R0R0R	Device	File system usage exceeded major threshold. Limit: 90.0%, Actual: 90.0%	☐	10/25/2012 10:08:56 1598 Internal 12
5. @HUB-1770R0R0R	Device	File system usage exceeded major threshold. Limit: 90.0%, Actual: 90.0%	☐	10/25/2012 10:08:56 1598 Internal 12

To acknowledge multiple events:

1. In the **Event Console** page, select the checkbox in the far right column for each event that you want to acknowledge.

2. Acknowledge the event(s) by doing one of the following:

- Click the **[Ack]** button.
- From the **Select Action** drop-down list, select **Acknowledge**, then click the **[Go]** button.

3. For each acknowledged event, a 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.

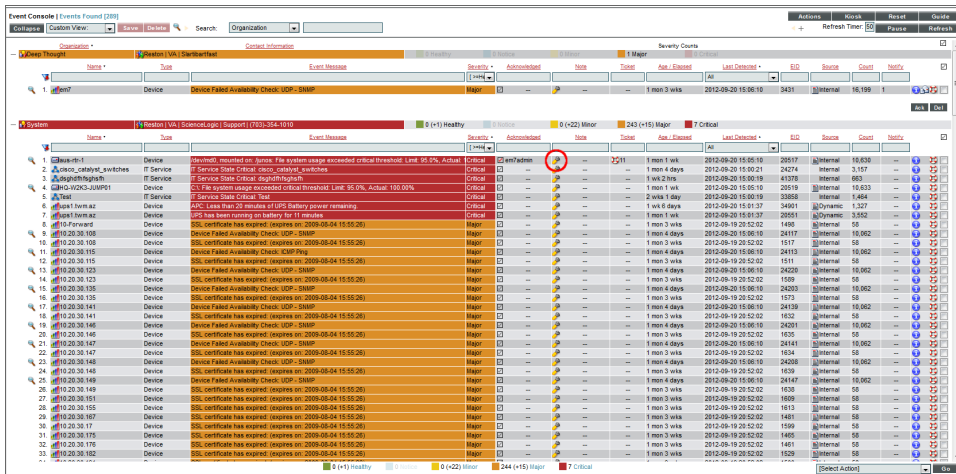
## Adding a Note About an Event

You can add brief notes to an event in the **Event Console** page. Each note will appear in the **Note** column for an event. The ScienceLogic platform 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:

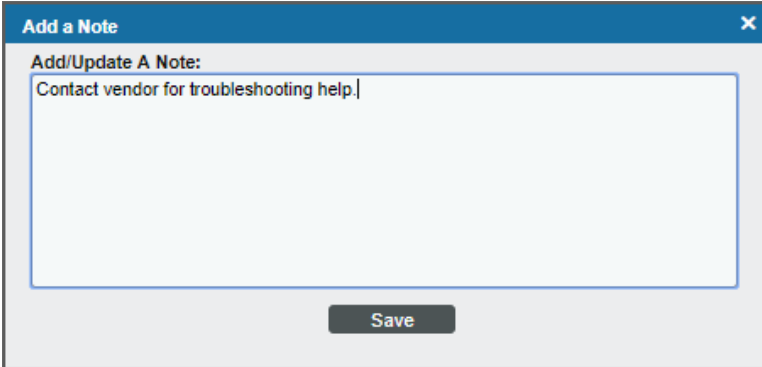
1. In the **Event Console** page, find the event to which you want to add a note.
2. In the **Note** column for that event, click on the wrench icon ()



Name	Status	Event Message	Severity	Acknowledged	Note	Date	Actions
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Health monitored on /dev/sda: File system usage exceeded critical threshold: Limit: 95.0%, Actual: 95.0%	Critical		Critical			1 mon 1 wk	[Ack] [Go] [Wrench]
Service State Critical: cisco_catalyst_switches	Critical		Critical			1 mon 4 days	[Ack] [Go] [Wrench]
Service State Critical: cisco_catalyst_switches	Critical		Critical			1 wk 2 wks	[Ack] [Go] [Wrench]
File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.0%	Critical		Critical			1 mon 1 wk	[Ack] [Go] [Wrench]
Service State Critical: Dell	Critical		Critical			2 wks 4 days	[Ack] [Go] [Wrench]
APC: Less than 20 minutes of UPS Battery power remaining	Critical		Critical			1 wk 6 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: KMP Pkg	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]
Device Failed Availability Check: UOP - 30AP	Major		Major			1 mon 4 days	[Ack] [Go] [Wrench]
SSL certificate has expired (expires on: 2009-08-04 15:55:26)	Major		Major			1 mon 3 wks	[Ack] [Go] [Wrench]



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



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

---

## Adding a Note to Multiple Events

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. The ScienceLogic platform 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:

1. In the **Event Console** page, find the events for which you want to add a note and/or overwrite the existing note.
2. For each event that you want to add and/or edit a note, select the checkbox in the last column.



3. In the **Select Action** drop-down field, select **Add/Update Event Note**, then click the **[Go]** button.

Organization	Name	Type	Event Message	Severity	Acknowledged	Total	External Ticket	Age / Bypass	Last Detected	ED	Source	Count	Notify
System	10.20.0.108	Device	Physical Memory has exceeded threshold: (80% currently (100%))	Minor		273738		1 mon 1 day	26/12/2013 12:30:14 pm	Dynamic	8,353	379	
System	10.20.0.191	Device	Printer Tray B paper tray empty: Tray B	Minor		273444		1 mon 1 day	26/12/2013 12:31:25 pm	Dynamic	8,361	366	
System	10.20.0.191	Device	Physical Memory has exceeded threshold: (80% currently (100%))	Minor		273707		1 mon 1 day	26/12/2013 12:30:37 pm	Dynamic	8,352	368	
System	192.168.34.84	Device	App. 238, Snippet: 135 reported a collection problem (Explanation: (noSuchName) There is	Minor		273421		1 mon 1 day	26/12/2013 12:31:08 pm	Internal	2,783	450	
System	192.168.37.10	Device	Network latency exceeded threshold: No Response	Minor		273487		1 mon 1 day	26/12/2013 12:32:21 pm	Internal	20,877	20	
System	10.100.1010	Device	Printer Bypass Tray paper tray empty: Bypass Tray	Minor		273541		1 mon 1 day	26/12/2013 12:31:25 pm	Dynamic	1,393	356	
System	san.juranda.local	Device	Physical Memory has exceeded threshold: (80% currently (84%))	Minor		273423		1 day 10 hrs	26/12/2013 12:30:12 pm	Dynamic	499		
System	AVANDCT018	Device	App. 238, Snippet: 135 reported a collection problem (Explanation: (noSuchName) There is	Minor		273423		1 mon 1 day	26/12/2013 12:30:47 pm	Internal	2,784	400	
System	BSND10970R02.dns.dns	Device	CPU: 1 has exceeded threshold: (80% currently (9499%))	Minor		273812		1 mon 1 day	26/12/2013 12:30:17 pm	Dynamic	8,345	17	
System	SRL1.CS72CF	Device	Network latency exceeded threshold: No Response	Minor		273455		1 wk 21 hrs	26/12/2013 12:32:21 pm	Internal	5,677		
System	MS500-2	Device	CPU: 9 has exceeded threshold: (90% currently (50000%))	Minor		273805		1 mon 1 day	26/12/2013 12:30:28 pm	Dynamic	8,353	19	
System	CHWEB-01	Device	Physical Memory has exceeded threshold: (80% currently (95%))	Minor		273455		1 wk 5 days	26/12/2013 12:30:05 pm	Dynamic	3,653		
System	csco-qaent1000.0	Device	Network latency exceeded threshold: No Response	Minor		273455		1 mon 1 day	26/12/2013 12:32:21 pm	Internal	20,877	28	
System	csco_10.0.21.5	Device	CPU: 9 has exceeded threshold: (90% currently (2489%))	Minor		273455		15 hrs 7 mins	26/12/2013 12:30:28 pm	Dynamic	101		
System	csco_10.20.0.108.simpl	Device	PSLA: ECHO RTT 0 is above the minor threshold 999.999 ms, currently 683 ms	Minor		273388		52 mins 34 secs	26/12/2013 12:25:28 pm	Dynamic	4		
System	csco_10.20.0.112	Device	CPU: 1 has exceeded threshold: (80% currently (1059%))	Minor		273388		1 day 12 hrs	26/12/2013 12:30:09 pm	Dynamic	444		
System	csco_10.20.0.129	Device	System or agent has recently restarted	Minor		273388		1 mon 1 day	26/12/2013 12:30:04 pm	Internal	8,352	491	
System	csco_10.20.1.4	Device	System or agent has recently restarted	Minor		273390		1 mon 1 day	26/12/2013 12:30:05 pm	Internal	8,352	491	
System	csco_10.20.1.9	Device	Printer Printer Cover: Simon cover open: Printer Cover Simon	Minor		273390		3 wks 1 day	26/12/2013 12:31:11 pm	Dynamic	1,959		
System	csco_10.20.0.21	Device	CPU: 1 has exceeded threshold: (80% currently (100%))	Minor		273390		17 mins 36 secs	26/12/2013 12:25:18 pm	Dynamic	3		
System	csco_10.20.0.22	Device	CPU: 1 has exceeded threshold: (80% currently (96%))	Minor		273390		21 mins 51 secs	26/12/2013 12:30:30 pm	Dynamic	4		
System	csco_10.20.0.30	Device	CPU: 1 has exceeded threshold: (80% currently (100%))	Minor		273390		17 mins 21 secs	26/12/2013 12:30:07 pm	Dynamic	4		
System	Conference-Room	Device	System or agent has recently restarted	Minor		273390		3 wks 2 hrs	26/12/2013 12:30:05 pm	Internal	3,708		
System	ms-ao-ism	Device	App. 238, Snippet: 135 reported a collection problem (Explanation: Timeout)	Minor		273390		1 day 1 hr	26/12/2013 12:31:05 pm	Internal	78		
System	ms-ao-ism	Device	App. 238, Snippet: 129 reported a collection problem (Explanation: Timeout)	Minor		273390		6 days 20 hrs	26/12/2013 12:30:28 pm	Internal	1,910		
System	ms-ao-ism	Device	Physical Memory has exceeded threshold: (80% currently (97%))	Minor		273390		2 days 14 hrs	26/12/2013 12:25:34 pm	Dynamic	403		
System	ms-ao-ism	Device	Physical Memory has exceeded threshold: (80% currently (97%))	Minor		273390		2 hrs 42 mins	26/12/2013 12:10:07 pm	Dynamic	13		
System	ms-8510-1-cisco.com	Device	System or agent has recently restarted	Minor		273388		1 mon 1 day	26/12/2013 12:30:04 pm	Internal	8,352	491	
System	SEL0159101777	Device	Printer HP Tray paper tray empty: HP Tray	Minor		273425		1 mon 1 day	26/12/2013 12:31:12 pm	Dynamic	1,392	490	
System	DELL2472DA	Device	Physical Memory has exceeded threshold: (80% currently (100%))	Minor		273733		1 mon 1 day	26/12/2013 12:30:44 pm	Dynamic	8,343	366	
System	fish_p2_ao	Device	System or agent has recently restarted	Minor		273733		27 mins 36 secs	26/12/2013 12:10:06 pm	Dynamic	2		
System	mf7	Device	Physical Memory has exceeded threshold: (80% currently (95%))	Minor		273737		1 wk 11 hrs	26/12/2013 12:30:16 pm	Dynamic	1,953		
System	mf7	Device	Physical Memory has exceeded threshold: (80% currently (84%))	Minor		273737		1 wk 12 hrs	26/12/2013 12:30:08 pm	Dynamic	1,959		
System	mf7	Device	Physical Memory has exceeded threshold: (80% currently (81%))	Minor		273737		17 mins 36 secs	26/12/2013 12:30:08 pm	Dynamic	3		
System	mf7	Device	Physical Memory has exceeded threshold: (80% currently (95%))	Minor		273737		1 wk 12 hrs	26/12/2013 12:30:07 pm	Dynamic	1,959		
System	mf7	Device	Physical Memory has exceeded threshold: (80% currently (84%))	Minor		273737		1 wk 12 hrs	26/12/2013 12:30:06 pm	Dynamic	1,959		
System	mf7	Device	Physical Memory has exceeded threshold: (80% currently (84%))	Minor		273737		1 wk 12 hrs	26/12/2013 12:30:06 pm	Dynamic	1,959		
System	mf7	Device	App. 238, Snippet: 129 reported a collection problem (Explanation: Timeout)	Minor		273737		52 mins 34 secs	26/12/2013 11:40:23 am	Dynamic	1,959		
System	mf7	Device	Physical Memory has exceeded threshold: (80% currently (82%))	Minor		273737		1 mon 1 day	26/12/2013 12:30:37 pm	Dynamic	8,353		

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

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

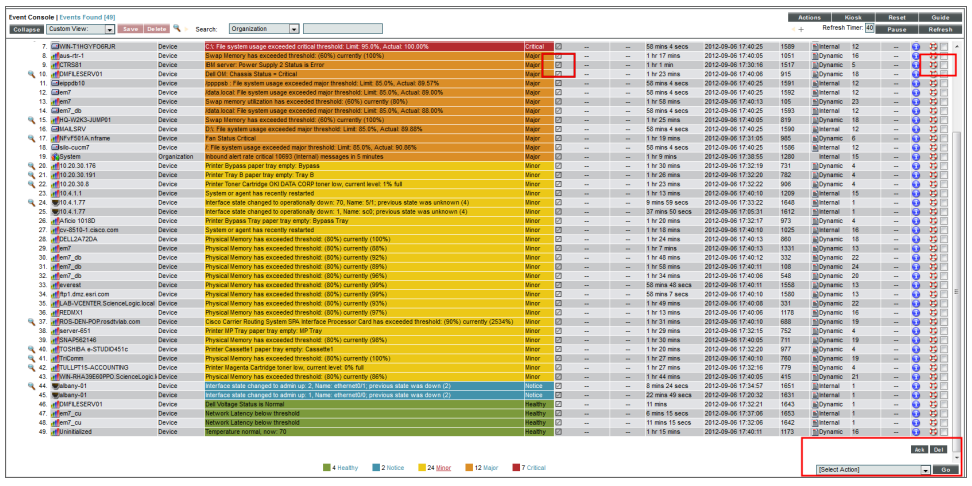
# Clearing One or More Events

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.



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, 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.

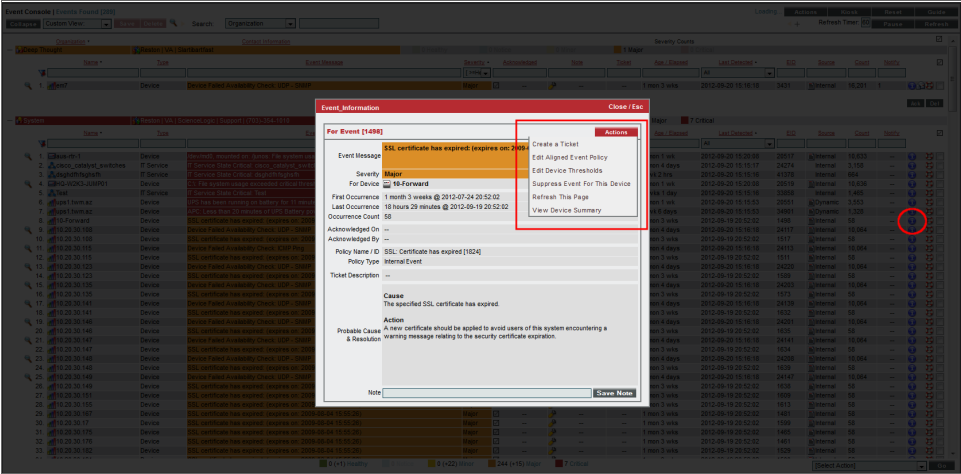
If a suppressed event occurs on a different device, it will appear in the **Event Console** page and on the **Viewing Events** page for that different device.

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:

1. Go to the **[Events]** tab.
2. In the **Event Console**, select the information icon (📘) 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

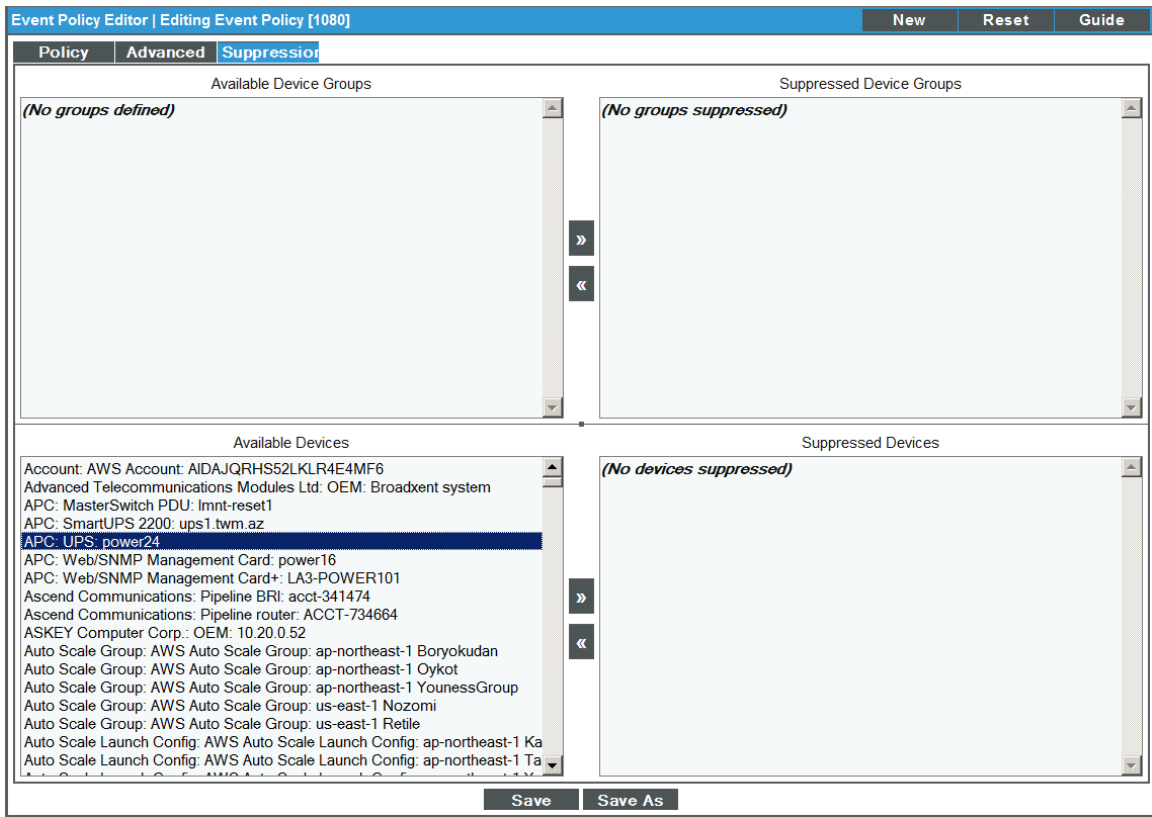
When you suppress an event on multiple devices, you are specifying that, in the future, if this event occurs again on any of those devices, the event will not appear in the **Event Console** page or the **Viewing Events** page for any of those devices.

To suppress an event on multiple devices:

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: EM7 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	Notice	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	--	--			

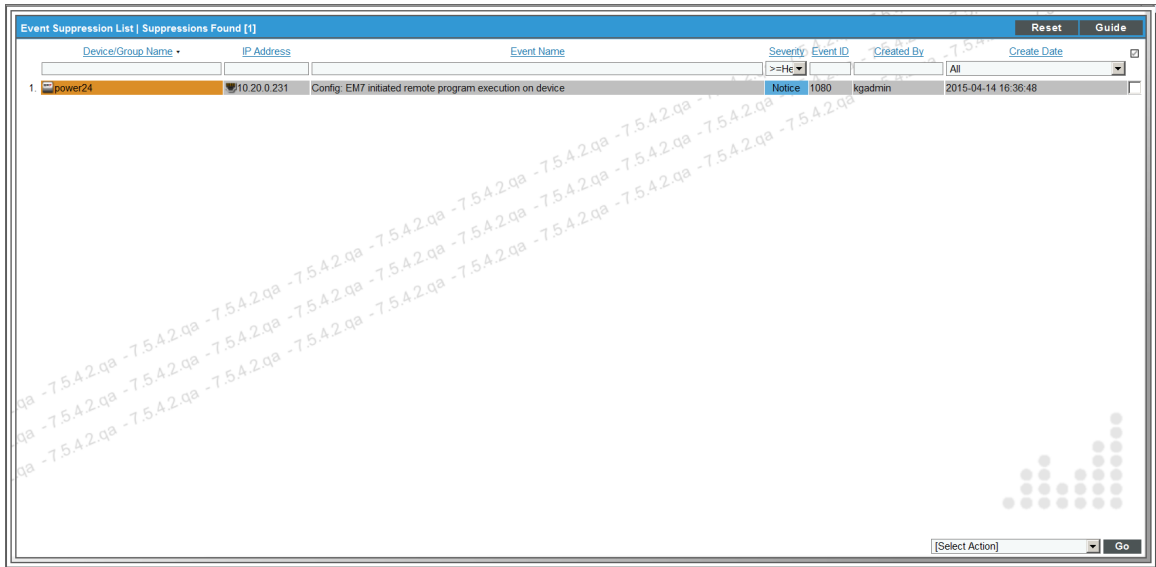
3. The **Event Policy Editor** page appears, with the **Suppressions** tab selected.



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

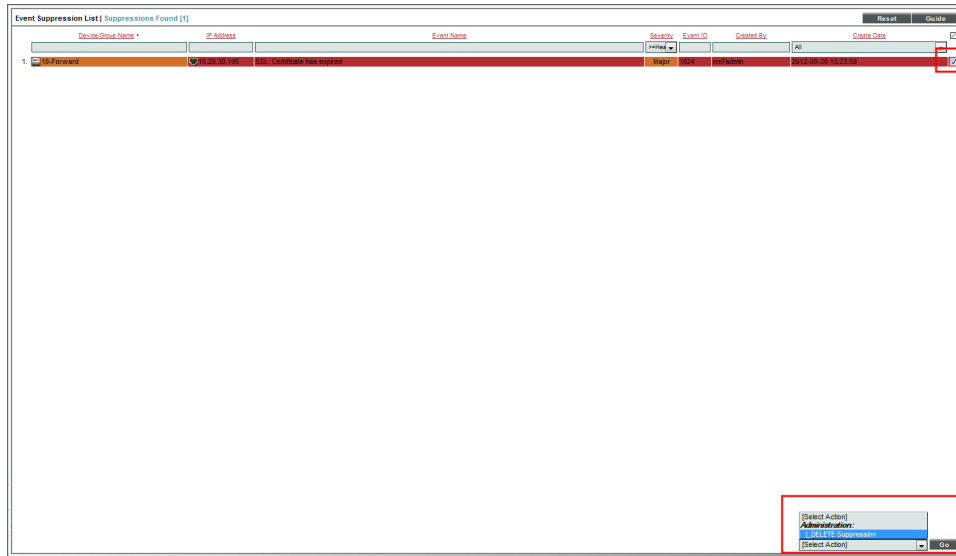
You can view a list of all suppressed events in the ScienceLogic platform and choose to unsuppress one or more of those events. When you unsuppress an event, if this event occurs again on the same device, the event will appear in the **Event Console** page.

**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 (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. Select the **[Go]** button.
5. In the future, if the unsuppressed event occurs again on the same device, the event will appear in the **Event Console** 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 **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:

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	Type	State	Enabled	Severity	Priority	IR	Extra	Time	Thresh	Edited By	Last Edited	External ID	Category
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: Tap Library Degraded	Dynamic	Enabled	No	Minor	0	899	60 Min.	0 Min.	0	em7admin	2012-07-07 00:14:30	--	--
4. ADIC: Tap Library Degraded	Dynamic	Enabled	No	Minor	0	899	60 Min.	0 Min.	0	em7admin	2012-07-07 00:14:30	--	--
5. AKACP: AC Voltage sensor detects no current	Syslog	Enabled	Yes	Critical	0	1517	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
6. AKACP: AC Voltage sensor now reporting Normal Status	Syslog	Enabled	Yes	Healthy	0	1522	15 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
7. AKACP: DC Voltage High Warning	Syslog	Enabled	Yes	Major	0	1528	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
8. AKACP: DC Voltage sensor High Critical	Syslog	Enabled	Yes	Critical	0	1528	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
9. AKACP: DC Voltage sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1527	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
10. AKACP: DC Voltage sensor Low Warning	Syslog	Enabled	Yes	Major	0	1529	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
11. AKACP: DC Voltage sensor returned to Normal Status	Syslog	Enabled	Yes	Healthy	0	1536	15 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
12. AKACP: Dry Contact Sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1516	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
13. AKACP: Dry contact sensor now Normal	Syslog	Enabled	Yes	Healthy	2	1521	15 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
14. AKACP: Humidity High Warning	Syslog	Enabled	Yes	Major	0	1524	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
15. AKACP: Humidity Low Warning	Syslog	Enabled	Yes	Major	0	1525	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
16. AKACP: Smoke Detector Alert	Syslog	Enabled	Yes	Critical	10	1522	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
17. AKACP: Smoke detector now Normal Status	Syslog	Enabled	Yes	Healthy	4	1518	15 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
18. AKACP: Water Sensor has detected water	Syslog	Enabled	Yes	Critical	0	1520	90 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
19. AKACP: Water sensor now Normal	Syslog	Enabled	Yes	Healthy	0	1519	15 Min.	0 Min.	0	em7admin	2012-07-07 00:15:08	--	--
20. ABeon: New Tapn Exited	Dynamic	Enabled	No	Critical	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	1406	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 18:48:11	--	--
26. ABeon: Battery Charge Normal	Dynamic	Enabled	No	Healthy	0	945	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
27. ABeon: Battery Run Time Remaining No Longer Critical	Dynamic	Enabled	No	Healthy	0	942	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
28. ABeon: Battery Status	Dynamic	Enabled	No	Major	0	941	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
29. ABeon: Calibration Test Completed	Dynamic	Enabled	No	Healthy	0	954	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
30. ABeon: Calibration Test Did Not Complete	Dynamic	Enabled	No	Minor	0	960	60 Min.	0 Min.	0	em7admin	2012-09-06 18:48:12	--	--
31. ABeon: Calibration Test Failed	Dynamic	Enabled	No	Major	0	956	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
32. ABeon: Communication Status Okay	Dynamic	Enabled	No	Healthy	0	949	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
33. ABeon: Communication Status Stopped	Dynamic	Enabled	No	Major	0	951	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
34. ABeon: Diagnostic Test Failed	Dynamic	Enabled	No	Critical	0	957	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
35. ABeon: Diagnostic Test In Progress	Dynamic	Enabled	No	Notice	0	958	30 Min.	0 Min.	0	em7admin	2012-09-06 18:48:12	--	--
36. ABeon: Diagnostic Test Passed	Dynamic	Enabled	No	Healthy	0	953	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
37. ABeon: Diagnostic Test Stopped	Dynamic	Enabled	No	Major	0	959	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:12	--	--
38. ABeon: Diagnostics Schedule Not Set	Dynamic	Enabled	No	Major	0	952	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
39. ABeon: Diagnostics Schedule Set	Dynamic	Enabled	No	Healthy	0	955	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
40. ABeon: Percent Battery Remaining No Longer Critical	Dynamic	Enabled	No	Healthy	0	944	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
41. ABeon: Temperature has exceeded threshold	Dynamic	Enabled	No	Minor	0	962	60 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
42. ABeon: Temperature has returned to normal	Dynamic	Enabled	No	Healthy	0	961	15 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
43. ABeon: UPS Battery Capacity	Dynamic	Enabled	No	Critical	0	939	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--
44. ABeon: UPS has Defective Battery Packs	Dynamic	Enabled	No	Major	0	936	90 Min.	0 Min.	0	em7admin	2012-09-06 18:48:11	--	--

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

- 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.

The screenshot shows the 'Event Policy Manager' interface with a table of 44 event policies. The table columns include: Event Policy Name, Type, State, R-Path, Severity, Vendor, ID, Extra, Time, Threshold, Edited By, Last Edited, External ID, and Category. Several rows are highlighted in red, and checkboxes in the right-hand column are checked for these rows. A red box highlights the 'Select Actions' dropdown menu at the bottom right, which is currently set to 'DISABLE these Event Policies'.

3

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

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

The selected event(s) will no longer appear in the ScienceLogic platform 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:

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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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	em7admn	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**.
- Select the **[Go]** button. The selected event(s) will once again appear in the ScienceLogic platform.

---

# Chapter

# 4

## Events and Tickets


---

### Overview

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

**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 **Event Console** page. 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), selecting the life ring icon () in the **Event Console** will either create a ScienceLogic ticket or an external ticket. See the [Event Ticket Behavior Settings](#) section for more information.


# Creating a Ticket from the Event Console

When viewing an event in the **Event Console** page, 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. In 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:

The screenshot shows the 'Ticket Editor' interface. At the top, there are tabs for 'Properties', 'Logs', 'Automation', and 'Message'. The 'Properties' tab is active. The 'Description' field contains '(New Ticket)'. The 'Organization' field is set to '[System]'. The 'Element' field is populated with '40.0.12.50 [ Linux | ICMP | IP: 10.0.12.50 | ID: 203 ]'. The 'Aligned Event' field shows a warning icon and '[163790] Failed to resolve host name'. Below these fields is the 'Ticket Properties' section, which includes fields for 'Ticket Description' (Failed to resolve host name), 'Sub-Organization' ([None]), 'Ticket State' (Open), 'Status' (Open), 'Severity' ([ Sev 3 / Major]), 'Category' (Abuse), 'Source' (Automated), 'Queue' (Asset Management), and 'Assigned User' (None). There is also a 'Version Target' field. Below the ticket properties is the 'Notes & Attachments' section, which includes a toolbar with various icons and a large text area for notes. A 'Save' button is located at the bottom of the interface.

2. Depending on the **Event Console Ticket Life Ring Button Behavior** setting in the **Behavior Settings** page (System > Settings > Behavior), selecting the life ring icon (🚒) will either create a ScienceLogic ticket or an external ticket. See the [Event Ticket Behavior Settings](#) section for more information.
3. Most of the fields are already populated with values from the event. You can accept these values or edit them. The following fields display:
  - **Description**. A brief description of the problem or ticket. If you create a ticket from an event in the **Event Console**, this field is populated automatically by the ScienceLogic platform.
  - **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 **Event Console**, this field is populated automatically by the ScienceLogic platform.

- **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 **Event Console**, this field is populated automatically by the ScienceLogic platform 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 > Select 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 the ScienceLogic platform 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 the ScienceLogic platform.
  - *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**, the ScienceLogic platform 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, the ScienceLogic platform automatically sends the user an email message as notification.
- **Custom Fields.** If your ScienceLogic 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, select 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 life-ring icon (🚫) in the **Event Console** is determined in the **Behavior Settings** page (System > Settings > Behavior). To change this behavior:

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



The screenshot shows the 'Behavior Settings' configuration page. The 'Event Console Ticket Life Ring Button Behavior' dropdown menu is highlighted with a red box and is currently set to 'Create / View EM7 Ticket'. Other settings include Interface URL, Password Expiration, Account Lockout Type, and various system and network parameters.

2. Select from the following options in the **Event Console Ticket Life Ring Button Behavior** field:
  - *Create/View EM7 Ticket*. When you select the life-ring icon () for an event in the **Event Console**, the ScienceLogic platform will display the **Ticket Editor** page, where you can define a ScienceLogic 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 life-ring icon () for that event (from the **Event Console**), the ScienceLogic platform 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, the ScienceLogic platform 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

In the ScienceLogic platform, in the **Event Console** page, the **External Ticket** column is provided for integrating events with an external ticketing system.

If an external ticket is aligned with an event, when you select the life-ring icon () for that event (from the **Event Console**), the ScienceLogic platform 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, the ScienceLogic platform 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 Event Console

The following two fields in the `master_events.events_active` database table in the ScienceLogic platform populate the values for external tickets in the **Event Console** page:


- **force\_ticket\_uri**. This field contains the URI that leads to the external ticket. In the **Event Console** page, clicking on the life-ring icon () for an external ticket 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 **External Ticket** column in the **Event Console** page.

The value stored in the `ext_ticket_ref` field for an event (i.e., the ticket number for that event on the external ticketing system) is displayed in the **External Ticket** column for that event.

For example, suppose the events in an off-site ScienceLogic 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 ScienceLogic system, we would define the following:

- **force\_ticket\_uri**. The URI that leads to the ticket in the off-site system. Clicking on the life-ring icon () opens a new window with the URI loaded.


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

- **ext\_ticket\_ref**. Name or ID number that is displayed in the **External Ticket** column in the **Event Console** page 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.

You can configure the ScienceLogic platform to trigger an automation policy when a user selects the life-ring icon () on the **Event Console** page. To configure this, in the **Behavior Settings** page (System > Settings > Behavior), in the field **Event Console Ticket Life Ring Button Behavior**, select *Create/View External Ticket*.

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 life-ring icon () in the **Event Console** page. 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 the ScienceLogic platform.
  - An SQL query action that updates the **ext\_ticket\_ref** and **force\_ticket\_uri** fields for the event. The value of **ext\_ticket\_ref** should be set to the value passed by the previous snippet action (accessed using the `_%EM7_RESULT_%` variable). The SQL query should use the %e variable (the event ID for the event that triggered the automation policy) to ensure that the query updates the correct event.



- An automation policy that runs when events are cleared. This automation policy would execute a snippet action that:
  - Performs an SQL query to retrieve the **ext\_ticket\_ref** value for the event that triggered the automation policy.
  - Resolves the appropriate ticket in the external ticketing system.

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

## Aligning an External Ticket with Multiple Events

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

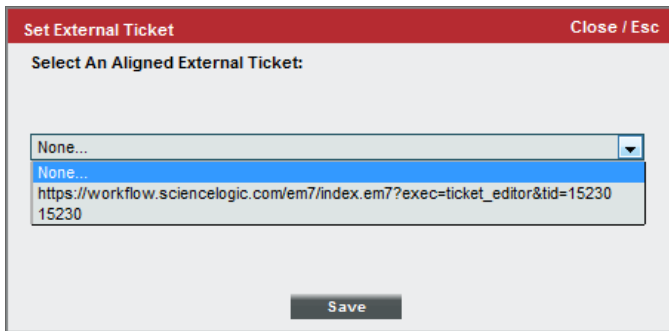
After linking an external ticket to a ScienceLogic event, you can copy that link to other related events. This section describes how to copy the link to an external ticket to multiple, related events.

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 select the **[Go]** button.



Organization	Name	Type	Event Threshold	Severity	Auto-Resolved	Index	External Ticket	Age_Classes	Last_Cleared	SLI	Source	Count	Notes	
501 System	10.20.0.176	Device	Printer Tray2 paper tray empty: Tray2	Minor	<input type="checkbox"/>	273543	1	1 month 1 day	2012/01/13 01:31:09 pm	8228494	Dynamic	1,395	386	
502 System	10.20.0.176	Device	Printer Bypass paper tray empty: Bypass	Minor	<input type="checkbox"/>	273546	1	1 month 1 day	2012/01/09 01:31:09 pm	8228498	Dynamic	1,396	386	
503 System	10.20.0.190	Device	CPU 1 has exceeded threshold: (80%) currently (103722921%)	Minor	<input type="checkbox"/>	273566	1	1 month 1 day	2012/01/11 01:55:51 pm	8227520	Dynamic	1,396	379	
504 System	10.20.0.191	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	<input type="checkbox"/>	273568	1	1 month 1 day	2012/01/11 01:55:48 pm	8228496	Dynamic	1,396	386	
505 System	10.20.0.191	Device	Printer Tray B paper tray empty: Tray B	Minor	<input type="checkbox"/>	273544	1	1 month 1 day	2012/01/13 01:31:09 pm	8228498	Dynamic	1,395	386	
506 System	10.20.0.191	Device	Network latency exceeded threshold: No Response	Minor	<input type="checkbox"/>	273545	1	1 month 1 day	2012/01/13 01:31:09 pm	8228498	Dynamic	1,395	386	
507 System	192.168.24.64	Device	App: 238, Snmpoid: 135 reported a collection problem (Explanation: (noSuchName) There is a	Minor	<input type="checkbox"/>	273421	1	1 month 1 day	2012/01/13 01:45:35 pm	8228178	Internal	2,788	400	
508 System	192.168.37.10	Device	Network latency exceeded threshold: No Response	Minor	<input type="checkbox"/>	273457	1	1 month 1 day	2012/01/13 01:52:21 pm	8228142	Internal	20,917	20	
509 System	192.168.37.10	Device	CPU 1 has exceeded threshold: (80%) currently (92%)	Minor	<input type="checkbox"/>	273457	1	12 min 48 secs	2012/01/13 01:55:51 pm	8550551	Dynamic	3	1	
510 System	10.10.10.80	Device	Printer Bypass Tray paper tray empty: Bypass Tray	Minor	<input type="checkbox"/>	273541	1	1 month 1 day	2012/01/13 01:31:09 pm	8228491	Dynamic	1,395	386	
511 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (84%)	Minor	<input type="checkbox"/>	273423	1	1 day 11 hrs	2012/01/13 01:51:13 pm	8550103	Dynamic	425	1	
512 System	192.168.37.10	Device	App: 238, Snmpoid: 135 reported a collection problem (Explanation: (noSuchName) There is a	Minor	<input type="checkbox"/>	273423	1	4 month 1 day	2012/01/13 01:45:29 pm	8228189	Internal	2,789	400	
513 System	192.168.37.10	Device	CPU 1 has exceeded threshold: (80%) currently (823%)	Minor	<input type="checkbox"/>	273812	1	1 month 1 day	2012/01/13 01:50:36 pm	8228220	Dynamic	8,361	17	
514 System	192.168.37.10	Device	Network latency exceeded threshold: No Response	Minor	<input type="checkbox"/>	273812	1	1 wk 22 hrs	2012/01/13 01:52:21 pm	8492099	Internal	5,717	1	
515 System	192.168.37.10	Device	CPU 0 has exceeded threshold: (90%) currently (50000%)	Minor	<input type="checkbox"/>	273805	1	1 month 1 day	2012/01/13 01:50:44 pm	8227930	Dynamic	8,369	19	
516 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (95%)	Minor	<input type="checkbox"/>	273805	1	1 wk 5 days	2012/01/13 01:50:06 pm	8421866	Dynamic	3,669	1	
517 System	192.168.37.10	Device	Network latency exceeded threshold: No Response	Minor	<input type="checkbox"/>	273455	1	1 month 1 day	2012/01/13 01:52:21 pm	8228140	Internal	20,917	20	
518 System	192.168.37.10	Device	CPU 0 has exceeded threshold: (80%) currently (3473%)	Minor	<input type="checkbox"/>	273455	1	16 hrs 27 mins	2012/01/13 01:50:49 pm	8546855	Dynamic	197	1	
519 System	192.168.37.10	Device	SQL: ECDC RTT 0 is above the minor threshold 599.999 ms, currently 627 ms	Minor	<input type="checkbox"/>	273358	1	2 mins 38 secs	2012/01/13 01:50:47 pm	8550600	Dynamic	1	1	
520 System	192.168.37.10	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273358	1	1 month 1 day	2012/01/13 01:50:03 pm	8228296	Internal	8,366	401	
521 System	192.168.37.10	Device	CPU 1 has exceeded threshold: (80%) currently (584%)	Minor	<input type="checkbox"/>	273358	1	1 hr 27 mins	2012/01/13 01:50:51 pm	8550019	Dynamic	18	1	
522 System	192.168.37.10	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273358	1	1 month 1 day	2012/01/13 01:50:03 pm	8228172	Internal	1,396	401	
523 System	192.168.37.10	Device	Printer Cover Simon cover open: Printer Cover Simon	Minor	<input type="checkbox"/>	273358	1	3 wk 1 day	2012/01/13 01:31:00 pm	8321056	Dynamic	1,061	1	
524 System	192.168.37.10	Device	CPU 1 has exceeded threshold: (80%) currently (94%)	Minor	<input type="checkbox"/>	273358	1	22 mins 34 secs	2012/01/13 01:50:00 pm	8550361	Dynamic	6	1	
525 System	192.168.37.10	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273358	1	2 wk 3 hrs	2012/01/13 01:50:06 pm	8492096	Internal	3,719	1	
526 System	192.168.37.10	Device	Network latency exceeded threshold: 292.56 ms	Minor	<input type="checkbox"/>	273358	1	1 min 4 secs	2012/01/13 01:52:21 pm	8550610	Internal	1	1	
527 System	192.168.37.10	Device	App: 235, Snmpoid: 129 reported a collection problem (Explanation: Timeout)	Minor	<input type="checkbox"/>	273358	1	6 days 21 hrs	2012/01/13 01:50:16 pm	8481750	Internal	1,017	1	
528 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (87%)	Minor	<input type="checkbox"/>	273358	1	2 days 16 hrs	2012/01/13 01:50:54 pm	8550517	Dynamic	416	1	
529 System	192.168.37.10	Device	App: 238, Snmpoid: 135 reported a collection problem (Explanation: Timeout)	Minor	<input type="checkbox"/>	273358	1	1 day 2 hrs	2012/01/13 01:45:58 pm	8549520	Internal	83	1	
530 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (97%)	Minor	<input type="checkbox"/>	273358	1	4 hrs 2 mins	2012/01/13 01:45:24 pm	8549073	Dynamic	21	1	
531 System	192.168.37.10	Device	System or agent has recently restarted	Minor	<input type="checkbox"/>	273358	1	1 month 1 day	2012/01/13 01:50:03 pm	8228296	Internal	8,366	401	
532 System	192.168.37.10	Device	Printer MP Tray paper tray empty: MP Tray	Minor	<input type="checkbox"/>	273425	1	1 month 1 day	2012/01/13 01:31:00 pm	8228229	Dynamic	1,394	400	
533 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	<input type="checkbox"/>	273733	1	1 month 1 day	2012/01/13 01:50:46 pm	8228233	Dynamic	1,395	386	
534 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (94%)	Minor	<input type="checkbox"/>	273733	1	1 wk 13 hrs	2012/01/13 01:50:18 pm	8473959	Dynamic	1,980	1	
535 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (95%)	Minor	<input type="checkbox"/>	273733	1	1 wk 13 hrs	2012/01/13 01:50:12 pm	8473786	Dynamic	1,980	1	
536 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (92%)	Minor	<input type="checkbox"/>	273733	1	1 wk 13 hrs	2012/01/13 01:50:07 pm	8473609	Dynamic	1,980	1	
537 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (84%)	Minor	<input type="checkbox"/>	273733	1	1 wk 13 hrs	2012/01/13 01:50:05 pm	8473609	Dynamic	1,980	1	
538 System	192.168.37.10	Device	App: 235, Snmpoid: 129 reported a collection problem (Explanation: Timeout)	Minor	<input type="checkbox"/>	273737	1	12 mins 59 secs	2012/01/13 01:40:28 pm	8550548	Dynamic	1	1	
539 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (92%)	Minor	<input type="checkbox"/>	273737	1	1 month 1 day	2012/01/13 01:50:42 pm	8550591	Dynamic	1,395	386	
540 System	192.168.37.10	Device	Physical Memory has exceeded threshold: (80%) currently (84%)	Minor	<input type="checkbox"/>	273739	1	1 month 1 day	2012/01/13 01:50:08 pm	8228205	Dynamic	1,395	386	

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





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

## Event Correlation and Parent and Child Events

---


### Overview

In the ScienceLogic platform, 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, the ScienceLogic platform does not display each occurrence in the **Event Console**. Instead, the platform 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**. For details on suppressing events for a single device, see the chapter on [Responding to Events](#).
- **Topology Events.** In the ScienceLogic platform, 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 in the **Event Console** page. The magnifying-glass icon () appears to the left of the parent event. When you click on the magnifying-glass icon, the list of child events is displayed. The child events are rolled up under the parent event and are not displayed in the **Event Console** page. For the parent event, the count column will be incremented to indicate the number of correlated child events. Optionally, you can define event categories that allow the ScienceLogic platform 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.** In the **Device Properties** page for each device, you can define an Event Mask. When a device uses the Event Mask setting, 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 list of all events that are masked under the event is displayed. For details on event masks, see the chapter on [Viewing Events](#).

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

The ScienceLogic platform performs two types of event correlation:

- **Automatic Event-Correlation.** During discovery, the ScienceLogic platform automatically discovers and defines parent-child relationships between devices.
- **Manual Event Correlation.** In the ScienceLogic platform, 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 in the **Event Console**. 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 in the **Event Console** page. The single event would describe the switch failure. The magnifying-glass icon () would appear to the left of the parent event. When you click on the magnifying-glass icon, the events for each attached device would be displayed. When you manually define a hierarchy between events, you can also include an event category. An event category allows the ScienceLogic platform to more efficiently align suppressing events with suppressible events.

---

## Event Correlation

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

- Define parent and child devices. The ScienceLogic platform does this automatically when it discovers Layer-2, CDP, LLDP, Layer-3, and VMware topology. For example, if the platform automatically discovers a switch and its clients, the platform 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 Views > Topology Maps pages or the Views > 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

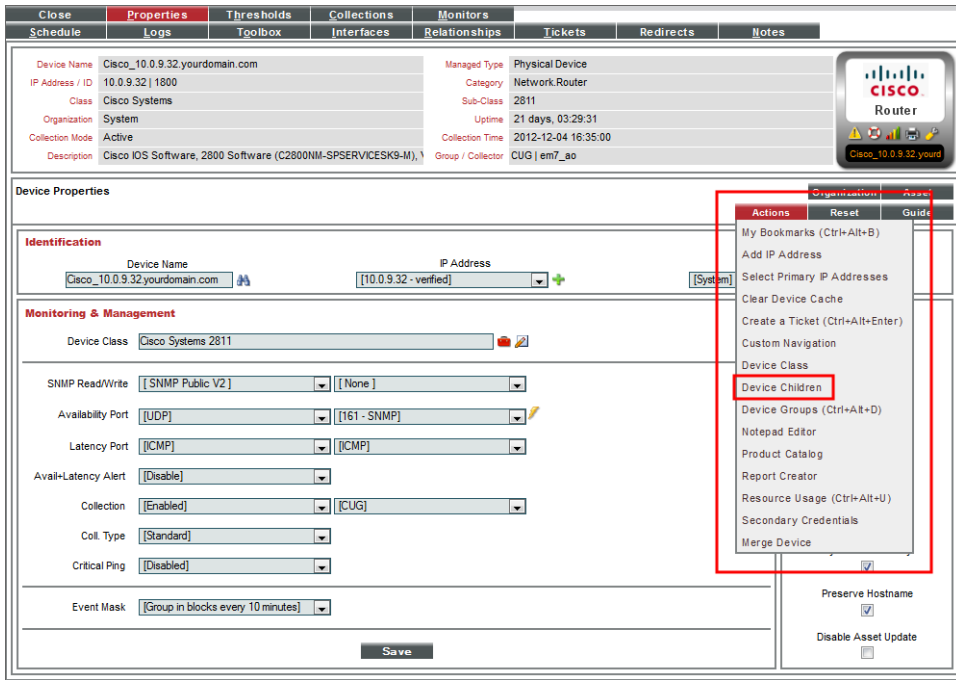
The **Device Children** modal page allows users to select one or more devices to become children of the currently selected device.

To add children to a device:

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

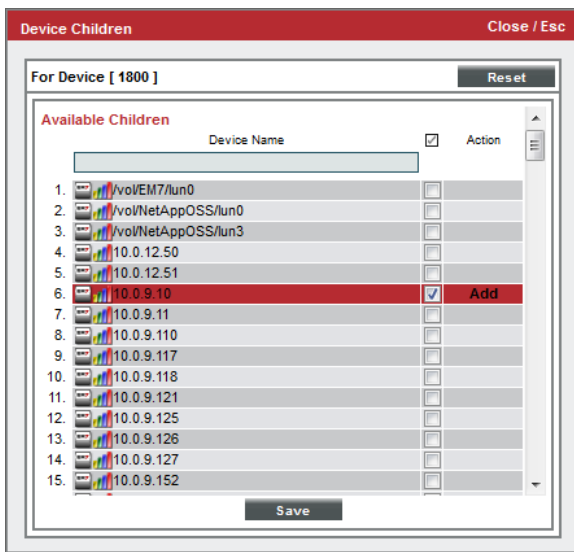
3. The **Device Properties** page appears:

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



4. In the **Device Properties** page, in the **[Actions]** drop-down list, select *Device Children*.

5. The **Device Children** modal page appears:



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

## Device Categories that Don't Support Children Devices

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

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

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

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

To determine a device's device category, look in the *Category* field in any page in the **Device Administration** or **Device Management** pages.

---

## Defining Suppressing and Suppressible Events

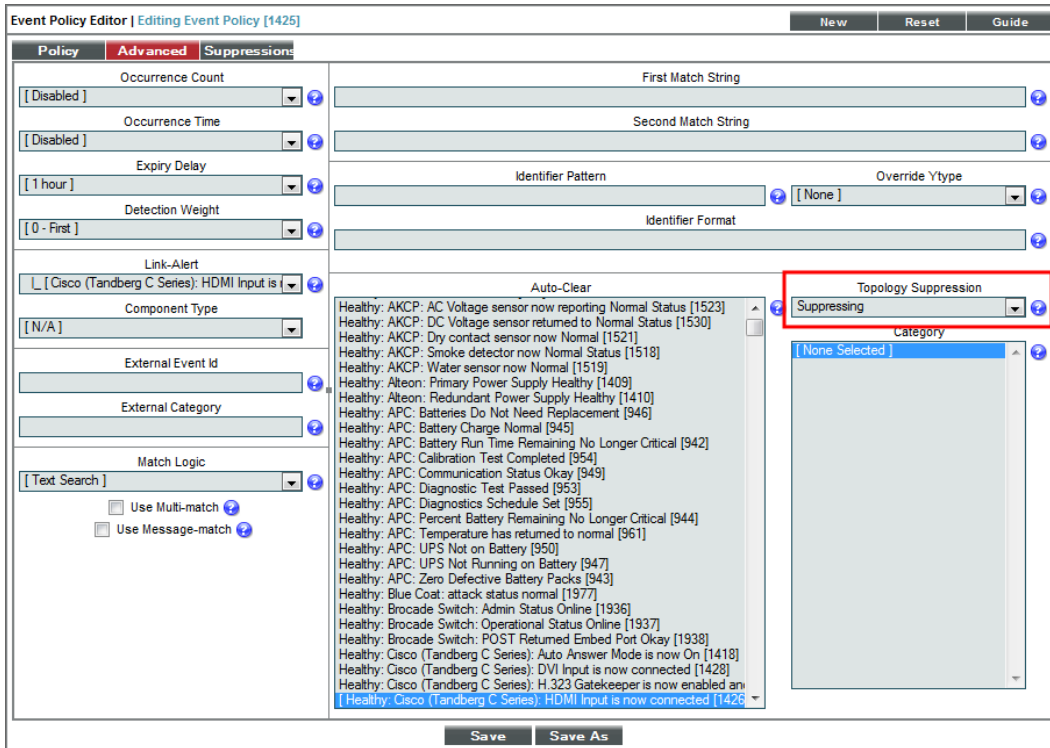
To manually configure event correlation, you must define two types of events:

- **Suppressing events.** If this event occurs on a parent device, the ScienceLogic platform 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 **Event Console**. The suppressible events will not appear in the **Event Console** page.
- **Suppressible events.** This type of event is suppressed on a child device only when a suppressing event occurs on the parent device.

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

To define an event as a suppressing event:

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

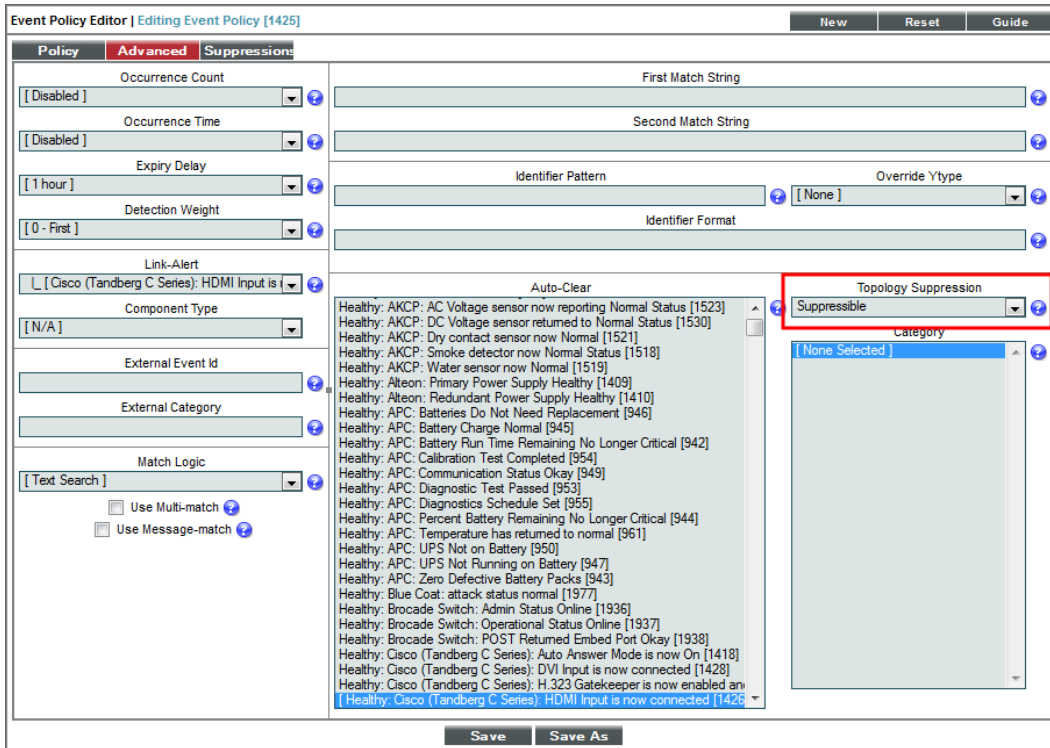


5. In the **Topology Suppression** field, select *Suppressing*.
6. Click **[Save]**.

In the future, when this event occurs on a device, the ScienceLogic platform will check if the device is a parent device. If the device is a parent device, specified events (suppressible events) with the same category will be suppressed on the children devices.

To define an event as a suppressible event:

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



5. In the **Topology Suppression** field, select *Suppressible*.
6. Click **[Save]**.

In the future, when this event occurs on a device, the ScienceLogic platform will check if the device is a child device. If the device is a child device, the platform will check to see if a suppressing event with the same category has occurred on the parent device. If a suppressing event has occurred on the parent device, the specified event will be suppressed on the child device.

For example:

- Suppose you have a device named *Boise-DMZ*. Suppose this device is a Cisco Catalyst switch. Suppose we define this switch as a parent device.
- Suppose we have a device named *HQ-W2K3-VC01*. Suppose this device is a server. Suppose we define this server as a child device to *Boise-DMZ*.
- Suppose we define the event "Poller: Interface operationally down" as a suppressing event.



- Suppose we define the event "Poller: Device not responding" as a suppressible event.
- Suppose we associate both events with the same event category.
- If an interface goes down on the switch *Boise-DMZ*, the platform will not be able to communicate with the server, *HQ-W2K3-VC01*, attached to the switch.
- So if the event "Poller: Interface operationally down" occurs on *Boise-DMZ*, the event "Poller: Device not responding" will be suppressed on the server *HQ-W2K3-VC01*. In the **Event Console** page, only the event "Poller: Interface operationally down" on the device *Boise-DMZ* will appear.

---

## Event Categories

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

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

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

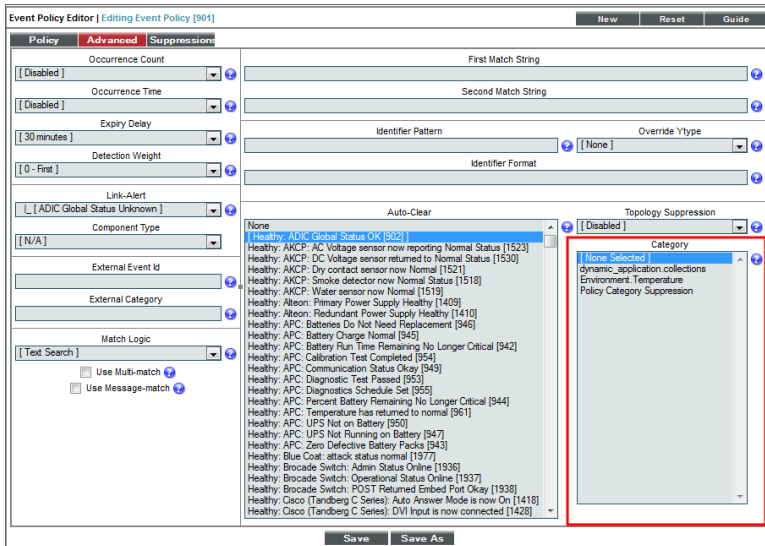
- Now suppose we define two event categories. Suppose we define "Environment.Temperature" and "Dynamic Applications.Collection":
  - Suppose you have a parent device that is a chassis and a child device that is a blade.
  - Suppose you define two suppressing events: one for when the ScienceLogic platform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

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

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

# Assigning an Event Category to an Event

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



If you define an event as **suppressing** and assign an event category to the event, when the event occurs, the ScienceLogic platform 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, the ScienceLogic platform 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, the ScienceLogic platform does not use the event category. The event category will have no effect.

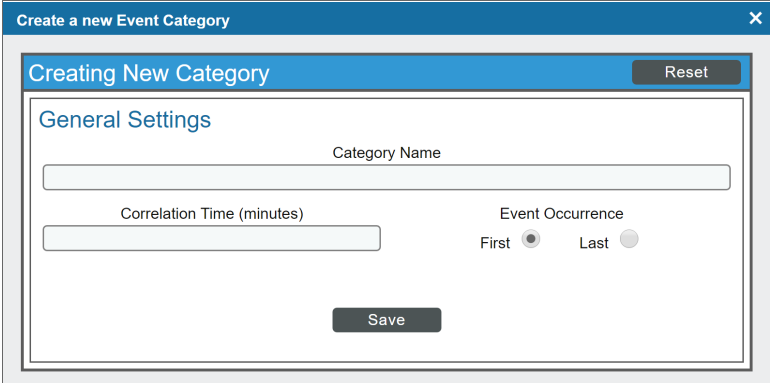
---

## 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 (Registry > Events > Categories).
2. In the **Event Category Manager** page, select the **[Create]** button.
3. The **Event Category Editor** page is displayed. In this page, you can define a new event category. Supply a value in the following fields:



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

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

---

## Editing an Event Category

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

To edit an event category:

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

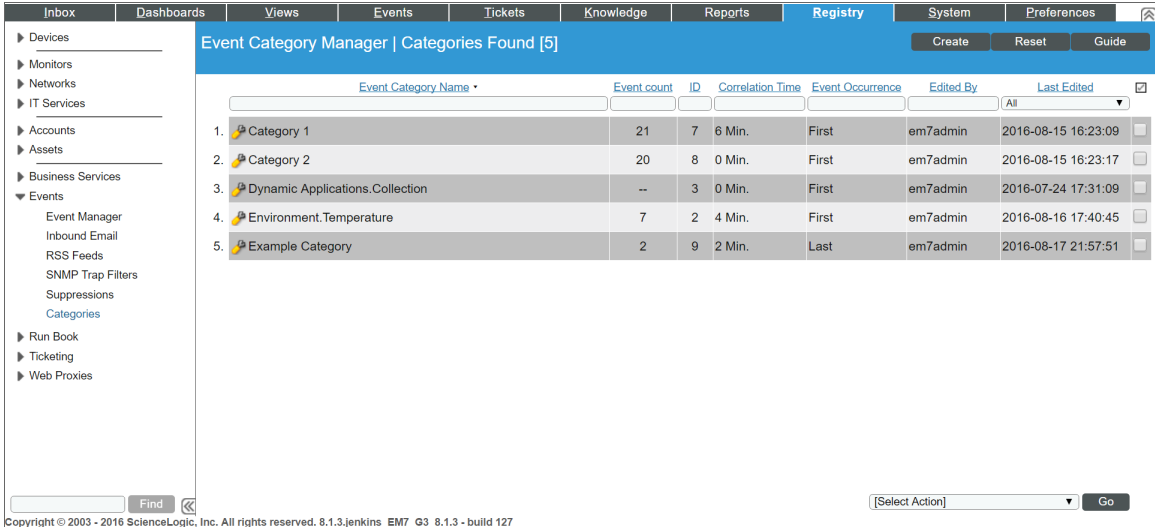
2. In the **Event Category Manager** page, select the wrench icon (🔧) of the event category you want to edit.
3. The **Event Category Editor** page is displayed.
4. In the **Event Category Editor**, you can edit the following fields:

The screenshot shows a window titled "Edit Event Categories" with a close button (X) in the top right corner. Below the title bar is a sub-header "Editing Category [7]" with "New" and "Reset" buttons. The main content area is titled "General Settings" and contains three fields: "Category Name" with the value "Category 1", "Correlation Time (minutes)" with the value "6", and "Event Occurrence" with radio buttons for "First" (selected) and "Last". At the bottom are "Save" and "Save As" buttons.

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

# Viewing the List of Event Categories

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



The screenshot shows the 'Event Category Manager' page with a table of 5 categories. The table has columns for Event Category Name, Event count, ID, Correlation Time, Event Occurrence, Edited By, and Last Edited. The categories listed are: Category 1 (21 events, 7 ID, 6 Min. correlation, First occurrence), Category 2 (20 events, 8 ID, 0 Min. correlation, First occurrence), Dynamic Applications.Collection (0 events, 3 ID, 0 Min. correlation, First occurrence), Environment.Temperature (7 events, 2 ID, 4 Min. correlation, First occurrence), and Example Category (2 events, 9 ID, 2 Min. correlation, Last occurrence). The interface includes a sidebar with navigation options like Devices, Monitors, Networks, IT Services, Accounts, Assets, Business Services, Events, Event Manager, Inbound Email, RSS Feeds, SNMP Trap Filters, Suppressions, Categories, Run Book, Ticketing, and Web Proxies. At the bottom, there is a 'Find' button and a '[Select Action]' dropdown.

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 the ScienceLogic platform.
- **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 the ScienceLogic platform, or last edited.

---

## Filtering the List of Event Categories

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

The list is dynamically updated as you select each filter. For each filter, you must make a selection from a drop-down menu or type text to match against. The ScienceLogic platform 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, the ScienceLogic platform 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, the ScienceLogic platform will not match a substring unless you use a special character.

### String and Numeric

- , (comma). Specifies an "OR" operation. Works for string and numeric values. For example:  
"dell, micro" matches all values that contain the string "dell" OR the string "micro".
- & (ampersand). Specifies an "AND" operation. Works for string and numeric values. For example:  
"dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.
- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:  
"!dell" matches all values that do not contain the string "dell".  
"! ^ micro" would match all values that do not start with "micro".  
"!fer\$" would match all values that do not end with "fer".  
"! ^ \$" would match all values that are not null.  
"! ^" would match null values.  
"! \$" would match null values.  
"!\*" would match null values.  
"happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

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



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

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

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

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

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

"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.

## Additional Examples

- "aio\$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo\$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!O\$". Matches only text that does not end with "O".
- "!^silo\$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!"^". Matches null values, typically represented as "--" in most pages.
- "!"\$". Matches null values, typically represented as "--" in most pages.

- "!"^\$". Matches all text that is not null.
- "silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s\*i!\*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" 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 "sXiXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol" and it does contain "02".
- "aggr, !vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr, !vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "\*". Matches all text.
- "!\*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- "!silo". Matches text that does not contain "silo".
- "!^silo\$". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.
- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "1n", and "2n".
- "n\*SAN". Matches text the contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".
- "^?n\*SAN\$". Matches text that begins with any single character, is following by "n", and then zero or any number of any characters, and ends in "SAN".

## Deleting One or More Event Categories

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

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

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

The screenshot displays the 'Event Category Manager' interface. The main content area shows 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"/>

Below the table, an action dropdown menu is open, showing the following options:

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

The 'Go' button is visible to the right of the dropdown menu.

Copyright © 2003 - 2016 ScienceLogic, Inc. All rights reserved. 8.1.3.jenkins\_EM7\_Q3\_8.1.3 - build 127

## Defining and Editing Event Policies

---

### Overview

The ScienceLogic platform includes pre-defined events for the most commonly encountered conditions on the most common platforms. The ScienceLogic platform allows you to customize these events. If the pre-defined events do not meet the needs of your organization, you can define new events. You can edit existing event policies and create new event policies in the **Event Policy Manager** page.

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

The ScienceLogic platform generates events by collecting logs and messages from the following:

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

- **Dynamic.** Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell the ScienceLogic platform how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. The ScienceLogic platform examines each new message in the device log and determines if the message matches an event definition. If it does, the platform generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the ScienceLogic system inserts a message in the associated device's log files, and the ScienceLogic system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
- **Email.** Message is generated by an email message sent to the platform. For more information on generating events with email messages, see the **Events from Email** chapter.
- **API.** Message was generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the manual **Run Book Automation**. For more information on snippet Dynamic Applications, see the manual **Snippet Dynamic Application Development**. For more information on the ScienceLogic API, see the manual **Using the ScienceLogic API**.
- **ScienceLogic agent.** Message is generated by log file messages collected by the ScienceLogic agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the **Monitoring Using the ScienceLogic agent** manual.

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

# Viewing the List of Event Policies

From the **Event Policy Manager** page, you can view a list of all event policies in the ScienceLogic platform. 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	Threshold	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	1298	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 Warning	Syslog	Enabled	Yes	Critical	0	1287	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
13. AKCP: Dry contact sensor now Normal	Syslog	Enabled	Yes	Healthy	2	1292	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
14. AKCP: Humidity High Warning	Syslog	Enabled	Yes	Major	0	1295	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
15. AKCP: Humidity Low Warning	Syslog	Enabled	Yes	Major	0	1296	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
16. AKCP: Smoke Detector Alert!	Syslog	Enabled	Yes	Critical	10	1293	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
17. AKCP: Smoke detector now Normal Status	Syslog	Enabled	Yes	Healthy	4	1289	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
18. AKCP: Water Sensor has detected water	Syslog	Enabled	Yes	Critical	0	1291	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
19. AKCP: Water sensor now Normal	Syslog	Enabled	Yes	Healthy	0	1290	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
20. 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	20	15 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--
30. APC: Calibration Test Did Not Complete	Dynamic	Enabled	Yes	Minor	0	27	60 Min.	0 Min.	0	em7admin	2015-05-14 11:24:54	--	--

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

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

- **Event Policy Name.** The name of the event.
- **Type.** Specifies the source for the event. Possible values are:
  - *Syslog.* Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices like MoMs. A syslog is an unsolicited message from a device to the ScienceLogic platform. Syslog is a standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools. For more information on syslogs, see the manual **Syslogs and Traps**.
  - *Internal.* Message is generated by a ScienceLogic process. The message is about the ScienceLogic system itself, instead of the devices that the ScienceLogic 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 the ScienceLogic platform. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device. For more information on traps, see the manual **Syslogs and Traps**.
  - *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell the ScienceLogic platform how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. The ScienceLogic platform examines each new message in the device log and determines if the message matches an event definition. If it does, the platform generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the ScienceLogic system inserts a message in the associated device's log files, and the ScienceLogic system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
  - *Email*. Message is generated by an email message sent to the platform. For more information on generating events with email messages, see the **Events from Email** chapter.
  - *API*. Message was generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the manual **Run Book Automation**. For more information on snippet Dynamic Applications, see the manual **Snippet Dynamic Application Development**. For more information on the ScienceLogic API, see the manual **Using the ScienceLogic API**.
  - *ScienceLogic agent*. Message is generated by log file messages collected by the ScienceLogic agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the **Monitoring Using the ScienceLogic agent** manual. *Monitoring*
- **State**. Specifies whether event is to be operational or not. Possible values are "enabled" or "disabled."
  - **P-Pack**. Specifies whether the event is included in a PowerPack.
  - **Severity**. The severity of the event. Choices are:
    - *Healthy*. Healthy events indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.
    - *Notice*. Notice events indicate a condition that does not affect service but about which users should be aware.
    - *Minor*. Minor events indicate a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
    - *Major*. Major events indicate a condition that impacts service and requires immediate investigation.



- **Critical.** Critical events indicate a condition that can seriously impair or curtail service and requires immediate attention (i.e., service or system outages).
- **Weight.** If two event definitions are very similar, the weight field specifies the order in which the ScienceLogic platform 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 the ScienceLogic platform.
- **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 the ScienceLogic platform, 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 ScienceLogic system where the event has a different event ID.
- **Category.** The category for the event. This is an optional field. If the platform will be sending this event to an external system, this field defines the event category for use by the external system.

## Filtering the List of Event Policies

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

The list is dynamically updated as you select each filter. For each filter, you must make a selection from a drop-down menu or type text to match against. The ScienceLogic platform 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, the ScienceLogic platform 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, the ScienceLogic platform will not match a substring unless you use a special character.

### String and Numeric

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

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

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

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

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

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

"! ^" would match null values.

"!\$" would match null values.

"!\*" would match null values.

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

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

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

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

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

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

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

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

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

## String

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

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

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

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

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

"! ^" would match null values.

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

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

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

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

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

"!\$" would match null values.

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

## Numeric

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### Additional Examples

- "aio\$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo\$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!0\$". Matches only text that does not end with "0".
- "!^silo\$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!. Matches null values, typically represented as "--" in most pages.
- "!"\$. Matches null values, typically represented as "--" in most pages.
- "!. Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s\*i\*i\*o\$". Matches text that contains the letter "s", "i", "i", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would match.
- "!^s\*i\*i\*o\$". Matches all text that does not contain the letter "s", "i", "i", "o", in that order. Other letters might lie between these letters. For example "sXiXo" 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

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

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

To create an event definition:

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

The screenshot shows the 'Event Policy Editor | Create New Event Policy' interface. It features a top navigation bar with 'New', 'Reset', and 'Guide' buttons. Below this are three tabs: 'Policy', 'Advanced', and 'Suppressions'. The 'Policy' tab is active, showing several configuration fields: 'Event Source' (set to 'Syslog'), 'Operational State' (set to '[Enabled]'), and 'Event Severity' (set to '[Major]'), each with a help icon. There are also 'Use Modifier' checkboxes. To the right, there are input fields for 'Policy Name' and 'Event Message'. Below these fields is a large 'Policy Description' area with a rich text editor toolbar containing icons for bold, italic, underline, strikethrough, text color, background color, bulleted list, numbered list, link, unlink, and code. The description area contains the placeholder text 'Start typing ...'. At the bottom center, there is a 'Save' button.

3. In the **Event Policy Editor** page and set of tabs, you can define a new event. The **Event Policy Editor** page contains three tabs:
  - **Policy**. Allows you to define basic parameters for the event. This tab is described in the following section.
  - **Advanced**. Allows you to define pattern-matching for the event and also define event roll-ups and suppressions.
  - **Suppressions**. Allows you to suppress the event on selected devices. When you suppress an event, you are specifying that, in the future, if this event occurs again on a specific device, the event will not appear in the **Event Console** page or the **Viewing Events** page for the device.

## Defining Basic Event Parameters in the Policy Tab

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

The screenshot shows the 'Event Policy Editor | Create New Event Policy' window. The 'Policy' tab is active, showing the following fields and options:

- Event Source:** A dropdown menu set to 'Internal'.
- Operational State:** A dropdown menu set to '[ Enabled ]'.
- Event Severity:** A dropdown menu set to '[ Major ]' with a 'Use Modifier' checkbox.
- Policy Name:** A text input field containing 'Poller: Device not responding'.
- Event Message:** A text area containing '%M %N'.
- Policy Description:** A rich text editor area containing:
 

**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.

Buttons for 'New', 'Reset', and 'Guide' are visible at the top right, and a 'Save' button is at the bottom center.

- **Event Source**. Specifies the source for the event. Choices are:
  - *Syslog*. Message is generated by the syslog protocol. Syslogs can be sent by devices and proxy devices like MoMs. A syslog is an unsolicited message from a device to the ScienceLogic platform. Syslog is a standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools. For more information on sylogs, see the manual **Syslogs and Traps**.
  - *Internal*. Message is generated by a ScienceLogic process. The message is about the ScienceLogic system itself, instead of the devices that the ScienceLogic 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 the ScienceLogic platform. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device. For more information on traps, see the manual **Syslogs and Traps**.
- *Dynamic*. Message is generated by a Dynamic Application alert. Dynamic Applications are customizable policies that tell the ScienceLogic platform how to monitor applications and devices. Users can define alerts in Dynamic Applications. An alert can trigger events based on the data collected by the Dynamic Application. Alerts allow users to examine and manipulate values retrieved by Dynamic Applications. When an alert evaluates to TRUE, the alert inserts a message in the associated device's device log. The ScienceLogic platform examines each new message in the device log and determines if the message matches an event definition. If it does, the platform generates an instance of that event. For example, an alert might be defined to evaluate to TRUE if the temperature of a chassis exceeds 100 degrees F. If the chassis temperature exceeds 100 degrees F, the alert evaluates to TRUE, the ScienceLogic system inserts a message in the associated device's log files, and the ScienceLogic system matches that message with an existing event and then triggers the event. For more information on defining and using alerts, see the **Dynamic Application Development** manual.
- *Email*. Message is generated by an email message sent to the platform. For more information on generating events with email messages, see the **Events from Email** chapter.
- *API*. Message was generated by inserting a message into the main database. These messages can be inserted by a snippet automation action, a snippet Dynamic Application, or by a request to the ScienceLogic API. For more information on snippet automation actions, see the manual **Run Book Automation**. For more information on snippet Dynamic Applications, see the manual **Snippet Dynamic Application Development**. For more information on the ScienceLogic API, see the manual **Using the ScienceLogic API**.
- *ScienceLogic agent*. Message is generated by log file messages collected by the ScienceLogic agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the **Monitoring Using the ScienceLogic agent** manual.
- *Rules Engine*. Message generated by the ScienceLogic 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.

The ScienceLogic platform will use the regular expression to search the log message and use the matching text in the event message.

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

- You can also use the following variables in this field:
  - %I ("eye"). For events with a source of "dynamic", this variable contains the index value from SNMP; this index value will be displayed in the Event Message. For Dynamic Applications, %I maps to the raw index that comes back from SNMP. For example, a walk of the MIB at .1.3.6.1.4.1.999.3.2.1 might return the following OIDs:

```
1.3.6.1.4.1.999.3.2.1.1.1
1.3.6.1.4.1.999.3.2.1.2.1,
1.3.6.1.4.1.999.3.2.1.3.1.
```

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

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

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

- **Event Severity.** Defines the severity of the event. Choices are:
  - *Healthy.* Healthy events indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.
  - *Notice.* Notice events indicate a condition that does not affect service but about which users should be aware.
  - *Minor.* Minor events indicate a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
  - *Major.* Major events indicate a condition that impacts service and requires immediate investigation.

- **Critical.** Critical events indicate a condition that can seriously impair or curtail service and requires immediate attention (i.e., service or system outages).
- **Use Modifier.** If selected, when the event is triggered, the ScienceLogic platform will check to see if the interface associated with this event has a custom severity modifier. If so, the event will appear in the **Event Console** with that custom severity modifier applied to the severity in the **Event Severity** field. For example, if an interface with an **Event Severity Adjust** setting of Sev -1 triggers an event with an **Event Severity** of Major and that event has the **Use Modifier** checkbox selected, the event will appear in the **Event Console** with a severity of Minor.
- **Policy Description.** Text that explains what the event means and what possible causes are. You can use the editor to format the description text, insert content from a saved template, and add an attachment, link, or image to the description. This text is displayed in the **Event Console** page and the **Ticket Console** page.

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

## Defining Pattern Matching and Advanced Behavior in the Advanced Tab

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

The screenshot shows the 'Event Policy Editor | Editing Event Policy [3637]' interface with the 'Advanced' tab selected. The interface is divided into several sections:

- Policy Section:** Contains dropdown menus for Occurrence Count (set to [Disabled]), Occurrence Time (set to [Disabled]), Expiry Delay (set to [1 hour]), and Detection Weight (set to [0 - First]).
- Link-Alert:** A dropdown menu currently set to [N/A].
- External Event Id and Category:** Two empty text input fields.
- Match Logic:** A dropdown menu set to [Text Search] with checkboxes for 'Use Multi-match' and 'Use Message-match'.
- First Match String and Second Match String:** Two empty text input fields.
- Identifier Pattern and Identifier Format:** Two empty text input fields.
- Override Ytype:** A dropdown menu set to [None].
- Auto-Clear:** A dropdown menu set to [None Selected].
- Topology Suppression:** A dropdown menu set to [Disabled].
- Category:** A dropdown menu set to [None Selected].

A scrollable list of event categories is visible in the center-right, including items like 'Cisco: IM&P Cluster Node A Error', 'Cisco: IM&P Cluster Node B Error', 'Cisco: IM&P SIP Proxy', 'Cisco: IM&P XCP Auth Component', and various 'Healthy: ADIC', 'Healthy: AKCP', 'Healthy: Alteon', 'Healthy: APC', and 'Healthy: AWS' entries.

At the bottom of the window 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 in the **Event Console**. 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 the ScienceLogic platform will create a new event message in the **Event Console**. 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 the ScienceLogic platform 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, the ScienceLogic platform will create a new event message in the **Event Console**. In the **Event Console**, the **Age/Elapsed** column will specify the time since the very first occurrence of the event, even though that occurrence did not appear in the **Event Console**. The **Count** column will specify the number of times the event has occurred, even though the event does not appear in the **Event Console** 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 the ScienceLogic platform 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 the ScienceLogic platform 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, the ScienceLogic platform uses only the event definition with the lowest weight. So the platform 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 ScienceLogic 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 the platform.

**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 the ScienceLogic platform. 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 the platform, see the manual *Syslogs and Traps*.
  - If a value is specified in this field, the platform examines the OID specified in this field. If the value stored in the OID matches the primary IP address of a device in the platform, the resulting event will be aligned with that device.
  - If a value is specified in this field, the platform 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 the platform, 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, the platform 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 the platform, 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, the platform 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 the platform 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 ScienceLogic 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 the platform 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 the platform 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, the platform will match a log message or alert to only one event policy. If a log message or alert matches multiple event policies, the platform 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, the platform will generate an event for every event policy that matches that single log message or alert.
- **Use Message-match.** If the platform has generated an event and then a second log message or alert matches the same event policy for the same entity, the platform will not generate a second event, but will increase the **count** value for the original event in the **Event Console** 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. the ScienceLogic platform'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 the ScienceLogic platform 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 the ScienceLogic platform'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, the ScienceLogic platform 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. The ScienceLogic platform 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 the platform.

**NOTE:** The ScienceLogic platform's expression matching is case-sensitive.

For details on the regular-expression syntax allowed by the ScienceLogic platform, 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 the platform knows an interface's "yName" (specified in the **Identifier Pattern** field) and the "yType" (specified in the **Override YType** field), the platform can determine the unique "yID" for the interface. The "yID" is stored in the table in which all instances of a specific sub-entity are stored. For example, for "yType" of "interface," the "yID" is a unique numeric ID for a specific interface on a specific device. This "yID" is stored in the table of all discovered interfaces (if\_id in master\_dev.device\_interfaces) and is unique within this table.
- **Identifier Format.** If the **Identifier Pattern** field returns multiple results, users can specify which results to use and in which order. Each result is represented by a variable. This field is optional.
  - %1. First match with identifier pattern. This is the default behavior if no value is supplied in the **Identifier Format** field.
  - %2. Second match with identifier pattern.
  - etc.
  - For example, users could specify "%2:%1" for "Interface %2: Peer %1"



**NOTE:** If you used the previous three fields to associate an event with an interface, then in the **Event Console** page, the link icon for this event will be for an interface and will lead to a performance report for the specific interface.

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

- **Auto-Clear.** If enabled, this field specifies whether an event can be cleared from the event list automatically. You can select one or more events from the list. The ScienceLogic platform automatically removes the current event from the **Event Console** 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 **Event Console**.

**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. The ScienceLogic platform automatically defines parent/child relationships when it discovers layer-2, CDP, LLDP, layer-3, and VMware topology. You can also manually define parent/child relationships between devices. For event correlation to occur, two types of events must be defined: *Suppressing Events* and *Suppressible Events*. For more details on topology suppression, see the chapter on [event correlation](#) in the **Events** manual.

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

- *Disabled.* This event is neither a parent event nor a child event.
- *Suppressing.* If this event occurs on a parent device, the platform will search all related children devices for suppressible events.
  - If you have assigned a **Category** to this event, the platform will search all the children devices and suppress all events that have been defined as *Suppressible* and are assigned to the same **Category**. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.
  - If you have not assigned a **Category** to this event, the platform will search all children devices and suppress all events that have been defined as *Suppressible* and are not assigned to a **Category**. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.

- The suppressible events will not appear in the **Event Console**. 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, the platform will suppress this event when it occurs on a child device and an event that has been defined as *Suppressing* occurs on its parent device. The suppressing event must have the same **Category** as the suppressible event. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.
    - If you have not assigned a **Category** to this event, when a *Suppressing* event that is not assigned to a **Category** occurs on the parent device the platform will search all children devices and suppress all events that have been defined as *Suppressible* and are not assigned to a **Category**. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.
    - The suppressible events will not appear in the **Event Console**. 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 the platform to more efficiently align suppressing events with suppressible events. When you align an event category to a suppressing or suppressible event, that event will be correlated with only events that are aligned with the same category. An event can be aligned to multiple categories; for event correlation to occur, the suppressing event and the suppressible event must both be aligned with a common category. For more details on event categories, see the chapter on [event correlation](#) in the **Events** manual.

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

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

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

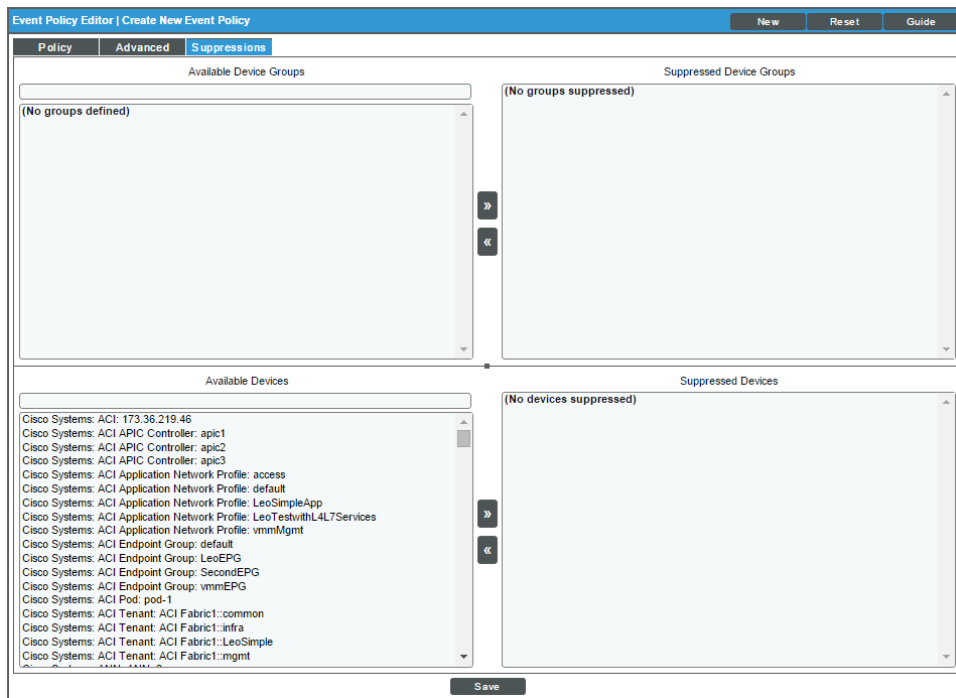
## Defining Event Suppressions in the Suppressions Tab

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

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

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



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

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

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

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

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

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

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

## Defining an Event Policy for a Specific Interface

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

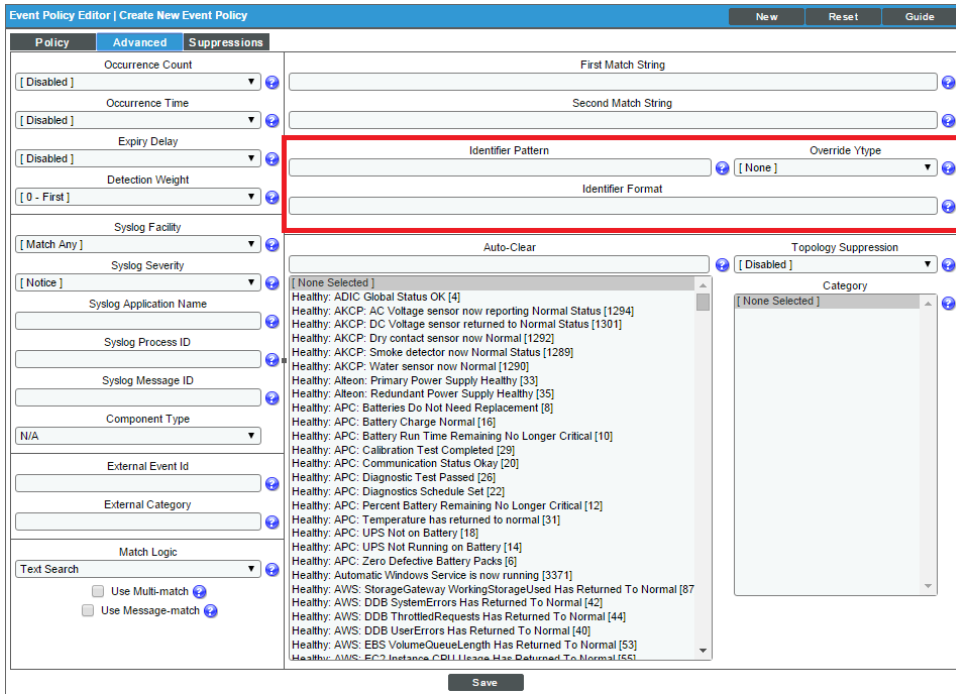
You can also include the interface name and the ScienceLogic platform's unique interface ID in automation policies associated with the event.

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

There are three database fields that the ScienceLogic platform 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 the ScienceLogic platform.

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

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

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

If these fields are used in an event:

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

## Defining Custom Severity for an Interface

In the **Interface Properties** page, you can define a custom severity for an interface. You can then configure an event to use this custom severity when the event occurs for that interface. For details on the **Interface Properties** page, see the chapter on *Network Interfaces* in the **Devices** manual.


For example, suppose interface Gi1/0/1 on a Cisco switch named cisco\_switch\_network1 is part of a mission-critical service. By default, event policies for interface events have a severity of "notice" or "major." You could define a custom severity modifier that increases the severity of those events to "critical" when they are generated for the Gi1/0/1 interface.

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

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

Now when any of those events occur on interface Gi1/0/1 on the switch cisco\_switch\_network1, the event will have an increased severity.

To define a custom severity for an interface:

1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).
2. Select the wrench icon () for the interface for which you want to view the **Interface Properties** page.

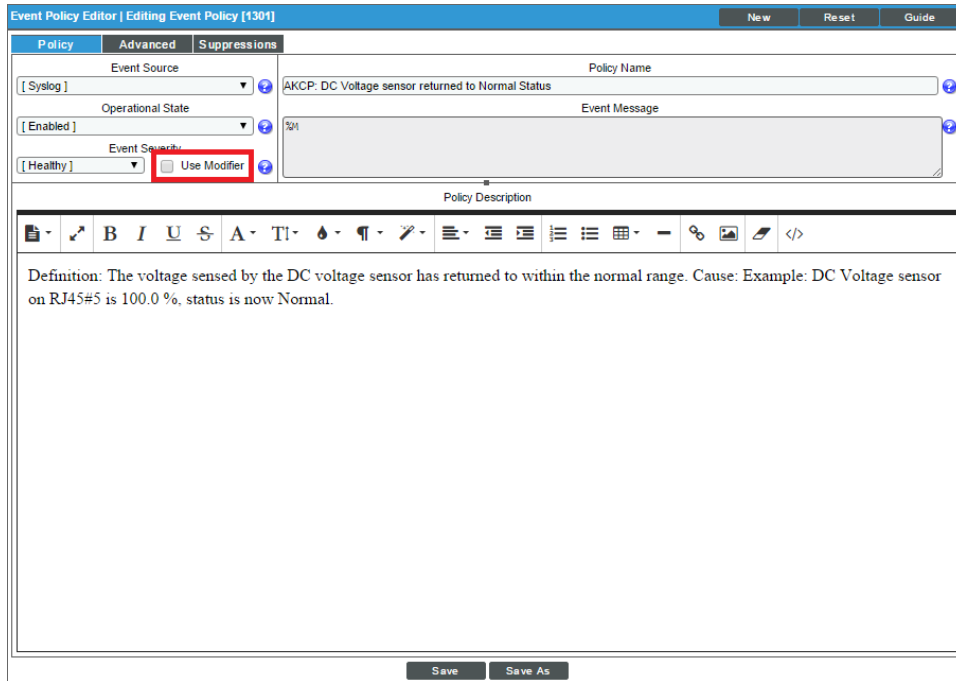
3. Supply a value in the **Event Severity Adjust** field. Select the **[Save]** button.

The screenshot shows the 'Interface Properties' window for interface 'e0a'. The 'Event Severity Adjust' dropdown menu is highlighted with a red box, showing '[ Default Severity ]' selected. Other fields include Interface Name, Port Description, MAC Address, IANA Type, Speed & Counter, Position & IfIndex, Admin/Oper Status, and TCP IP Address.

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

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

**CAUTION:** If you edit an event policy that was imported into your ScienceLogic 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 overwritten. For more information on PowerPacks, see the manual **PowerPacks**.



To edit an existing event policy:

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

Event Policy Name	Type	State	P-Pack	Severity	Weight	ID	Expiry	Time	Thresh	Colled By	Last Colled	External ID	Category
1 ADIC Global Status Failed	Dynamic	Enabled	Yes	Major	0	2	90 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--
2 ADIC Global Status OK	Dynamic	Enabled	Yes	Healthy	0	4	15 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--
3 ADIC Global Status Unknown	Dynamic	Enabled	Yes	Notice	0	3	30 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--
4 ADIC Tape Library Degraded	Dynamic	Enabled	Yes	Minor	0	1	60 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--
5 AKCP: AC Voltage sensor detects no current	Syslog	Enabled	Yes	Critical	0	1288	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
6 AKCP: AC Voltage sensor now reporting Normal Status	Syslog	Enabled	Yes	Healthy	0	1294	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
7 AKCP: DC Voltage High Warning	Syslog	Enabled	Yes	Major	0	1299	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
8 AKCP: DC Voltage sensor High Critical	Syslog	Enabled	Yes	Critical	0	1297	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
9 AKCP: DC Voltage sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1298	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
10 AKCP: DC Voltage sensor Low Warning	Syslog	Enabled	Yes	Major	0	1300	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
11 AKCP: DC Voltage sensor returned to Normal Status	Syslog	Enabled	Yes	Healthy	0	1301	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
12 AKCP: Dry Contact Sensor Low Critical	Syslog	Enabled	Yes	Critical	0	1287	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
13 AKCP: Dry contact sensor now Normal	Syslog	Enabled	Yes	Healthy	2	1292	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
14 AKCP: Humidity High Warning	Syslog	Enabled	Yes	Major	0	1295	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
15 AKCP: Humidity Low Warning	Syslog	Enabled	Yes	Major	0	1296	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
16 AKCP: Smoke Detector Alert!	Syslog	Enabled	Yes	Critical	10	1293	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
17 AKCP: Smoke detector now Normal Status	Syslog	Enabled	Yes	Healthy	4	1289	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
18 AKCP: Water Sensor has detected water	Syslog	Enabled	Yes	Critical	0	1291	90 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
19 AKCP: Water sensor now Normal	Syslog	Enabled	Yes	Healthy	0	1290	15 Min.	0 Min.	0	em7admin	2015-05-14 11:25:44	--	--
20 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. 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 in the **Event Console** page or the **Viewing Events** page for the device. 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 ScienceLogic 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 the ScienceLogic platform 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

The ScienceLogic platform includes automation features that allow you to define specific event conditions and the actions you want the platform to execute when those event conditions are met. These features can be found under the Registry > Run Book link in the NavBar.

This chapter provides an overview of these features.

---

### 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 the ScienceLogic platform 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 the ScienceLogic platform to an external device.
- Create a new ticket (using ticket templates defined in Registry > Ticketing > Templates page).
- Update an existing ticket.
- Write an SNMP value to an existing SNMP object on an external device.

- Execute a custom Snippet (Python program).
- Query a database.

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

---

## Creating Automation Policies and Action Policies

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

---

# Chapter

# 8

## Events from Email

---

### Overview

The ScienceLogic platform 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 the ScienceLogic platform, 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 the ScienceLogic platform to trigger events from those log entries.

---

### Configuring Events from Email

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

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

## RSS Feeds and Events

---

### Overview

The ScienceLogic platform includes two types of RSS feeds that can be used with events:

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

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

---

### Viewing Events with an RSS Feed

Custom RSS feeds allow you to view information about tickets and events without being logged in to the ScienceLogic platform. Custom RSS feeds from the platform can be viewed through a browser or through most free and commercially available feed viewers.

### Defining a Custom RSS Feed

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

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

1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds).



2. Select the **[Refresh]** button to clear any values from the fields in the editor pane.

3. In the **Global Settings** pane, supply values in the following fields:
  - **Feed Name.** Name of the feed. Can be any combination of alphanumeric characters, up to 64 characters in length.
4. In the **Custom RSS Feeds** page, under the **Ticket Settings** pane, you can specify the criteria that a ticket must meet to be included in the RSS feed. Supply values in the following fields:
  - **Ticket Queues.** The RSS feed will include tickets only from the selected queues. You can select from a drop-down list of all ticket queues that you are allowed to view. By default, no queues are selected. To enable the RSS feed, you must select at least one queue. For more information on ticket queues, see the chapter on *Ticket Queues* in the **Ticketing** manual.
  - **Assigned Only.** If you select this checkbox, the RSS feed will include only tickets that have been assigned.
  - **Status.** The RSS feed will include only tickets with the status you select. The choices are:
    - *All.* Tickets of all statuses will be included in the RSS feed.
    - *Open.* Only tickets with a status of Open will be included in the RSS feed.
    - *Working.* Only tickets with a status of Working will be included in the RSS feed.
    - *Pending.* Only tickets with a status of Pending will be included in the RSS feed.
    - *Resolved.* Only tickets with a status of Resolved will be included in the RSS feed.
    - *O/W/P.* All tickets with a status of open, working, or pending will be included in the RSS feed.

- **Minimum Severity.** The RSS feed will include only tickets with a severity equal to or greater than the severity you select. Choices are:
    - *Severity 5/Healthy.* All tickets will be included in the RSS feed.
    - *Severity 4/Notice.* Healthy tickets will **not** be included in the RSS feed.
    - *Severity 3/Minor.* Healthy tickets and Notice tickets will **not** be included in the RSS feed.
    - *Severity 2/Major.* Healthy, Notice, and Minor tickets will **not** be included in the RSS feed.
    - *Severity 1/Critical.* Healthy, Notice, Minor, and Major tickets will **not** be included in the RSS feed.
5. In the **Custom RSS Feeds** page, under the **Event Settings** pane, you specify the criteria that an event must meet to be included in the RSS feed. Supply values in the following fields:
- **For Organization.** This box will contain a list of all organizations about which you are allowed to view information. Select one or more organizations for which you want to view event information. (To select multiple organizations, hold down the **<Ctrl>** key while clicking.) The RSS feed will include only events assigned to the selected organization(s). Users must select at least one organization from this list.
  - **Unacknowledged Only.** Select this checkbox to include only unacknowledged events in the RSS feed. For details on acknowledging events, see the [section on acknowledging events](#).
  - **Age Less Than.** The RSS feed will include only events with an age equal to or less than the selected age.
  - **Minimum Severity.** The RSS feed will include only events with a severity equal to or greater than the severity you select. Choices are:
    - *Healthy.* All tickets will be included in the RSS feed.
    - *Notice.* Healthy tickets will **not** be included in the RSS feed.
    - *Minor.* Healthy tickets and Notice tickets will **not** be included in the RSS feed.
    - *Major.* Healthy, Notice, and Minor tickets will **not** be included in the RSS feed.
    - *Critical.* Healthy, Notice, Minor, and Major tickets will **not** be included in the RSS feed.
  - **Device Group Filter.** The RSS feed will include only events associated with devices in the selected device group. In this field, you can select a device group from a list of all device groups you are allowed to view. For more information on Device Groups, see the manual on **Device Groups and Templates**.
6. Click **[Save]** to save the new Custom RSS Feed.

## Editing a Custom RSS Feed

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

To edit an existing RSS feed:


1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds)
2. In the **Custom RSS Feeds** page, go to the RSS Feeds registry pane at the bottom of the page.


The screenshot displays the 'Custom RSS Feeds' configuration interface. It is divided into two main sections: a top configuration pane and a bottom registry table.

**Top Configuration Pane:**

- Global Settings:** Feed Name (text input).
- Ticket Settings:**
  - Ticket Queues: A list box containing '[All My Ticket Queues]', 'Asset Management', 'Bar', 'Change Management', 'Documentation', 'Facilities', 'Help Desk', 'Monitoring', 'Provisioning', and 'Service Level'.
  - Assigned Only:  [ Check = Enabled ]
  - Status: [ Open ] (dropdown)
  - Minimum Severity: [ Sev 0 / Healthy ] (dropdown)
- Event Settings:**
  - For Organization: A list box containing '[All Organizations]', 'Bar', 'Deep Thought', 'Foo', 'New Org', 'ScienceLogic', and 'System'.
  - Unacknowledged Only:  [ Check = Enabled ]
  - Age Less than: [ 1 hour ] (dropdown)
  - Minimum Severity: [ Healthy ] (dropdown)
  - Device Group Filter: [ All Device Groups ] (dropdown)
  - [ Save ] button

**Bottom Registry Table:**

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

3. Select the wrench icon (  ) of the RSS feed you want to edit.
4. The top pane will be populated with values from the selected RSS feed. You can edit one or more values.
5. Click **[Save]** to save your changes.

To delete an existing custom RSS feed

1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds).
2. In the **Custom RSS Feeds** page, go to the RSS Feeds registry pane, at the bottom of the page.

3. Select the bomb icon (💣) of the RSS feed you want to delete.

The screenshot displays the 'Custom RSS Feeds' configuration interface. It is divided into two main sections: configuration settings and a table of existing feeds.

**Configuration Settings:**

- Global Settings:** Includes a 'Feed Name' text field.
- Ticket Settings:** Includes a 'Ticket Queues' dropdown menu with options like 'Asset Management', 'Bar', 'Change Management', etc.
- Event Settings:** Includes a 'For Organization' dropdown menu with options like 'All Organizations', 'Bar', 'Deep Thought', etc.
- Assigned Only:** A checkbox labeled 'Check = Enabled'.
- Status:** A dropdown menu with 'Open' selected.
- Minimum Severity:** A dropdown menu with 'Sev 0 / Healthy' selected.
- Unacknowledged Only:** A checkbox labeled 'Check = Enabled'.
- Age Less than:** A dropdown menu with '1 hour' selected.
- Minimum Severity:** A dropdown menu with 'Healthy' selected.
- Device Group Filter:** A dropdown menu with 'All Device Groups' selected.
- A 'Save' button is located at the bottom right of the configuration area.

**RSS Feeds Table:**

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

A red circle highlights the bomb icon (💣) in the 'Unack'd Events' column for the 'Test' feed.

4. The RSS feed will be deleted from the ScienceLogic platform.

## Viewing a Custom RSS Feed

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

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

1. Go to the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds).
2. In the **Custom RSS Feeds** page, go to the RSS Feeds registry pane, at the bottom of the page.

3. Select the RSS icon (📡) of the RSS feed you want to view.

The screenshot shows an RSS feed interface. At the top, there is a yellow banner with the text "all\_events\_tickets" and a "Subscribe to this feed" button. Below this, the feed displays a list of events and tickets. Each entry includes a heading, a date, and a brief description. For example, the first entry is "Major Event [296] | File system usage exceeded (major) threshold Limit: 85% Actual: 85.26% /data.local" dated "Today, June 16, 2010, 1 hour ago". The second entry is "Notice Event [295] | -Test Description-" dated "Today, June 16, 2010, 3 hours ago". The third entry is "Critical Event [290] | Ticket For Device: 10.20.30.131" dated "Monday, June 14, 2010, 6:09:35 PM". The fourth entry is "Critical Event [291] | Ticket For Device: 10.20.30.20" dated "Monday, June 14, 2010, 6:09:35 PM". The fifth entry is "Critical Event [292] | Ticket For Device: 10.20.30.73" dated "Monday, June 14, 2010, 6:09:35 PM". The sixth entry is "Critical Event [293] | Ticket For Device: 10.20.30.137" dated "Monday, June 14, 2010, 6:09:35 PM". On the right side, there is a sidebar with "Displaying 295 / 295" and "Sort by: All".

4. The RSS feed displays in a browser window.
  - The window displays a list of all entries in the feed, and details on each entry (event or ticket).
  - Clicking on the ticket heading displays a new window containing the Ticket Report for that ticket.
  - In the Ticket Report, clicking on the "click here to login" link takes the user to the ScienceLogic appliance where the ticket resides. Depending upon key privileges, users can then edit the ticket. Any changes to the ticket are dynamically updated in the RSS feed.

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

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

---

## Defining an External RSS Feed to Trigger Events

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

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

The ScienceLogic platform allows you to monitor the following types of RSS feeds:

- RSS 1.0+
- RSS 2.0+
- ATOM

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

## Viewing the List of Monitored RSS Feeds

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

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

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

## Defining an RSS Feed to Monitor

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

1. Go to the **RSS News Feed Manager** page (Registry > Events > RSS Feeds).
2. In the **RSS News Feed Manager** page, select the **[Create]** button.

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

The screenshot shows a modal window titled "Add RSS Feed" with a "Close / Esc" button in the top right corner. Inside the modal is a form titled "RSS Feed Editor" with the following fields:

- Channel Name:
- RSS URL:
- Organization: [System] (dropdown)
- Collection: [Enabled] (dropdown)
- Eventing/Severity: [None] (dropdown)
- Collector: em7\_a0 (dropdown)

A "Save" button is located at the bottom center of the form.

4. In the **RSS Feed Editor** modal page, supply a value in each of the following fields:
  - **Channel Name**. Name of the RSS feed. If you choose to trigger events based on updates to the RSS feed, this value will appear in the **Entity** field of the event.
  - **RSS URL**. URL of the RSS feed.
  - **Organization**. Organization to associate with this monitoring policy.
  - **Collection**. Specifies whether the ScienceLogic platform should retrieve data from the RSS feed. Choices are *Enabled* or *Disabled*.
  - **Eventing**. Specifies whether the ScienceLogic platform will create an event when a new article is detected in the RSS feed. Select from the drop-down list:
    - *None*. No event appears when new articles are detected.
    - *Event Console*. A description of the new article appears as an event in the **Event Console** page.
  - **Severity**. If new articles will trigger an event in the **Event Console** page, specifies the severity of the event. Select from the drop-down list of all event severities.
  - **Collector**. Specifies the Data Collector that will monitor the RSS feed. Select from the available choices in the drop-down list. For All-In-One Appliances, this field does not apply.
5. Click [**Save**] to save the policy and monitor the RSS feed.

## Editing a Monitored RSS Feed

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

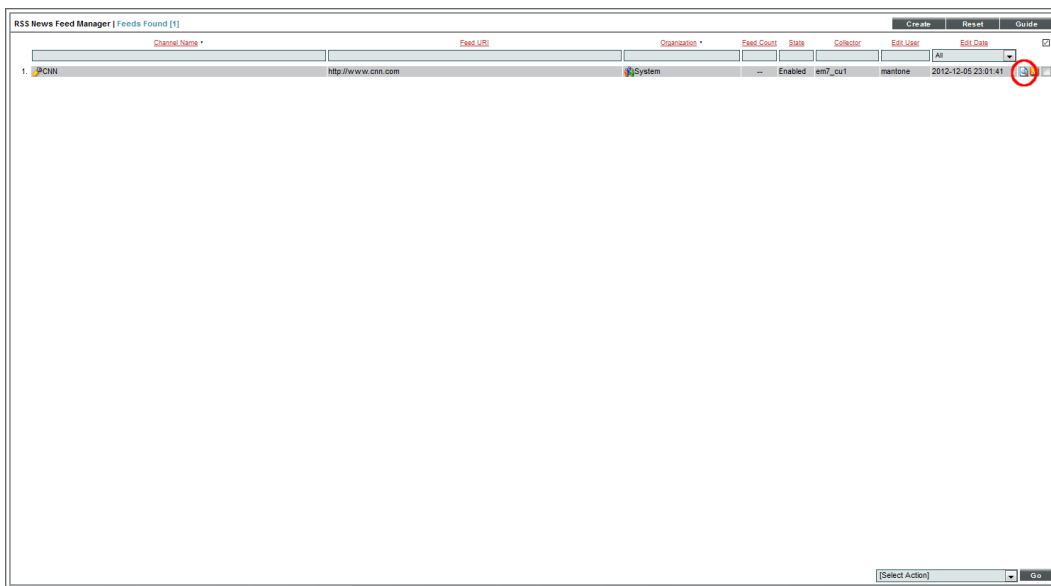
1. In the **RSS News Feed Manager** page, select the wrench icon (🔧) of the monitored RSS feed you want to edit.

2. The **RSS Feed Editor** page appears, populated with values from the monitored RSS feed you selected.
3. In the **RSS Feed Editor**, you can edit the values in one or more fields. For a description of each field, see the previous section on [Defining an RSS Feed to Monitor](#).
4. Click **[Save]** to save your changes to the policy.

## Viewing Articles from an RSS Feed

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

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





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

For Organization [ System ] | Channel: CNN | Articles Found [16]

Search where Title is like  Search

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

Delete

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

**News Feed Articles**

[Airport Wi-Fi and mobile services are lacking](#)

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

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

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

## Performing Administrative Tasks on One or More Monitored RSS Feeds

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

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

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



2. In the **Select Action** drop-down list, select one of the following actions:
  - **DELETE Feed Policy.** Deletes the monitored RSS feed. The ScienceLogic platform no longer monitors that RSS feed.
  - **ENABLE Collection.** The ScienceLogic platform will retrieve data from the selected news-feed policies.
  - **DISABLE Collection.** The ScienceLogic platform will not retrieve data from the selected news-feed policies.
  - **ENABLE Eventing.** The ScienceLogic platform will display an event when a new article is detected in the RSS feed.
  - **DISABLE Eventing.** The ScienceLogic platform will not display an event when a new article is detected in the RSS feed.

- *Move News Feed To (list of organizations)*. Associate selected news feed policies with selected organization.
- *Change Collector (list of collectors)*. Associate selected news feed policies with selected collector.

3. The selected action will be applied to each selected RSS feed.

## Reports for Events

---

### Overview

The ScienceLogic platform provides the following types of reports on events:

- **Event Statistics report from the Event Console page.** This report displays information about all active events on all devices in the ScienceLogic platform.
- **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 the ScienceLogic platform.
- **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.

The following sections describe each type of event report.

---

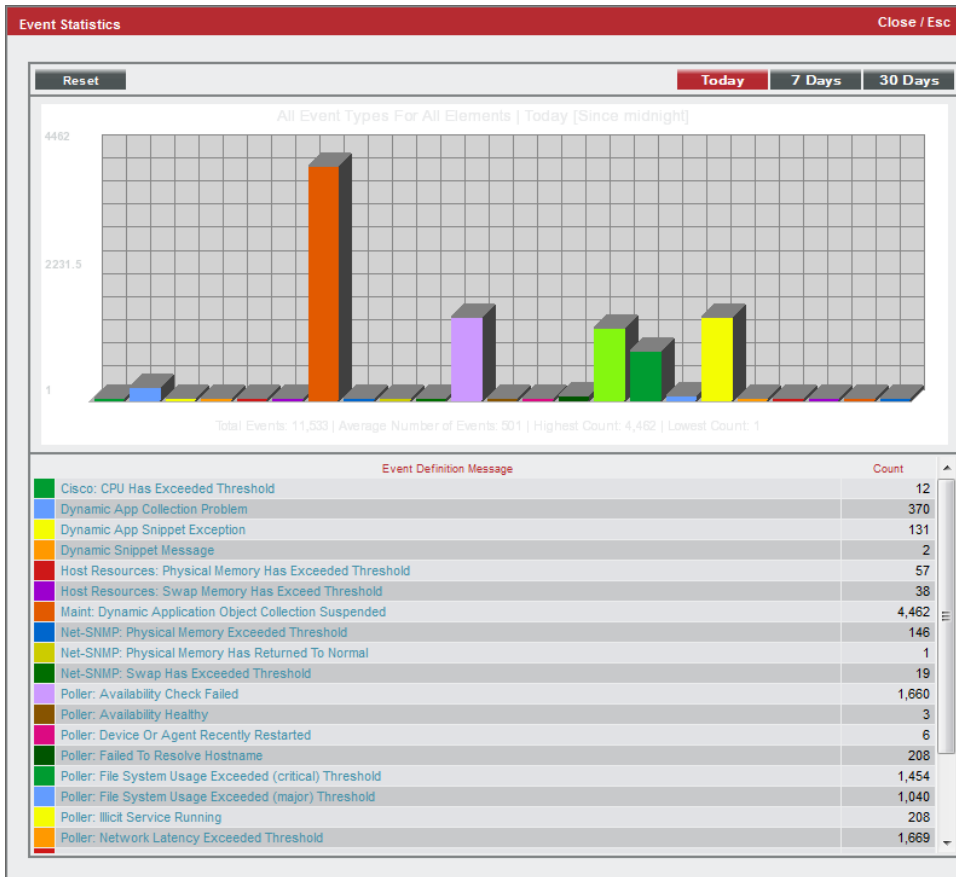
### Event Statistics in the Event Console page

The **Event Statistics** modal page 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:

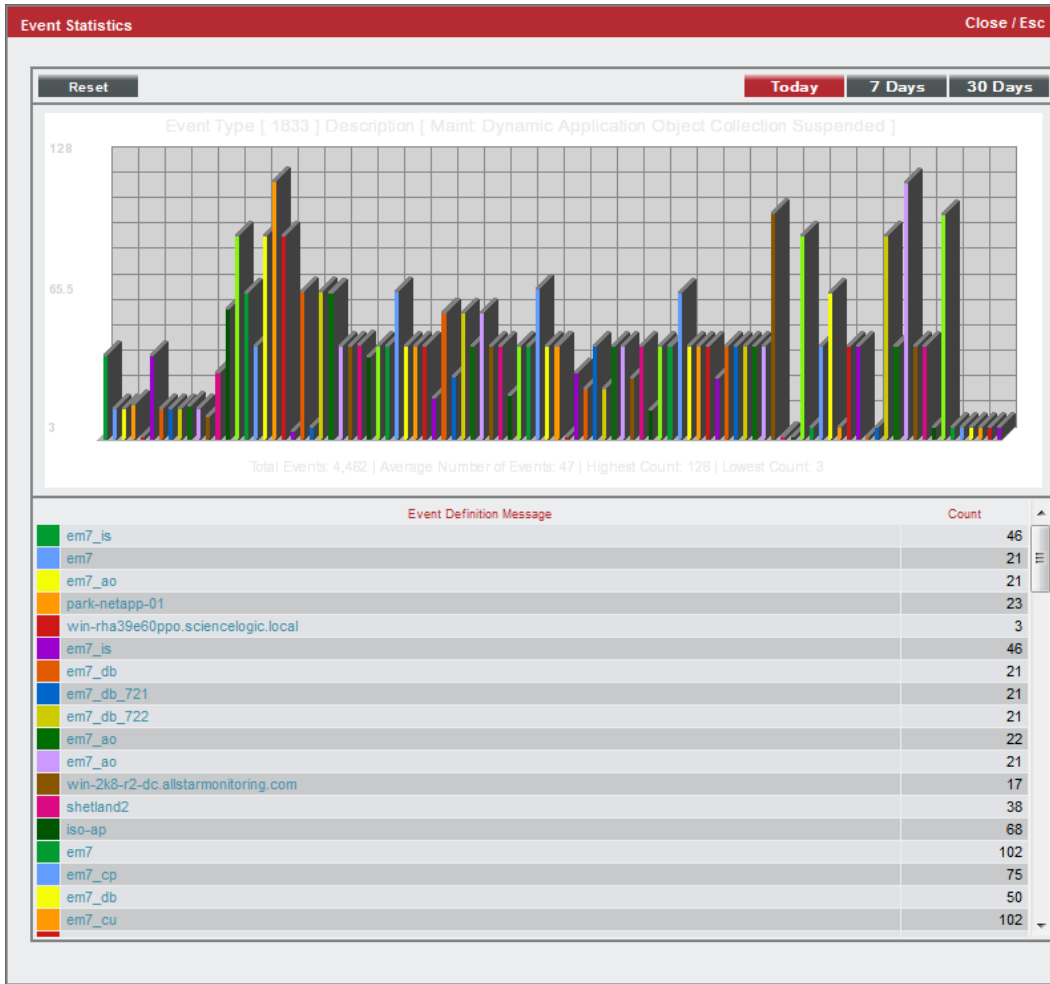
1. Go to the **[Events]** tab.
2. In the **Event Console** page, in the **[Actions]** drop-down list, select **Event Statistics**.
3. The Event Statistics report is displayed.
4. Initially, the **Event Statistics** page displays the bar graph "All Event Types for All Elements" for the past day.



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.

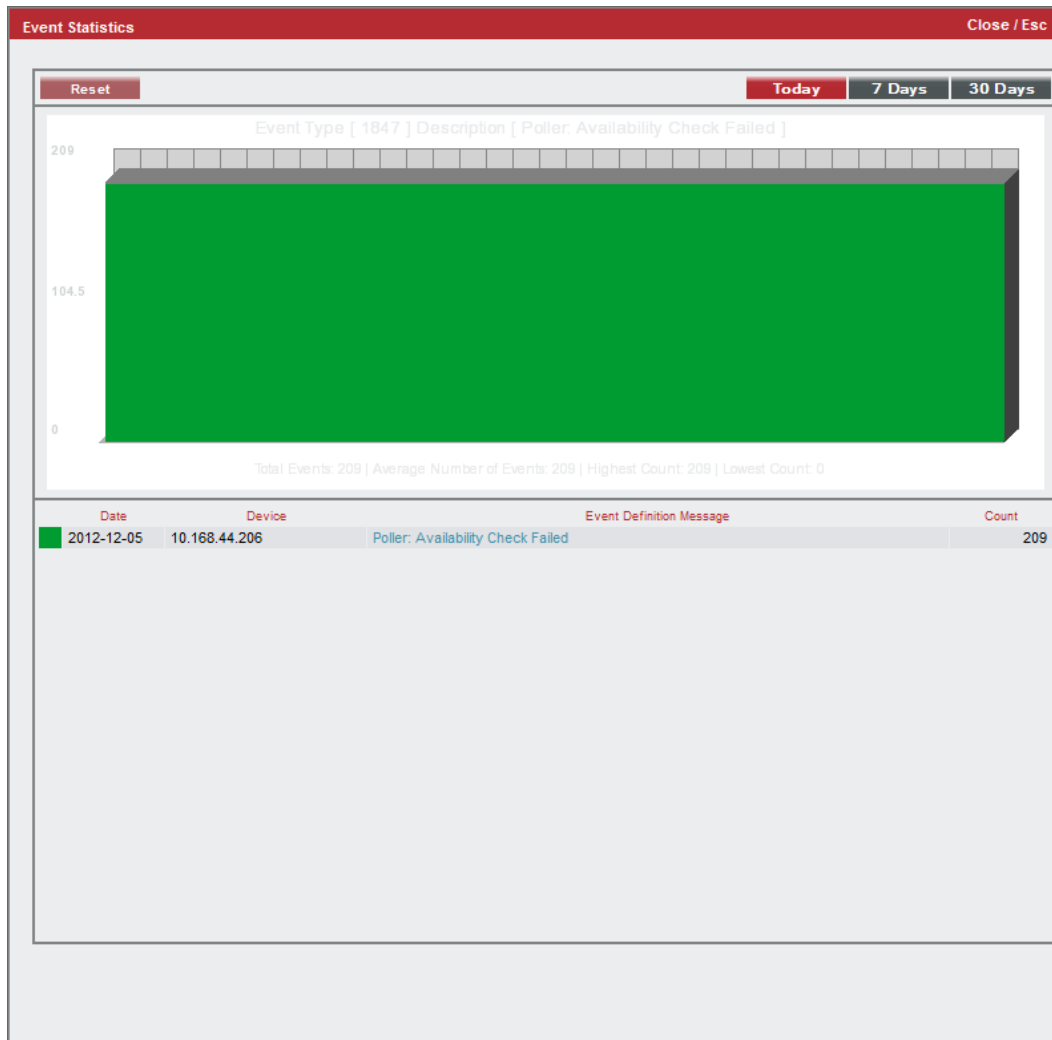
6. Clicking on a bar displays the "Single Event Type on All Elements" bar graph.



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:

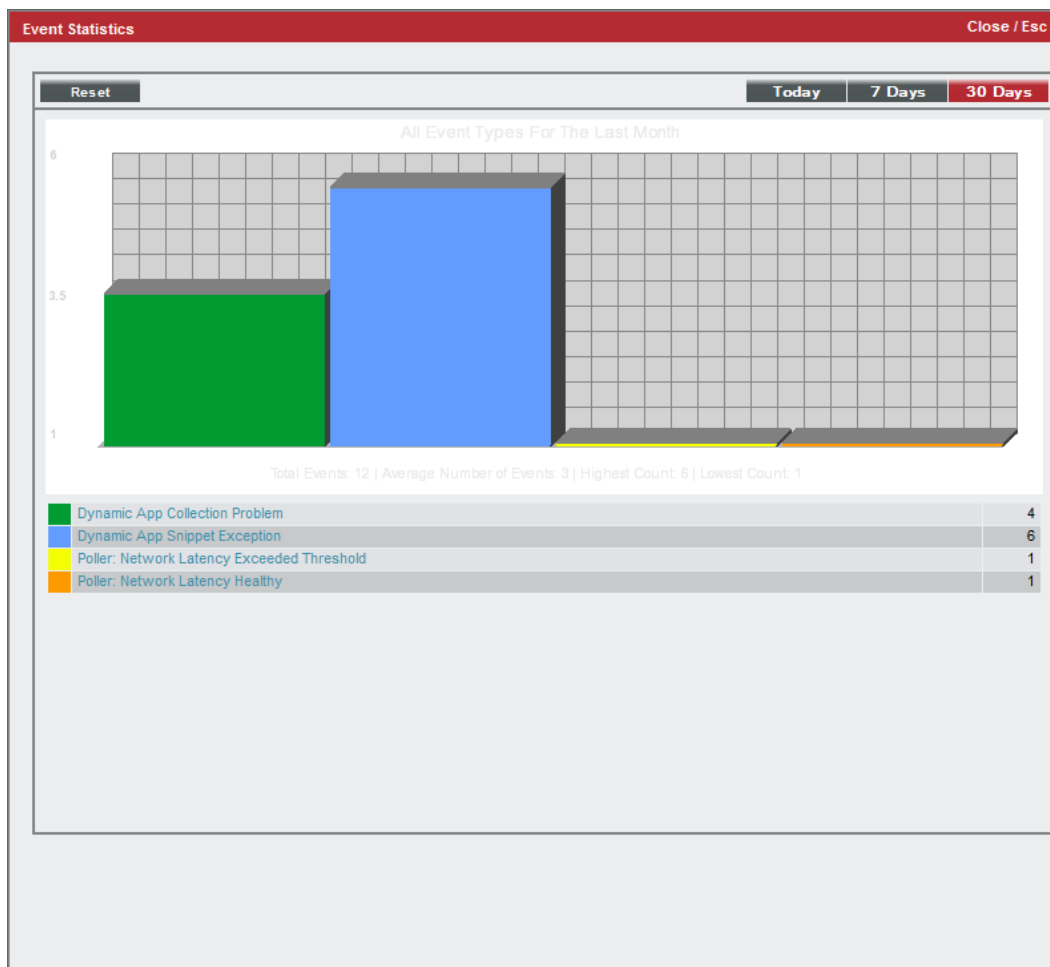
1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, select the bar graph icon (📊) for the device for which you want to view Event Statistics.

Device Name	IP Address	Device Category	Device Class   Sub-class	DID	Organisation	Current State	Collection Group	Collection State	SNMP Credentials	SNMP Version
1	10.0.9.10	Servers	NetApp   LUN	213	System	🟢 Healthy	CUG	Active	SNMP Public V1	V1
2	10.0.9.10	Servers	NetApp   LUN	1782	System	🟢 Healthy	CUG	Active	SNMP Public V1	V1
3	10.0.9.10	Servers	NetApp   LUN	1783	System	🟢 Healthy	CUG	Active	SNMP Public V1	V1
4	10.0.12.50	Pingable	Linux   ICMP	203	System	🟡 Major	CUG	Active	cSnmS	V2
5	10.0.9.12.51	Pingable	Linux   ICMP	204	System	🟢 Healthy	CUG	Active	--	--
6	10.0.9.10	Pingable	Ping   ICMP	1778	System	🟡 Major	CUG	Active	--	--
7	10.0.9.11	Pingable	Ping   ICMP	1779	System	🟡 Major	CUG	Active	--	--
8	10.0.9.110	Pingable	Linux   ICMP	1817	System	🟢 Healthy	CUG	Active	--	--
9	10.0.9.117	Pingable	Linux   ICMP	1816	System	🟡 Major	CUG	Active	--	--
10	10.0.9.118	Pingable	Linux   ICMP	1815	System	🟢 Healthy	CUG	Active	--	--
11	10.0.9.121	Pingable	Ping   ICMP	1785	System	🟢 Healthy	CUG	Active	--	--
12	10.0.9.125	Pingable	Linux   ICMP	1796	System	🟢 Healthy	CUG	Active	--	--
13	10.0.9.126	Pingable	Linux   ICMP	1798	System	🟢 Healthy	CUG	Active	--	--
14	10.0.9.127	Pingable	Linux   ICMP	1797	System	🟢 Healthy	CUG	Active	--	--
15	10.0.9.152	Pingable	FreeBSD   ICMP	1860	System	🟢 Healthy	CUG	Active	--	--
16	10.0.9.164	Pingable	Linux   ICMP	1823	System	🟢 Healthy	CUG	Active	--	--
17	10.0.9.185	Pingable	Ping   ICMP	1850	System	🟢 Healthy	CUG	Active	--	--
18	10.0.9.187	Pingable	Ping   ICMP	1849	System	🟢 Healthy	CUG	Active	--	--
19	10.0.9.189	Pingable	Linux   ICMP	1843	System	🟢 Healthy	CUG	Active	--	--
20	10.0.9.201	Pingable	Linux   ICMP	1799	System	🟢 Healthy	CUG	Active	--	--
21	10.0.9.239	Pingable	Linux   ICMP	1822	System	🟢 Healthy	CUG	Active	--	--
22	10.0.9.40	Pingable	FreeBSD   ICMP	1819	System	🟢 Healthy	CUG	Active	--	--
23	10.0.9.63	Pingable	Linux   ICMP	1841	System	🟢 Healthy	CUG	Active	--	--
24	10.0.9.8	Pingable	Ping   ICMP	1867	System	🟡 Major	CUG	Active	--	--
25	10.0.9.81	Pingable	Linux   ICMP	1861	System	🟢 Healthy	CUG	Active	--	--
26	10.0.9.9	Pingable	Ping   ICMP	1868	System	🟡 Major	CUG	Active	--	--
27	10.168.44.206	Pingable	Ping   ICMP	224	System	🟡 Major	CUG	Unavailable	--	--
28	10.100.100.46	Pingable	FreeBSD   ICMP	1741	System	🟢 Healthy	CUG	Active	cSnmS	V2
29	10.0.9.100	Unknown	Avocent   OEM	1829	System	🟢 Healthy	CUG	Active	cSnmS	V2
30	10.0.9.1	Servers	NetApp   Aggregate	227	System	🟡 Minor	CUG	Active	SNMP Public V1	V1
31	10.0.9.1	Servers	NetApp   Aggregate	1760	System	🟢 Healthy	CUG	Active	SNMP Public V1	V1
32	10.0.9.30	Network Switches	Cisco Systems   Catalyst 6509-CatOS	1799	System	🟡 Major	CUG	Active	SNMP Public V2	V2
33	10.0.9.31	Network Router	Cisco Systems   12800Y06	1801	System	🟡 Major	CUG	Active	SNMP Public V2	V2
34	10.0.9.32	Network Router	Cisco Systems   2811	1800	System	🟡 Major	CUG	Active	SNMP Public V2	V2
35	10.0.9.33	Network Router	Cisco Systems   2811	1802	System	🟡 Major	CUG	Active	SNMP Public V2	V2
36	10.0.9.35	Network Router	Cisco Systems   3845	1804	System	🟡 Major	CUG	Active	SNMP Public V2	V2
37	10.0.9.35	Control Domain on host: xenserver-misc	Xen VM   Xen VM	222	System	🟢 Healthy	CUG	Active	--	--
38	10.0.9.35	Control Domain on host: xenserver-misc	Xen VM   Xen VM	221	System	🟢 Healthy	CUG	Active	--	--
39	10.0.9.35	Control Domain on host: xenserver-misc	Xen VM   Xen VM	1748	System	🟢 Healthy	CUG	Active	--	--
40	10.0.9.35	Control Domain on host: xenserver-misc	Xen VM   Xen VM	1759	System	🟢 Healthy	CUG	Active	--	--
41	10.0.9.35	Control Domain on host: xenserver-misc	Xen VM   Xen VM	1756	System	🟢 Healthy	CUG	Active	--	--
42	10.0.9.35	Control Domain on host: xenserver-misc	Xen VM   Xen VM	1757	System	🟢 Healthy	CUG	Active	--	--
43	10.0.9.35	Control Domain on host: xenserver-misc	Xen VM   Xen VM	1755	System	🟢 Healthy	CUG	Active	--	--

3. The ScienceLogic platform displays the **Device Reports** panel for the device. In the **Device Reports** panel for the device, select the **[Events]** tab.
4. The **Viewing Events** page appears. In the **Viewing Events** page, select the **[Stats]** button.
5. The **Event Statistics** page appears.

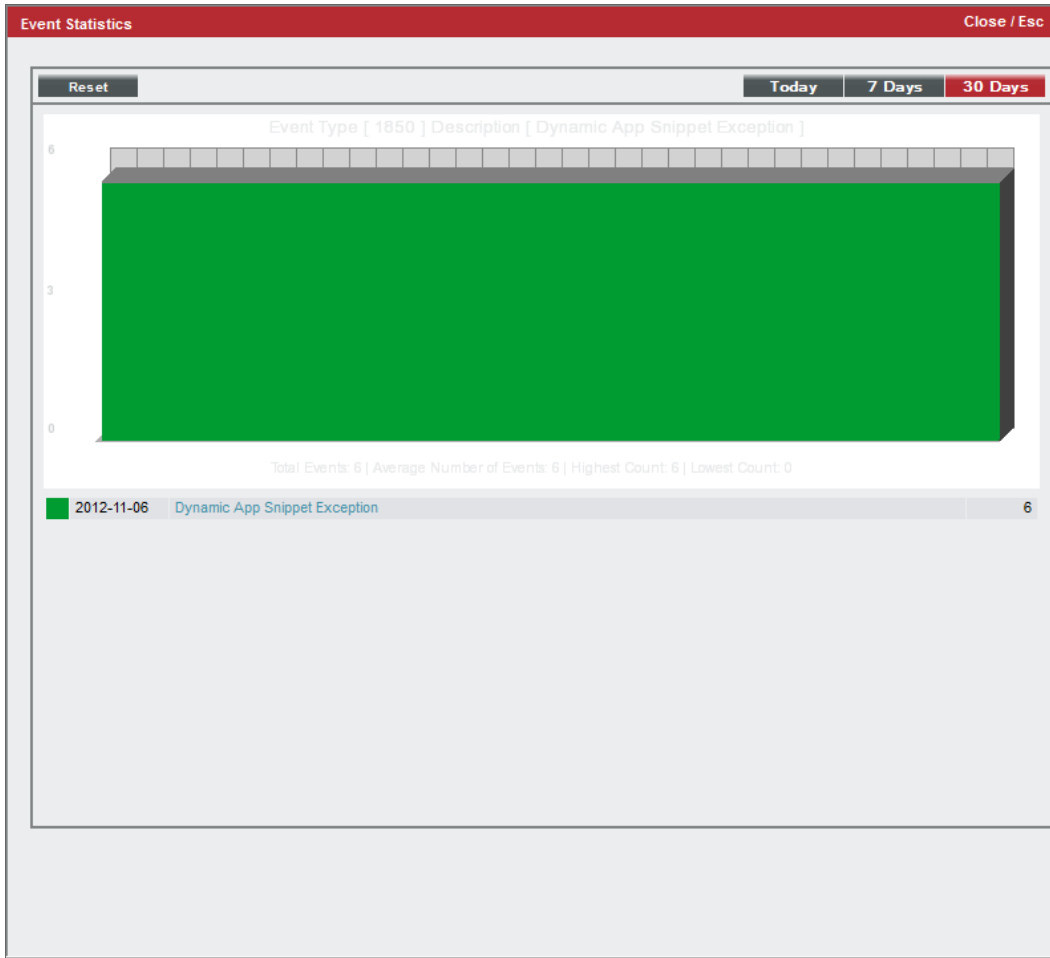


6. By default, the **Event Statistics** page displays the graph "All Event Types for the Last Month." This graph displays all events that have occurred on the device this month. This graph displays:



- 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.

7. 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]** tab allows you to create custom reports as well as view predefined reports. The ScienceLogic platform includes many predefined reports 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, the ScienceLogic platform automatically removes the current event from the **Event Console**. 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 **Event Console**.
- 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** tab, see the chapter on *Default Reports* in the **Reports** manual.

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

## Event Clear Map Report

To generate and view the Event Clear Map report:

1. Go to the **Run Quick Report** page for the Event Clear Map report (Reports > Run Report > Events > Event Clear Map).

2. Supply values in the following fields:

- **Sort By.** Specifies how the report will be organized. Choices are:
  - *Severity.* Events will be grouped by severity.
  - *Event Name.* Events will be listed alphabetically by event name. The secondary sort will be by severity.
  - *Event ID.* Events will be listed by event policy ID. Event ID is a unique numerical ID assigned by the ScienceLogic platform 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 the ScienceLogic platform 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**.

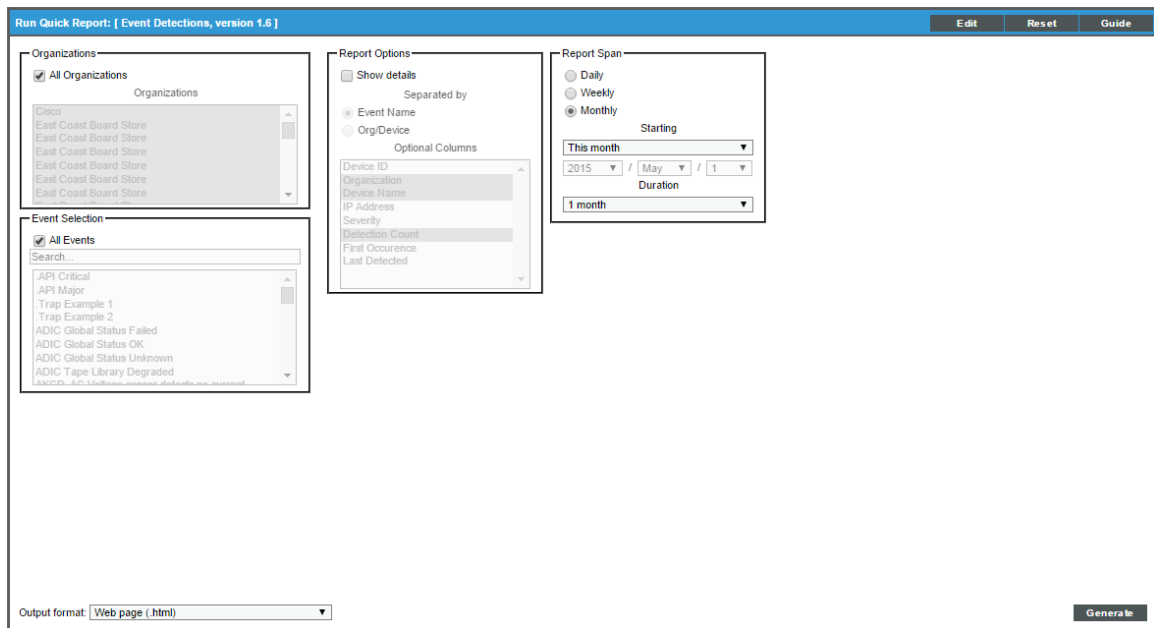
- **Cleared Event**. The name of the event.
- **Severity**. The severity of the event. Choices are Healthy, Notice, Minor, Major, and Critical.
- **Source**. Specifies the source for the event. Choices are:
  - *Syslog*. Standard log format supported by most networking and UNIX-based devices and applications. Windows log files can be converted to syslog format using conversion tools.
  - *Internal*. Message generated by the ScienceLogic platform.

- *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 the ScienceLogic platform. A trap indicates that an emergency condition or a condition that merits immediate attention has occurred on the device.
  - *Dynamic*. Message generated by the ScienceLogic platform's Dynamic Application tool. This tool allows the ScienceLogic platform 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 the ScienceLogic platform 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 ( $\leq 0 = 0 = \geq$ ) or whether the event to the right clears the event to the left ( $0 = = >$ ).
  - **Clearing Event**. Name of the event defined to auto-clear the event in **Cleared Event**.

## Event Detections Report

To generate and view the Event Detections report:

1. Go to the **Run Quick Report** page for the Event Detections report (Reports > Run Report > Events > Event Detections).



2. Supply a value in each of the following fields:

- **All Organizations.** All events associated with all organizations will be included in the report.
- **Organizations.** This list contains an entry for each organization in the ScienceLogic platform. 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 the ScienceLogic platform.
  - 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 the ScienceLogic platform will save the generated report. Choices are:
  - *ODF Spreadsheet*. Displays the output in the OpenOffice spreadsheet application.
  - *Microsoft Excel*. Displays the output in an .xlsx file.
  - *Web page*. Displays the output in an .html file.
  - *Adobe Acrobat*. Displays the output in a .pdf file.
- **[Generate]**. This button generates the report, using the parameters you specified in this page.

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

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

## Unique Event Detections Report

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

Device		Event Type	Jul 2015	Total
em7-ib1.lit [4]	em7-ib1.lit [4]	Net-SNMP: Physical Memory exceeded threshold	1	1
em7-ib1.lit [4]	em7-ib1.lit [4]	Poller: Added application monitoring for device	2	2
WIN-2012-22	DOCS.LOCAL [74]	Poller: Availability Check Failed	1	1
WIN-2012-22	DOCS.LOCAL [74]	Poller: Network Latency Exceeded Threshold	1	1
em7_a0 [1067]	em7_a0 [1067]	Dynamic App Snippet Exception	2	2
em7_a0 [1067]	em7_a0 [1067]	Poller: Added application monitoring for device	2	2
em7_a0 [1067]	em7_a0 [1067]	Poller: Device or agent recently restarted	1	1
em7_a0 [1067]	em7_a0 [1067]	Poller: Network Latency Exceeded Threshold	1	1
em7_a0 [1067]	em7_a0 [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
<b>Sum for Organization: TCP</b>			<b>20</b>	<b>20</b>



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'. It features several configuration panels: 'Device Selection' (with 'All devices' selected and lists for 'Organizations' and 'Devices by Organization'), 'Separated by' (with 'Organization' selected), 'Sort by' (with 'Organization' selected), 'Event Types' (with 'All events' selected and a list of event types), 'Report Span' (with 'Monthly' selected and 'Starting' set to 'This month'), 'Report Sections' (with 'Both' selected), and an 'Output format' dropdown 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 the ScienceLogic platform 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 the ScienceLogic platform. 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

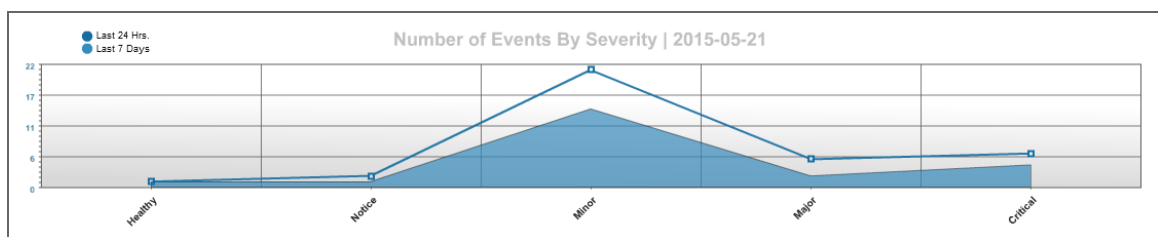
The **Event Overview** page includes a **Select Date** drop-down list in the upper right of the page. This drop-down allows you to define the date for the reports on this page.

- **Select Date.** Allows you to select a date. The ScienceLogic platform 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, the ScienceLogic platform 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

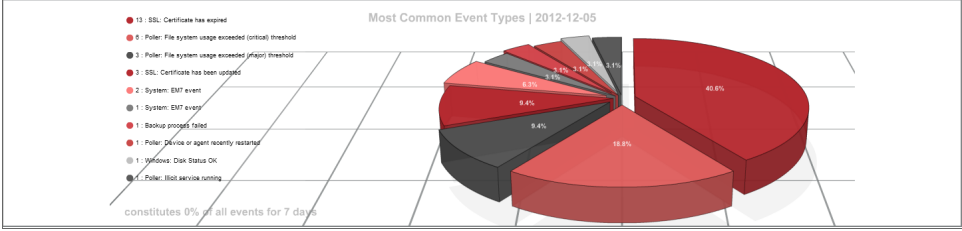
This graph displays event distribution by severity for the last 24 hours and for the last 7 days.



- 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

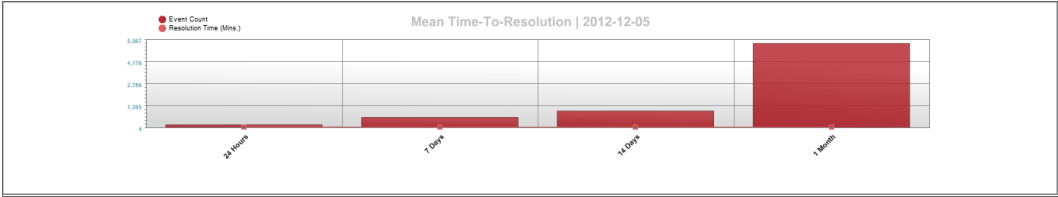
This pie graph displays the ten most frequently occurring events for the last seven days.



- 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.

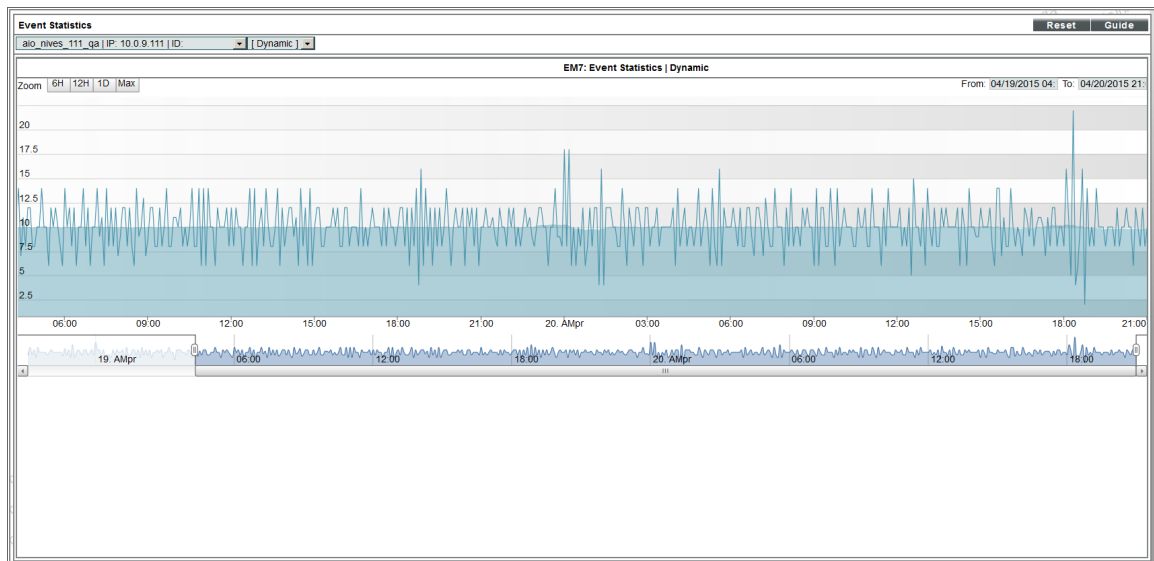
## Fields

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 the ScienceLogic platform.
  - *Trap*. Event was generated by an SNMP trap.
  - *Dynamic*. Event was generated by a Dynamic Application alert.
  - *API*. The event was generated by an external API.
  - *Email*. The event was generated by an incoming email.

## The Graph

The graph displays the average number of events processed by the selected ScienceLogic server, for the selected duration.



- The y-axis displays the average number of events.
- The x-axis displays time. The increments vary, depending upon the selected date range (from the **Preset** buttons).
- Mousing over any point in any line displays the high, low, and average value at that time-point in the **Data Table** pane.
- You can use your mouse to scroll the report to the left and right.

## Settings that Affect Events

---

### Overview

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

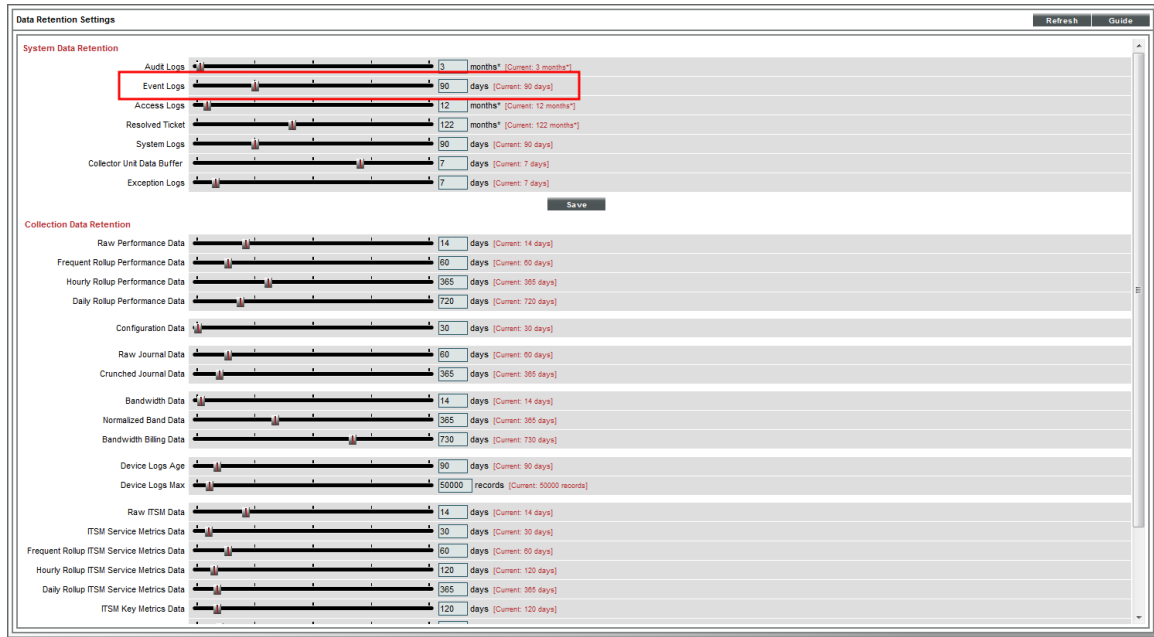
---

### Data Retention Settings that Affect Events

To define data retention settings for events, perform the following steps:

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:



- **Event Logs.** You can select the number of days that the ScienceLogic platform 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, perform the following steps:

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



2. In the **Behavior Settings** page, the following system setting affects events:

The screenshot shows the 'Behavior Settings' page with two columns of settings. The 'Event Clearing Mode' setting is highlighted with a red box. The settings are as follows:

Setting Name	Value
Interface URL	http://10.0.9.206
Force Secure HTTPS	<input type="checkbox"/>
Password Expiration	[ disabled ]
Password Hash Method	[ SHA-512 (FIPS 140-2 compliant) ]
Account Lockout Type	[ Lockout by Username (default) ]
Account Lockout Attempts	[ 3 attempts ]
Single Instance Login (Admins)	[ Disabled ] -1
Single Instance Login (Users)	[ Disabled ] -1
Account Lockout Duration	[ 1 hour ]
Lockout Contact Information	800-SCH-LOGIC
Login Header Title	
System Identifier	
Ping & Poll Timeout (Msec)	[ 1000 ]
SNMP Poll Timeout (Msec)	[ 1000 ]
SNMP Failure Retries	[ 1 ]
DHCP Community Strings (Comma separated)	public
Strip FQDN From Inbound Email Device Name	[ Enabled ]
Event Console Ticket Life Ring Button Behavior	[ Create / View EM7 Ticket ]
API Internal Req Account	[ em7admin ]
Prevent Browser Saved Credentials	<input type="checkbox"/>
Use CDP Topology	<input checked="" type="checkbox"/>
Enable Community String indexing (VLAN Topology)	<input type="checkbox"/>
Default Country	[ United States ]
System Timezone	[ L Eastern ]
NFS Detection Disable	<input checked="" type="checkbox"/>
Port Polling Type	[ Half Open ]
Initial Discovery Scan Level	[ 0. Model Device Only ]
Rediscovery Scan Level (Nightly)	[ 0. Model Device Only ]
Discovery Scan Throttle	[ Disabled ]
Port Scan All IPs	[ 0. Disabled ]
Port Scan Timeout	[ 120000 Msec ]
Restart Windows Services (Agent required)	[ 0. Disabled ]
Hostname Precedence	[ DNS Reverse Lookup ]
Interface Name Precedence	[ Interface Name ]
DNS Hostnames	[ Strip Domain Name (Hostname) ]
Event Clearing Mode	[ Clear Selected Only ]
Patch Maintenance Minimum Severity	[ 2. Minor ]
SSL Certificate Expiry Soon	[ 4 months ]
SSL Certificate Expiry Imminent	[ 1 week ]
Asset Warranty Expiry	[ 1 month ]
Domain Name Expiry	[ 1 month ]
Validate Phone Number	[ Disabled ]

- **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 in the **Event Console**.



## System Settings that Affect Event Tickets

The behavior of the life-ring icon (🔔) in the **Event Console** is determined in the **Behavior Settings** page (System > Settings > Behavior). To change this behavior:

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

The screenshot shows the 'Behavior Settings' page with various configuration options. The 'Event Console Ticket Life Ring Button Behavior' field is highlighted with a red box and set to 'Create / View EM7 Ticket'. Other visible settings include 'Interface URL' (http://em7.mydomain.com), 'Force Secure HTTPS' (checked), 'Password Expiration' (disabled), 'Password Hash Method' (MD5 legacy), 'Password Minimum Length' (8), 'Account Lockout Type' (Lockout by Username), 'Account Lockout Attempts' (2 attempts), 'Login Delay' (Disabled), 'Single Instance Login (Admins)' (Disabled), 'Single Instance Login (Users)' (Disabled), 'Account Lockout Duration' (1 hour), 'Lockout Contact Information' (800-SCH-LOGIC), 'Login Header Title', 'System Identifier', 'Ping & Poll Timeout (Msec.)' (1000), 'SNMP Poll Timeout (Msec.)' (1000), 'SNMP Failure Retries' (1), 'Initially Discovered Interface Poll Rate' (15 minutes), 'DHCP Community Strings (Comma separated)' (public), 'Strip FQDN From Inbound Email Device Name' (Enabled), 'Prevent browser saved Credentials' (checked), 'Display Previous Login in Footer' (unchecked), 'Prevent Loading Interface in External Frames' (checked), 'Ignore trap agent-addr varbind' (unchecked), 'Hide Perpetual License Usage' (checked), 'Use CDP Topology' (checked), 'Enable Community String Indexing (VLAN Topology)' (unchecked), 'Default Country' (United States), 'System Timezone' (UTC), 'NFS Detection Disable' (checked), 'Port Polling Type' (Half Open), 'Initial Discovery Scan Level' (Advanced Port Discovery), 'Rediscovery Scan Level (Nightly)' (Advanced Port Discovery), 'Discovery Scan Throttle' (Disabled), 'Port Scan All IPs' (Enabled), 'Port Scan Timeout' (120000 Msec), 'Restart Windows Services (Agent required)' (Disabled), 'Hostname Precedence' (SNMP System Name), 'Interface Name Precedence' (Interface Name), 'DNS Hostnames' (Strip Domain Name (Hostname)), 'Event Clearing Mode' (Clear All in Group), 'Maintenance Minimum Severity' (Healthy), 'Patch Maintenance Minimum Severity' (Healthy), 'SSL Certificate Expiry Soon' (4 months), 'SSL Certificate Expiry Imminent' (1 week), 'Asset Warranty Expiry' (1 month), 'Domain Name Expiry' (1 month), 'Validate Phone Number' (Disabled), and 'Dashboard Maximum Series Count Per Widget' (8).

2. Select from the following options in the **Event Console Ticket Life Ring Button Behavior** field:

- **Create/View EM7 Ticket.** When you select the life-ring icon (🔔) for an event in the **Event Console**, the ScienceLogic platform will display the **Ticket Editor** page, where you can define a ScienceLogic 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 life-ring icon (🔔) for that event (from the **Event Console**), the ScienceLogic platform 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, the ScienceLogic platform 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 - 2018, 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](mailto:legal@sciencelogic.com)



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

International: +1-703-354-1010