



Run Book Automation

SL1 version 10.1.0

Table of Contents

Introduction	4
What is Run Book?	5
Custom Settings	5
Automation Policies	6
Action Policies	8
Automation Policies	9
What is an Automation Policy?	10
Before You Begin	11
Viewing the List of Automation Policies	11
Filtering the List of Automation Policies	12
Special Characters	15
Creating an Automation Policy	17
User Initiated Automations	25
PowerPacks that Contain User Initiated Automations	25
Locating a User Initiated Automation	26
Running a User Initiated Automation	29
Creating a User Initiated Automation	31
Scheduling an Automation Policy	34
Creating an Automation Schedule	35
Creating an Automation Policy Limited by Schedule	38
Creating an Automation Policy to Run on a Schedule	41
Manually Executing a Scheduled Automation Policy	44
"Clear" Policies	44
Aligning an Automation Policy with the System Organization	45
Ordering Actions in an Automation Policy	45
Automation Policies and Event Masks and Event Correlation	46
Events Not Displayed on the Events Page that Might Affect Automation Policies	47
Example	47
Editing an Automation Policy	49
Deleting One or More Automation Policies	50
Action Policies	51
What is an Action Policy?	52
Viewing the List of Action Policies	53
Filtering the List of Action Policies	55
Creating an Action Policy	56
Creating a Custom Action Type	58
Examples:	61
Creating an Action Policy that Sends an Email Notification	62
Creating an Action Policy that Sends an SNMP Trap	64
Using the Default ScienceLogic MIBs to Build an SNMP Trap	65
Default Traps from SL1	65
Varbinds	67
Example Trap	69
Creating the Action Policy	69
Creating an Action Policy that Creates a New Ticket	71
Creating an Action Policy that Sends an SNMP Set	72
Creating an Action Policy that Executes an SQL Query	74
Creating an Action Policy that Updates an Existing Ticket	76
Creating an Action Policy that Sends an AWS SNS Message	77
Setting up a Topic ARN in AWS	77

Creating the Action Policy for AWS SNS	78
Using the Action Policy in an Automation Policy for AWS SNS	79
Creating an Action Policy that Runs an Integration Service Application	81
Creating an Action Policy that Sends an HTTP Request	83
Creating an Action Policy that Uses a Custom Action Type	84
Using the Results of a Previous Action	85
Using the em7_result_list Variable	86
Snippet Actions	88
Creating an Action Policy that Executes a Snippet	89
Writing Snippet Code	91
Snippet Functions	91
Snippet Variables	94
Credential Dictionary Structure	94
Using the Results of Previous Actions	96
Examples	99
Action Policy that Sends an Email Message	100
Automation Policy	100
Action Policy	101
Sent Email	102
Action Policy that Sends an SNMP Trap to an External Server	102
Automation Policy	103
Action Policy	104
Sent Trap	105
Action Policy that Creates a Ticket	105
Automation Policy	106
Action Policy	107
Ticket Template	108
Resulting Ticket	109
Action Policy that Writes an SNMP Value to an External Server	110
Action Policy that Sends an SQL Query to an External Server	110
Automation Policy	111
Action Policy	112
Action Policy that Executes a Snippet and Triggers a New Alert	113
Action Policy that Executes a Snippet and Sends the Results to a Second Action Policy	116
Automation Policy	116
Snippet Action Policy	118
Ticket Action Policy	119
Ticket Template	120
Resulting Ticket	121
Run Book Variables	122
Run Book Variables	123



Chapter 1

Introduction

Overview

This chapter describes the automation policies and the action policies that you can use to create a SL1 Run Book Automation.

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

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

This chapter covers the following topics:

<i>What is Run Book?</i>	5
<i>Custom Settings</i>	5
<i>Automation Policies</i>	6
<i>Action Policies</i>	8

What is Run Book?

SL1 includes automation features that allow you to specify actions you want SL1 to execute automatically when specific event conditions are met. Automation in SL1 is divided into two parts:

- An **automation policy** defines the event conditions that can trigger an automatic action.
- An **action policy** defines an action that can be triggered by an automation policy. An action policy can perform one of the following tasks:
 - Send an email message to a pre-defined list of users and/or external contacts.
 - Send an SNMP trap from SL1 to an external device.
 - Create a new ticket (using ticket templates defined in the **Ticket Templates** page [Registry > Ticketing > Templates]).
 - Update an existing ticket. An action policy can change the status and/or severity of an existing ticket and/or add a note to an existing ticket. For this action policy to trigger successfully, a ticket must be associated with the event that triggered the action.
 - Write an SNMP value to an existing SNMP object on an external device.
 - Query a database.
 - Run a custom python script, called a snippet.
 - Send an SNS Message to a Topic ARN (Amazon Resource Name). All subscribers to the Topic ARN will receive the message.
 - Run an Integration Service application.
 - Send an HTTP request.

If an automation policy has a Policy Type of *Scheduled*, then an Automation Schedule from the **Automation Schedule Manager** page (Registry > Run Book > Schedules) is required instead of an event condition to trigger the automation. You can use an Automation Schedule to automatically trigger Run Book Automations. The actions are executed according to the schedule, regardless of event status, or you can manually execute a scheduled automation policy at any time. You can also use an Automation Schedule as a criteria in event-triggered Run Book Automations. For more information, see [Scheduling an Automation Policy](#).

In addition, you can enable **user initiated automations** that let a user manually trigger an automation policy and its aligned action policies in the SL1 user interface. The list of available user initiated automations for an event are based on the organization, devices, and events that are aligned with the automation policy. For more information, see [User Initiated Automations](#).

Custom Settings

The process that executes Run Book tasks is parallelized. The default settings for parallelization are appropriate for most SL1 systems. However, the Run Book feature does include internal settings that can be changed to support extremely large SL1 systems. For help customizing Run Book for your environment, contact ScienceLogic Customer Support.

Automation Policies

An **automation policy** defines the event conditions that can trigger an automation action. To view a list of automation policies, create an automation policy, or edit an action policy, go to the **Automation Policy Manager** page (Registry > Run Book > Automation).

NOTE: If an automation policy has a Policy Type of *Scheduled*, then an Automation Schedule from the **Automation Schedule Manager** page (Registry > Run Book > Schedules) is required instead of an event condition to trigger the automation. For more information, see [Scheduling an Automation Policy](#).

NOTE: You can enable **user initiated automations** that let a user manually trigger an automation policy and its aligned action policies in the SL1 user interface. For more information, see [User Initiated Automations](#).

When the event criteria in an automation policy are met, one or more actions are executed. These actions are defined in an action policy. To view a list of action policies, create an action policy, or edit an action policy, go to the **Action Policy Manager** page (Registry > Run Book > Actions).

For example, an automation policy might specify the following:

- If the event "illicit process" occurs on device "mailserver01",
- and the event is not cleared within five minutes,
- then execute the action policy "Email NOC".

The action policy "Email NOC" could notify all NOC staff about the "illicit process" event.

NOTE: When an automation policy executes actions, the time stamps for the actions will use the time zone defined in the **System Timezone** field (System > Settings > Behavior page). However, the timestamp for the Event Action Log window will display the user's local time zone, as defined in the **Account Information** page (Preferences > Account > Information). For more information, see "My Contact Information" in the Introduction to SL1 > User Preferences section of the user manual.

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

NOTE: Scheduled automation works differently. For more information, see [Scheduling an Automation Policy](#).

- At least one of the specified events must have occurred.
- Event(s) must have occurred on at least one of the specified devices.
- Event(s) must have specified severity (critical, major, minor, notice, or healthy).
- Event(s) must have specified status (event is not cleared, event is now acknowledged, ticket is not created for event).
- Specified amount of time must elapse after the event occurs and before the other criteria are evaluated by SL1.
- Specified text must appear in the event message.

Automation Policy Editor | Editing Automation Policy [8]
Reset

Policy Name
AWS: Disable EC2 and EBS Instances

Policy Type
[Active Events]

Policy State
[Disabled]

Policy Priority
[Default]

Organization
[System]

Criteria Logic
[Severity >=] [Healthy,]

Match Logic
[Text search]

Match Syntax

[and no time has elapsed]

Repeat Time
[Only once]

[since the first occurrence,]

Align With
[Device Groups]

[and event is NOT cleared]

☒ Trigger on Child Rollup

[and all times are valid]

☐ Include events for entities other than devices (organizations, assets, etc.)

Available Device Groups
Servers

Aligned Device Groups
AWS EBS Volumes
AWS EC2 Instances

Available Events
[3283] Critical: AKCP: AC Voltage sensor detects no cu
[3292] Critical: AKCP: DC Voltage sensor High Critical
[3293] Critical: AKCP: DC Voltage sensor Low Critical
[3282] Critical: AKCP: Dry Contact Sensor Low Critical
[3288] Critical: AKCP: Smoke Detector Alert

Aligned Events
[1698] Notice: Component Device Record Created

Available Actions
SNMP Trap [1]: EM7 Event Trap
Snippet [5]: AWS: Disable Instance By Tag
Snippet [5]: AWS: Discover from EC2 IP
Snippet [5]: AWS: Get EC2 Instance Configuration
Snippet [5]: AWS: Merge Physical with Component

Aligned Actions
1. Snippet [5]: AWS: Get EC2 Instance Configur
2. Snippet [5]: AWS: Disable Instance By Tag

Save Save As

When the criteria are met, the automation policy triggers the execution of one or more specified action policies. The automation policy specifies one or more actions to execute and the order in which to execute those actions.

To create an automation policy, go to the **Automation Policy Manager** page (Registry > Run Book > Automation). For details, see [Automation Policies](#).

Action Policies

An **action policy** is an action that can be automatically triggered in SL1 when certain event criteria are met. To view a list of action policies, create an action policy, or edit an action policy, go to the **Action Policy Manager** page (Registry > Run Book > Actions). For details on creating action policies, see [Action Policies](#).

NOTE: The triggers for action policies are defined in an automation policy on the **Automation Policy Manager** page (Registry > Run Book > Automation).

An action policy can perform one of the following tasks:

- Send an email message to a pre-defined list of users and/or external contacts.
- Send an SNMP trap from SL1 to an external device.
- Create a new ticket (using ticket templates defined in the **Ticket Templates** page [Registry > Ticketing > Templates]).
- Update an existing ticket. An action policy can change the status and/or severity of an existing ticket and/or add a note to an existing ticket. For this action policy to trigger successfully, a ticket must be associated with the event that triggered the action.
- Write an SNMP value to an existing SNMP object on an external device.
- Query a database.
- Run a custom python script, called a snippet.
- Send a Message to a Topic ARN (Amazon Resource Name). All subscribers to the Topic ARN will receive the message.
- Run an Integration Service application.
- Send an HTTP request.



Chapter 2

Automation Policies

Overview

This chapter describes the automation policies found on the **Automation Policy Manager** page (Registry > Run Book > Automation).

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

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

This chapter covers the following topics:

<i>What is an Automation Policy?</i>	10
<i>Before You Begin</i>	11
<i>Viewing the List of Automation Policies</i>	11
<i>Filtering the List of Automation Policies</i>	12
<i>Special Characters</i>	15
<i>Creating an Automation Policy</i>	17
<i>User Initiated Automations</i>	25
<i>Scheduling an Automation Policy</i>	34
<i>"Clear" Policies</i>	44
<i>Aligning an Automation Policy with the System Organization</i>	45
<i>Ordering Actions in an Automation Policy</i>	45
<i>Automation Policies and Event Masks and Event Correlation</i>	46

Events Not Displayed on the Events Page that Might Affect Automation Policies	47
Example	47
Editing an Automation Policy	49
Deleting One or More Automation Policies	50

What is an Automation Policy?

An **automation policy** defines the combination of event conditions that can trigger an automatic action.

When the criteria in an automation policy is met, one or more actions are executed. Each action is defined in an action policy. Action policies are described in detail in the section on [Action Policies](#).

NOTE: When an automation policy executes actions, the time stamps for the actions will use the time zone defined in the System > Settings > Behavior page, in the **System Timezone** field. However, "Send an Email Notification" actions will use the time zone associated with each recipient's account, as defined in the **Account Preferences** page for each recipient. For more information on the Account Preferences, see the chapter on *Managing User Accounts* in the manual **Organizations and Users**.

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

- At least one of the specified events must have occurred.
- Event(s) must have occurred on at least one of the specified devices.
- Event(s) must have specified severity (critical, major, minor, notice, or healthy).
- Event(s) must have specified status (event is not cleared, event is now acknowledged, ticket is not created for event).
- Specified amount of time must elapse after the event occurs and before the other criteria are evaluated by SL1.
- Specified text must appear in the event message.

NOTE: If an automation policy has a Policy Type of *Scheduled*, then an Automation Schedule from the **Automation Schedule Manager** page (Registry > Run Book > Schedules) is required instead of an event condition to trigger the automation. For more information, see [Scheduling an Automation Policy](#).

NOTE: You can enable **user initiated automations** that let a user manually trigger an automation policy and its aligned action policies in the SL1 user interface. For more information, see [User Initiated Automations](#).

Before You Begin

Before you define automation policies, you should consider:

- The types of automatic actions that SL1 can trigger in response to an automation policy. The choices are:
 - Send an email message to a pre-defined list of users and/or external contacts.
 - Send an SNMP trap from SL1 to an external device.
 - Create a new ticket (using ticket templates defined in the **Ticket Templates** page [Registry > Ticketing > Templates]).
 - Update an existing ticket. An action policy can change the status and/or severity of an existing ticket and/or add a note to an existing ticket. For this action policy to trigger successfully, a ticket must be associated with the event that triggered the action.
 - Write an SNMP value to an existing SNMP object on an external device.
 - Query a database.
 - Run a custom python script, called a snippet.
 - Send an SMS Message to a Topic ARN (Amazon Resource Name). All subscribers to the Topic ARN will receive the message.
- The event conditions that are most critical to your business or organization.
- The event conditions that are best suited to an automatic response (instead of a manual response).

Viewing the List of Automation Policies

The **Automation Policy Manager** page (Registry > Run Book > Automation) displays a list of all existing automation policies.

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

TIP: To sort the list of automation 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.

To view the list of automation policies:

1. Navigate to the **Automation Policy Manager** page (Registry > Run Book > Automation).

Automation Policy Manager | Automation Policies Found [22] TRIAL LICENSE: 44 DAYS REMAINING

[Create](#) [Reset](#) [Guide](#)

Automation Policy Name	ID	Policy State	Policy Priority	Organization	Devices	Events	Actions	Edited By	Last Edited	
1. AWS: Disable EBS Instances by EC2 Tag	9	Disabled	Default	System	1 group	1	2	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
2. AWS: Disable EC2 and EBS Instances by EC2 Tag	8	Disabled	Default	System	2 groups	1	2	em7admin	2018-09-24 15:23:39	<input checked="" type="checkbox"/>
3. AWS: Disable or Discover EC2 Instances	10	Disabled	Default	System	1 group	1	3	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
4. AWS: Discover EC2 Instances	11	Disabled	Default	System	1 group	1	2	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
5. AWS: Merge with EC2	13	Disabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
6. AWS: Vanish Terminated EC2 Instances	12	Disabled	Default	System	1 group	1	1	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
7. Cisco: ACI Device Class Realignment	16	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	<input type="checkbox"/>
8. Cisco: ACI Tenant Device Creation	14	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	<input type="checkbox"/>
9. Cisco: ACI Tenant Device Rename	15	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	<input type="checkbox"/>
10. Cisco: AppDynamics Application Discovery	22	Enabled	Default	System	All	2	1	em7admin	2019-01-02 15:19:29	<input type="checkbox"/>
11. Cisco: CSP Cluster Creation	1	Enabled	Default	System	All	1	2	em7admin	2018-09-24 15:23:08	<input type="checkbox"/>
12. Cisco: CSP Component Alignment	3	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:08	<input type="checkbox"/>
13. Cisco: CSP Component to Physical Merge	2	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:08	<input type="checkbox"/>
14. Cisco: CUCM Root Device update	7	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:31	<input type="checkbox"/>

[Select Action] [Go](#)

2. The **Automation Policy Manager** page displays the following about each automation policy:

- **Automation Policy Name.** Name of the automation policy.
- **ID.** Unique numeric identifier, automatically assigned by SL1 to each automation policy.
- **Policy State.** Specifies whether the policy can be executed (enabled) or cannot be executed (disabled).
- **Policy Priority.** Specifies whether this policy is high-priority or default priority. These options determine how the policy is queued.
- **Organization.** Organization associated with the automation policy.
- **Devices.** Number of devices included in the criteria for the automation policy.
- **Events.** Number of events included in the criteria for the automation policy.
- **Actions.** Number of action policies that will be executed by the automation policy.
- **Edited By.** User who created or last edited the automation policy.
- **Last Edited.** Date and time the automation policy was created or last edited.

Filtering the List of Automation Policies

The **Automation Policy Manager** page includes nine filters. You can filter the list of automation policies by one or more of the following parameters: automation policy name, automation ID, policy state, policy priority, organization, number of devices included in the automation policy, number of events included in the automation policy, number of actions executed by the automation policy, user who created or last edited the policy, and date the policy was created or last edited. You can specify one or more parameters to filter the list of automation policies. Only automation policies that meet all of the filter criteria will be displayed in the **Action Policy Manager** page.

The list of automation policies is dynamically updated as you select each filter. For each filter except **Last Edited**, you must enter text to match against. SL1 will search for automation policies that match the text, including partial matches. Text matches are not case-sensitive. You can use **special characters** in each filter.

To filter the list of automation policies:

1. Navigate to the **Automation Policy Manager** page (Registry > Run Book > Automation).

Automation Policy Manager | Automation Policies Found [22] TRIAL LICENSE: 44 DAYS REMAINING

Create Reset Guide

Automation Policy Name *	ID	Policy State	Policy Priority	Organization	Devices	Events	Actions	Edited By	Last Edited	
1. AWS: Disable EBS Instances by EC2 Tag	9	Disabled	Default	System	1 group	1	2	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
2. AWS: Disable EC2 and EBS Instances by EC2 Tag	8	Disabled	Default	System	2 groups	1	2	em7admin	2018-09-24 15:23:39	<input checked="" type="checkbox"/>
3. AWS: Disable or Discover EC2 Instances	10	Disabled	Default	System	1 group	1	3	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
4. AWS: Discover EC2 Instances	11	Disabled	Default	System	1 group	1	2	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
5. AWS: Merge with EC2	13	Disabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
6. AWS: Vanish Terminated EC2 Instances	12	Disabled	Default	System	1 group	1	1	em7admin	2018-09-24 15:23:39	<input type="checkbox"/>
7. Cisco: ACI Device Class Realignment	16	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	<input type="checkbox"/>
8. Cisco: ACI Tenant Device Creation	14	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	<input type="checkbox"/>
9. Cisco: ACI Tenant Device Rename	15	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	<input type="checkbox"/>
10. Cisco: AppDynamics Application Discovery	22	Enabled	Default	System	All	2	1	em7admin	2019-01-02 15:19:29	<input type="checkbox"/>
11. Cisco: CSP Cluster Creation	1	Enabled	Default	System	All	1	2	em7admin	2018-09-24 15:23:08	<input type="checkbox"/>
12. Cisco: CSP Component Alignment	3	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:08	<input type="checkbox"/>
13. Cisco: CSP Component to Physical Merge	2	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:08	<input type="checkbox"/>
14. Cisco: CUCM Root Device update	7	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:31	<input type="checkbox"/>

(Select Action) Go

2. The **Automation Policy Manager** page displays a list of automation policies. To sort the list, you can enter a value in one or more of the following headings:

- **Automation Policy Name.** Name of the automation policy. You can enter text to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching policy name.
- **ID.** Unique numeric identifier, automatically assigned by SL1 to each automation policy. You can enter numbers to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching automation ID.
- **Policy State.** Specifies whether the policy can be executed (enabled) or cannot be executed (disabled). You can enter text to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching state.
- **Policy Priority.** Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued. You can enter text to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching priority.
- **Organization.** Organization associated with the automation policy. You can enter text to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching organization.
- **Devices.** Number of devices included in the criteria for the automation policy. You can enter numbers to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching number of aligned devices.

- **Events.** Number of events included in the criteria for the automation policy. You can enter numbers to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching number of aligned events.
- **Actions.** Number of action policies that will be executed by the automation policy. You can enter numbers to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching number of aligned action policies.
- **Edited By.** The user who last edited the automation policy. You can enter text to match, including special characters, and the **Automation Policy Manager** page will display only automation policies that have a matching username in the **Edited By** field.
- **Last Edited.** Only those automation policies that match all of the previously selected fields and have the specified creation date or last-edited date will be displayed. The choices are:
 - *All.* Display all automation policies that match the other filters.
 - *Last Minute.* Display only automation policies that have been created within the last minute.
 - *Last Hour.* Display only automation policies that have been created within the last hour.
 - *Last Day.* Display only automation policies that have been created within the last day.
 - *Last Week.* Display only automation policies that have been created within the last week.
 - *Last Month.* Display only automation policies that have been created within the last month.
 - *Last Year.* Display only automation policies that have been created within the last year.

Special Characters

When filtering a list in a registry page, you can include the following special characters to search each field except those that display date and time:

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

Special Character	Description	Example
, (comma)	(For strings or numeric values) Specifies an OR operation.	"dell,micro" would match all values that contain the string "dell" OR the string "micro".
& (ampersand)	(For strings or numeric values) Specifies an AND operation.	"dellµ" would match all values that contain both the string "dell" AND the string "micro", in any order.
! (exclamation point)	(For strings or numeric values) Specifies a NOT operation. NOTE: You can also use the "!" character in combination with the arithmetic special characters (min-max, >, <, >=, <=, =) described below.	"!dell" would match all values that do not contain the string "dell".
* (asterisk)	(For strings or numeric values) Specifies a "match-zero-or-more" operation. For a string, matches any string that matches the text before and after the asterisk. For a numeral, matches any numeral that contains the text.	<ul style="list-style-type: none"> "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)	(For strings or numeric values) Specifies a "match any one character" operation.	<ul style="list-style-type: none"> "l?ver" would match the strings "oliver", "levers", and "liver", but not "believers". "135?" would match the numbers "1350", "1354", and "1359", but not "13502".
^ (caret)	(For strings only) Specifies a "match the beginning" operation. Matches any string that begins with the specified string.	"^sci" would match "scientific" and "sciencelogic", but not "conscious".
\$ (dollar)	(For strings only) Specifies "match the ending". Matches any string that ends with the specified string.	"ter\$" would match the string "renter" but not the string "terrific".

Special Character	Description	Example
	NOTE: You can use both ^ and \$ if you want to match an entire string. For example, "^tern\$" would match the strings "tern" or "Tern" or "TERN"; it would not match the strings "terne" or "cistern".	
min-max	(For numeric values only) Matches any value between the specified minimum value and the maximum value, including the minimum and the maximum.	"1-5" would match 1, 2, 3, 4, and 5.
- (dash)	(For numeric values only) A "half open" range. Matches values including the specified minimum and greater, or including the specified maximum and lesser.	<ul style="list-style-type: none"> "1-" matches 1 and greater, so it would match 1, 2, 6, 345, etc. "-5" matches 5 and less, so it would match 5, 3, 1, 0, etc.
> (greater than)	(For numeric values only) Matches any value greater than the specified value.	">7" would match all values greater than 7.
< (less than)	(For numeric values only) Matches any value less than the specified value.	"<12" would match all values less than 12.
>= (greater than or equal to)	(For numeric values only) Matches any value that is equal to or greater than the specified value.	">=7" would match all values 7 and greater.
<= (less than or equal to)	(For numeric values only) Matches any value that is equal to or less than the specified value.	"<=12" would match all values 12 and less.
= (equal)	<p>(For numeric values only) Matches a value that is equal to the specified value.</p> <p>You can also use this special character to match a negative value, as demonstrated in the example.</p>	"=-5" would match "-5" instead of being evaluated as the "half open range" as described above.

Creating an Automation Policy

An automation policy defines the event conditions that must be met before SL1 will trigger an automatic action (defined in an action policy).

You can also create a "user initiated" automation policy that lets a user trigger an automation action (from an action policy) on an as needed, ad hoc basis. A user initiated automation does not require that the event-based logic in the **Criteria Logic** section matches to *True* in the automation policy, as the user action supersedes that criteria. For more information, see [User Initiated Automations](#).

In addition, if an automation policy has a Policy Type of *Scheduled*, then an Automation Schedule from the **Automation Schedule Manager** page (Registry > Run Book > Schedules) is required instead of an event condition to trigger the automation. For more information, see [Scheduling an Automation Policy](#).

To create an automation policy:

1. Navigate to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the **[Create]** button. The **Automation Policy Editor** page appears:

The screenshot shows the 'Automation Policy Editor | Creating New Automation Policy' interface. At the top right is a 'Reset' button. The form is organized into several sections:

- Policy Metadata:** Fields for Policy Name, Policy Type (dropdown with '[Active Events]'), Policy State (dropdown with '[Enabled]'), Policy Priority (dropdown with '[Default]'), and Organization (dropdown with 'East Coast').
- Logic Configuration:**
 - Criteria Logic:** A series of dropdowns for '[Severity >=]', '[Minor,]', '[and 5 minutes has elapsed]', '[since the first occurrence,]', '[and event is NOT cleared]', and 'and all times are valid'.
 - Match Logic:** A dropdown for '[Text search]'.
 - Match Syntax:** A text input field.
 - Repeat Time:** A dropdown for '[Only once]'.
 - Align With:** A dropdown for '[Devices]'.
- Options:** Two checkboxes: 'Trigger on Child Rollup' and 'Include events for entities other than devices (organizations, assets, etc.)'.
- Device and Event Management:**
 - Available Devices:** A list box containing 'East Coast', 'ScienceLogic, Inc.: EM7 All-In-One: gmstack02', 'System', 'Cisco Systems: 7609S: 7609S-NPE3.cisco.com', and 'Cisco Systems: CUCM Server: CUCM10-01.qa.science'.
 - Aligned Devices:** A list box containing '(All devices)'.
 - Available Events:** A list box containing several critical alerts from AKCP, such as 'Critical: AKCP: AC Voltage sensor detects no cu'.
 - Aligned Events:** A list box containing '(All events)'.
 - Available Actions:** A list box containing actions like 'SNMP Trap [1]: EM7 Event Trap', 'Snippet [5]: AWS: Disable Instance By Tag', 'Snippet [5]: AWS: Discover from EC2 IP', 'Snippet [5]: AWS: Get EC2 Instance Configuration', and 'Snippet [5]: AWS: Merge Physical with Component'.
 - Aligned Actions:** An empty list box with up and down arrow controls.

At the bottom center is a 'Save' button.

3. In the **Automation Policy Editor** page, supply a value in each of the following fields:
 - **Policy Name.** Name of the automation policy.
 - **Policy Type.** Specifies whether the automation policy will search for cleared events or active events, or if this will be a scheduled automation policy. You choices are:
 - *Active Events.* The automation policy will search active events to find events that meet the criteria.
 - *Cleared Events.* The automation policy will search cleared events to find events that meet the criteria.

- *Scheduled*. The automation policy will execute as specified by a selected Automation Schedule. The Automation Policy will not search events to match criteria. For more information, see [Scheduling an Automation Policy](#).
- *User Initiated*. The Automation policy lets the user execute an "ad hoc" automation on an event from the **Events** page, an **Event Investigator** page, or a **Service Investigator** page. For more information, see [User Initiated Automations](#).

NOTE: If you select *User Initiated*, the following fields are hidden: **Policy Priority**, **Criteria Logic**, **Match Logic**, **Match Syntax**, **Repeat Time**, and **Trigger on Child Rollup**.

- *Active Events/User Initiated*. The automation policy enables all of the features of the "Active Events" and the "User Initiated" Policy Types. As a result, this automation policy can be triggered by active events that meet the criteria in the policy, or a user can manually trigger the automation.
- **Policy State**. Specifies whether the policy can be executed (enabled) or cannot be executed (disabled).
- **Policy Priority**. Specifies whether this policy is high priority or default priority. Options are:
 - *Default*. This policy is placed into a default queue. SL1 includes multiple worker tasks that constantly check this queue and execute policies in this queue. If there are no policies in the default queue, the worker tasks execute policies in the high-priority queue.
 - *High*. This policy is placed into the high-priority queue. SL1 includes multiple worker tasks that constantly check this queue and execute the policies. For details on configuring the number of worker tasks for high-priority policies, contact ScienceLogic Customer Support. If there are no policies in the high-priority queue, the worker tasks execute policies in the Default queue.
- **Organization**. Organization associated with the automation policy. If you select the *System* organization, the behavior of the **Available Devices** and **Available Device Groups** fields is affected.
- **Criteria Logic**. These fields specify the conditions that must be met before SL1 executes the action specified in the automation policy. All conditions must be met for at least one of the selected events on one of the selected devices.
 - *Severity Operator*. Used in conjunction with the *Severity* field. Choices are:
 - *Severity >=*. Severity is greater than or equal to.
 - *Severity =*. Severity must be equal to.
 - *Severity*. Event must have the specified severity or have a severity greater than or equal to the specified severity. The choices are:
 - Critical
 - Major
 - Minor
 - Notice
 - Healthy

- *Elapsed time*. The length of time that must elapse after the event occurs but before SL1 evaluates the other criteria in the automation policy. The choices are intervals of time ranging from "no time has elapsed" to "1 month has elapsed", and you must then specify whether the elapsed time is counted "since the first occurrence" or "since the activation time". You might use this field to allow users to manually perform actions before the automation actions are executed.
- *Since*. Specifies the ScienceLogic event that is applied to *Elapsed time*. The choices are:
 - since the first occurrence
 - since the activation time (when an event became active). For more information, see the **Events** manual.
- *Status*. Event must have the specified status. The choices are:
 - and event is NOT cleared
 - and event is NOT acknowledged
 - and ticket is NOT created
 - and event IS acknowledged
 - and ticket IS created
 - and external ticket IS requested
 - and external ticket IS created

NOTE: The *Status* options "and external ticket IS requested" and "and external ticket IS created" require that you select *Create/View External Ticket* for the global setting **Event Console Ticket Life Ring Button Behavior** in the **Behavior Settings** page (System > Settings > Behavior). You can use this *Status* to trigger a custom run book action to create a ticket on the external system or perform actions after a ticket is created on the external system. For more information on system settings, see the chapter on *Global Settings* in the **System Administration** manual.

NOTE: The *Status* option "and ticket IS created" requires that you select *Create/View EM7 Ticket* for the global setting **Event Console Ticket Life Ring Button Behavior** in the **Behavior Settings** page (System > Settings > Behavior). You can use this *Status* to trigger a custom run book action that performs actions after a ticket is created on the SL1. For more information on system settings, see the chapter on *Global Settings* in the **System Administration** manual.

NOTE: The **Elapsed Time** and **Status** fields do not appear if you selected *Cleared Events* in the **Policy Type** field.

- *Time/Schedule*. Specifies the timespan during which the Automation Policy can execute the aligned actions. The choices are:
 - *and all times are valid*. The Automation Policy can execute the aligned actions when all the criteria are met. There is no schedule associated with the criteria.

- *and the following schedule is active*. The Automation Policy can execute the aligned actions during the timespan specified in the selected schedule.
 - *and the following schedule is NOT active*. The Automation Policy can execute the aligned actions during any time except the timespan specified in the selected schedule. You would use this option in cases where you want to restrict event-driven automation from running during a particular time.
- *Schedule*. If in the *Time/Schedule* field you specified "and the following schedule is active" or "and the following schedule is NOT active", select a schedule in this field. Note that ad hoc automation schedules, which specify a single point in time, will not be shown in this field.
- **Match Logic**. Specifies whether to process the **Match Syntax** field as a regular expression or a simple text match. This field is optional. However, if you enter a value in the **Match Syntax** field, you must also select a value in this field.
 - **Match Syntax**. An optional string to further filter events. For SL1 to execute the actions specified in the policy, the event message must match the text or regular expression defined in this field. For example, if you want to be notified only when an event occurs on a specific sub-entity (like an interface or a file system), you can specify a text match or regular expression that will match that sub-entity in this field. Can be any combination of alpha-numeric characters, up to 48-characters in length. SL1's expression matching is case-sensitive.
 - **Repeat Time**. The frequency at which SL1 should execute the automation policy while the conditions are still met. The choices range from "every 30 seconds until satisfied" to "every 2 hours until satisfied", or "only once".

NOTE: The **Repeat Time** field does not appear if you selected *Cleared Events* in the **Policy Type** field

- **Align With**. Specifies whether to align this automation policy with one or more devices, one or more device groups, or one or more organizations.
 - *Devices*. The **Available Devices** field will appear below, where you can select devices to associate with the automation policy.
 - *Device Groups*. The **Available Device Groups** field will appear below, where you can select device groups to associate with the automation policy.
 - *Policy Organization*. The **Available Devices in Organization** field will appear below, where you can select one or more devices to associate with the automation policy. The list of devices comprises all devices in the organization specified in the **Organization** field.
 - *IT Services*. The **Available IT Services** field will appear below, where you can select one or more IT Services to associate with the automation policy.
- **Trigger on Child Rollup**. Affects events that are rolled up, either using event correlation or event masks. If selected, all events in a suppression group can trigger the automation policy. If not selected, only a single event in a suppression group can trigger the automation policy.

- **Include events for entities other than devices (organizations, assets, etc.).** If you select this checkbox, the automation policy can match events that are not associated with a device. The automation policy will match events that are not associated with a device only if you do not select specific devices or device groups from the **Available Devices**, **Available Device Groups**, **Available Devices in Organization**, or **Available IT Services** field.
- **Available Devices.** If you selected *Devices* in the **Align With** field, this field displays a list of all devices in SL1. You can select one or more devices in this field. The selected event(s) and event criteria must occur on one of the selected devices before the automation policy will be executed.

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

- **To select a device**, highlight it and click the right-arrow button.
- **If you do not select any devices**, the automation policy automatically evaluates all devices associated with the organization you selected in the **Organization** field. If you selected *System* in the **Organization** field, the automation policy automatically evaluates all devices in SL1. Additionally, if the **include events for entities other than devices (organizations, assets, etc.)** checkbox is checked, the automation policy will **evaluate all events associated with all organizations that are not associated with a device**, regardless of the organization selected in the **Organization** field.
- **If you select specific devices**, the automation policy will evaluate all selected devices.

NOTE: Not selecting specific devices allows an automation policy to evaluate events that are aligned with an entity other than a device.

- **Aligned Devices.** This pane displays a list of all devices aligned with the automation policy. To de-select a device, highlight it and click the left-arrow button.
- **Available Device Groups.** If you selected *Device Groups* in the **Align With** field, this field displays a list of all device groups in SL1. You can select one or more device groups in this field. The selected event(s) and event criteria must occur on at least one device in one of the selected device groups before the automation policy will be executed.

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

- **To select a device group**, highlight it and click the right-arrow button.
- **If you do not select any device groups**, the automation policy automatically evaluates all device groups to which you have access. Additionally, if the **Include events for entities other than devices (organizations, assets, etc.)** checkbox is checked, the automation policy will **evaluate all events associated with all organizations that are not associated with a device**, regardless of the organization selected in the **Organization** field.
- **If you select specific device groups**, the automation policy will evaluate all selected device groups.

NOTE: Not selecting specific device groups allows an automation policy to evaluate events that are aligned with an entity other than a device.

- **Aligned Device Groups.** This pane displays a list of all device groups aligned with this automation policy. To de-select a device group, highlight it and click the left-arrow button. Note that selecting a device group aligns all devices that are part of the device group with the automation policy.
- **Available Devices in Organization.** If you selected *Policy Organization* in the **Align With** field, this field displays only devices from the organization selected in the **Organization** field. You can select one or more devices in this field. The selected event(s) and event criteria must occur on one selected device before the automation policy will be executed.

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

- **To select a device**, highlight it and click the right-arrow button.
- **If you do not select any devices**, the automation policy automatically evaluates all devices associated with the organization you selected in the **Organization** field. Additionally, if the **Include events for entities other than devices (organizations, assets, etc.)** checkbox is checked, the automation policy will **evaluate all events associated with the organization specified in the Organization field that are not associated with a device**.
- **If you select specific devices**, the automation policy will evaluate all selected devices.

NOTE: Not selecting specific devices allows an automation policy to evaluate events that are aligned with an entity other than a device.

- **Aligned Devices.** This pane displays a list of all devices aligned with this automation policy. To de-select a device, highlight it and click the left-arrow button.
- **Available IT Services.** If you selected *IT Services* in the **Align With** field, this field displays a list of all IT Services in SL1. You can select one or more IT Services in this field. The selected event(s) and event criteria must occur for one of the selected IT Services before the automation policy will be executed.

NOTE: You can use the field at the top of the **Available IT Services** field to filter the list of IT service policies. If you enter an alpha-numeric string in the field, the **Available IT Services** field will include only IT service policies that match the string.

- **To select an IT Service**, highlight it and click the right-arrow button.
- **If you do not select any IT Services**, the automation policy automatically evaluates all IT Services associated with the organization you selected in the **Organization** field. If you selected **System** in the **Organization** field, the automation policy automatically evaluates all IT Services in SL1.
- **If you select specific IT Services**, the automation policy will evaluate all selected devices.

NOTE: Not selecting specific IT Services allows an automation policy to evaluate events that are aligned with an entity other than an IT Service.

- **Aligned IT Services.** This pane displays a list of all IT Services aligned with this automation policy. To de-select an IT Service, highlight it and click the left-arrow button.
- **Available Events.** Displays a list of all defined events in SL1. You can select one or more events in this field. One of the selected events and event criteria must occur on one selected device before the automation policy will be executed. **To select an event**, highlight it and click the right-arrow button. This pane also displays the ID number for each aligned event policy to ensure you select the relevant policy.

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

- **Aligned Events.** This pane displays a list of all events aligned with this automation policy, along with the ID number of the aligned event policy. To de-select an event, highlight it and click the left-arrow button.

NOTE: If a triggering event (that is, an event specified in the **Aligned Events** field is not aligned with a device (but is instead aligned with an organization), and you have also selected one or more **Aligned Actions** that must be executed on a Data Collector, SL1 will 1) Not execute the action policy; 2) Create a log entry in the audit log for the organization aligned with the triggering event, noting that the criteria in the automation policy were met, but that the action policy was not executed. This does not apply to Action Policies created on an All-In-One Appliance.

- **Available Actions.** Displays a list of all action policies in SL1. (Action policies are defined in Registry > Run Book > Actions.) You can select one or more action policies in this field. If the selected event(s) and event criteria occur on the selected devices or for the selected IT Services, the selected action policies will be executed. To select an action policy, highlight it and click the right arrow-button.

NOTE: You can use the field at the top of the **Available Actions** field to filter the list of action policies. If you enter an alpha-numeric string in the field, the **Available Actions** field will include only action policies that match the string.

- **Aligned Actions.** This pane displays a list of all action policies aligned with this automation policy.
 - **To de-select an action policy,** highlight it and click the left-arrow button.
 - **To change the order in which one or more action policies are executed,** highlight the action policy and use the up-arrow or down-arrow to move the policy within the list.

NOTE: If you selected multiple action policies in the automation policy, the action policies will be executed in the order specified in the **Aligned Actions** field. To change the order of one or more action policies, highlight the action policy and use the up-arrow or down-arrow to move the policy within the list.

- **[Save].** Saves a new automation policy or saves changes to an existing automation policy.
- **[Save As].** If you supply a new value in the **Policy Name** field, saves the current automation policy, including any edits, as a new policy with a new name.

4. Click the **[Save]** button to save the new automation policy or save changes to an existing automation policy.

User Initiated Automations

You can run or create a "user-initiated" automation policy that lets a user trigger an automation action (from an action policy) on an as-needed, "ad hoc" basis. A user initiated automation does not require that the event-based logic in the **Criteria Logic** section matches to *True* in the automation policy as the user action supersedes that criteria.

PowerPacks that Contain User Initiated Automations

The *Datacenter Automation Utilities* PowerPack is required for all Automation PowerPacks.

The *Datacenter Advanced Enrichment Actions* PowerPack is required for Cisco Automation PowerPacks.

NOTE: Follow the installation and configuration instructions in the release notes for the PowerPacks containing the automations you want to use. You must meet all prerequisites for each PowerPack before the automations from that PowerPack will be available in the **Tools** pane in SL1.

The following is a partial list of the PowerPacks that contain user initiated automation policies:

- Cisco IOS Automation Policies PowerPack version 102 or later
- Cisco IOS-XE Automation Policies PowerPack version 102 or later
- Cisco IOS-XR Automation Policies PowerPack version 102 or later
- Cisco Networking Automation Policies PowerPack version 102 or later
- Linux SSH Automation Policies User Initiated Automation PowerPack
- Network Connectivity User Initiated Automation PowerPack
- VMware User Initiated Automation PowerPack
- Windows PowerShell User Initiated Automation PowerPack

For a complete list of PowerPacks containing user initiated automation policies, see the [PowerPacks](#) page of the ScienceLogic Support Site.

NOTE: To run user initiated automations with a device group, the device group must use a *static* list of devices, not a dynamic list of devices.

Locating a User Initiated Automation

You can run a user initiated automation from the **Run Book Actions** section of the **Tools** pane. The **Tools** pane is available on the Event Drawer for an event on the **Events** page, the **Event Investigator** page for an event, and the **Service Investigator** page for a service.

A **Tools** pane with a **Run Book Actions** section is available in the following locations in SL1 :

- The Event Drawer for an event on the **Events** page. The event must be aligned with a device to enable the Event Drawer. To open the Event Drawer, click the down arrow icon (▼) for that event:

The screenshot shows the ScienceLogic Events page. At the top, there are filters for severity: 4 Critical, 22 Major, 9 Minor, 22 Notice, and 3 Healthy, totaling 60 Events. A search bar is present. The main table lists events with columns: SEVERITY, NAME, MESSAGE, EVENT ID, EVENT SOURCE, EVENT TYPE, LAST DETECTED, AUTOMATED ACTIONS, ACKNOWLEDGE, and CLEAR. The 'AUTOMATED ACTIONS' column is highlighted with a red box. Below the table, a 'Vitals' graph is shown on the left. In the center, a 'Tools' drawer is open, showing a search bar and a list of tools: Availability, Ping, Whois, Port Scan, and Deep Port Scan. On the right, a 'Logs' section shows a list of log entries with columns: AGE, SEVERITY, and MESSAGE. The 'Event Drawer' for a specific event is also visible, showing details about the event and the device it is associated with.

TIP: If needed, click the Select Columns icon (⚙️) and select *Automated Actions* to add that column to the **Events** page. This column lists the number of automated actions for each event, and you can click the number to open the **Event Actions Log** window.

- The **Event Investigator** page for an event. Select the event from the **Events** page to view the **Event Investigator** page:

Events | Activity | Em7admin | ScienceLogic

Poller: File system usage exceeded (major) threshold

Major | 14 minutes 53 seconds Ago | 846 Occurrences | First seen 8 days 19 hours Ago

/data.local/db: File system usage exceeded major threshold: Limit: 85.0%, Actual: 89.00%

Probable Cause & Resolution

Event Definition: A file system on the server has exceeded its usage threshold.

Action: Review file system usage on the hardware tab for this device and to confirm which filesystem(s) are getting full. Take appropriate application action to reduce the load on these filesystems.

em7ao | 10.64.68.17 | System

Tools

Type to run an action on this device

- DEFAULT TOOLS
 - Availability
 - Ping
 - Who Is
 - Port Scan
 - Deep Port Scan
- ARP Lookup
- ARP Ping
- Trace Route
- BUNBOOK ACTIONS
 - Run File System Diagnostics (SSH)

Logs

AGE	SEVERITY	MESSAGE
7 minutes 29 seconds	Minor	Physical Memory has exceeded threshold: (80%) currently (86.52201380333948%)
7 minutes 37 seconds	Major	DRBD: This node is not UpToDate
7 minutes 50 seconds		Host Resource: Storage Utilization (/data.local/db) of type HtStorageFixedDisk has exceeded major threshold 83%, currently 85.00% (89.00%)
7 minutes 50 seconds		Host Resource: Storage Utilization (/home) of type HtStorageFixedDisk has exceeded major threshold 83%, currently 85.00% (89.00%)

Note

TIP: To see if an event was associated with an automation, click the **[Actions]** button (≡) from the **Events** page and select *View Automation Actions*. The **Event Actions Log** window appears, with a list of all previously run automations. In the classic user interface, you can open the **Event Actions Log** window from the **Events Console** by clicking the View Notification Log icon (📄) when the value in the **Notify** column increases.

- The **Service Investigator** page for a service. Select the service from the **Business Services** page to view the **Service Investigator** page, and then scroll down to the **[Events]** tab. To open the Event Drawer for an event for that service, click the down arrow icon (▼):

The screenshot shows the Service Investigator page for a service named 'ashok-ds-test'. The page has a top navigation bar with 'Back', 'Overview', 'Devices', and 'Status Policy' tabs. The 'Overview' tab is selected. Below the navigation bar, there are three status cards: 'Health' (Major), 'Availability' (Available), and 'Risk' (75% Major). To the right of these cards is an 'Events' tab, which is highlighted with a red box. Below the 'Events' tab, there is a table of events. The table has columns for 'ORGANIZATION', 'SEVERITY', 'NAME', 'MESSAGE', 'AGE', 'TICKET ID', 'COUNT', 'EVENT NOTE', 'MASKED EVENTS', 'AUTO...', 'ACKNOWLEDGE', and 'CLEAR'. The first three rows of the table are highlighted with a red box. The first row shows a 'Minor' event with the message 'Network latency exceeded threshold: 193.8895 ms.' and an age of '1 minute 6 second'. The second row shows a 'Minor' event with the message 'Network latency exceeded threshold: No Response.' and an age of '2 days 1 hour'. The third row shows a 'Minor' event with the message 'Network latency exceeded threshold: No Response.' and an age of '2 days 1 hour'. Below the table, there is a 'Tools' section with a search bar and a list of tools: 'ARP Ping', 'Availability', 'Ping', 'Whois', 'Trace Route', and 'Run Ping (IPv4)'. The 'Tools' section is also highlighted with a red box. To the right of the 'Tools' section, there is a 'Logs' section with a table of logs. The table has columns for 'AGE', 'SEVERITY', and 'MESSAGE'. The first three rows of the table are highlighted with a red box. The first row shows a 'Major' event with the message 'Device Failed Availability Check: ICMP Ping' and an age of '36 minutes 8 se'. The second row shows a 'Minor' event with the message 'Network latency exceeded threshold: No Response.' and an age of '36 minutes 8 se'. The third row shows a 'Major' event with the message 'Device Failed Availability Check: ICMP Ping' and an age of '41 minutes 9 se'.

Running a User Initiated Automation

In most situations, you would run a user initiated automation in response to an event that just occurred. If you have Automation PowerPacks installed on your SL1 system, the **Event Actions Log** window for that event might contain diagnostic information from other automations that have already run, including information that helps you determine which user initiated automation you should run next to address the cause of the event.

To run a user initiated automation:

1. On the **Events** page, locate the event.
2. Click the Actions button (≡) for the event and select *View Automation Actions*. The **Event Actions Log** window appears:

```

Event Actions Log | For Event [5880]
2020-05-28 13:38:13
Automation Policy Network Connectivity: Run NMAP on Monitored Ports action Datacenter Automation: Format Output as HTML ran Unsuccessfully
Message Snippet (60) executed with incident: Traceback (most recent call last):
File "loptem7\backend\silo_common\automation\exec_snippet.py", line 73, in execute_snippet
File "", line 39, in
File "loptem7\envs\decompressor.py", line 11, in wrapper
File "loptem7\envs\memory_calculator.py", line 16, in wrapper
File "loptem7\envs\memory_calculator.py", line 57, in calculate_available_memory_based_on_last_results
File "loptem7\envs\memory_calculator.py", line 70, in calculate_last_results_size
File "loptem7\envs\memory_calculator.py", line 91, in calculate_emt_last_result_size
File "loptem7\envs\memory_calculator.py", line 96, in calculate_data_size
File "usr\lib64\python2.7\json\__init__.py", line 243, in dumps
return _default_encoder.encode(obj)
File "usr\lib64\python2.7\json\encoder.py", line 207, in encode
chunks = self.iterencode(o, _one_shot=True)
File "usr\lib64\python2.7\json\encoder.py", line 270, in iterencode
return _iterencode(o, 0)
File "usr\lib64\python2.7\json\encoder.py", line 184, in default
raise TypeError(repr(o) + " is not JSON serializable")
TypeError: ValueError(Error executing action. The device must contain at least one monitored port.) is not JSON serializable
Result: None
2020-05-28 13:37:58
Automation Policy Network Connectivity: Run Ping (IPv4) action Datacenter Automation: Format Output as HTML ran Successfully
Message Snippet (60) executed without incident
Result: formatted output: Enrichment Command Output
Command: ping -c 5 10.2.2.17
PING 10.2.2.17 (10.2.2.17): 56(84) bytes of data.
--- 10.2.2.17 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 3999ms
}
2020-05-28 13:37:58
Automation Policy Network Connectivity: Run Traceroute (IPv4) action Datacenter Automation: Format Output as HTML ran Successfully
Message Snippet (60) executed without incident
Result: formatted output: Enrichment Command Output
Command: traceroute 10.2.2.17
traceroute to 10.2.2.17 (10.2.2.17): 30 hops max, 60 byte packets
1 10.64.164.5 (10.64.164.5) 4.560 ms 4.505 ms 4.479 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *

```

3. On the **Event Actions Log** window, review any existing automations that have already run, along with any diagnostic information or instructions that might appear for the event.
4. Go to the **Tools** pane on the **Events** page, on the **Event Investigator** page, or on the **Service Investigator** page [Events] tab.
5. From the **Run Book Actions** section on the **Tools** pane, click to run the relevant user initiated automation:

The screenshot shows the 'Events' page with a table of events. The 'Tools' pane is open, displaying a modal window for running actions. The 'RUN BOOK ACTIONS' tab is selected, showing a list of actions. The 'Run Book Actions' tab is highlighted with a red box.

SEVERITY	NAME	MESSAGE	EVENT ID	EVENT SOURCE	EVENT TYPE	LAST DETEC	AUTOMATED ACTIO...	ACKNOWLEDGE	CLEAR
Major	aym-win10	Device Failed Availability Check: ICMP Ping	1013	Internal	Device	May 29, 20...	5	✓ Acknowledge	✗ Clear
Major	aym-win2012r2-0	Device Failed Availability Check: ICMP Ping	3305	Internal	Device	May 29, 20...	5	✓ Acknowledge	✗ Clear
Major	10.2.2.15	Device Failed Availability Check: ICMP Ping	5878	Internal	Device	May 29, 20...	5	✓ Acknowledge	✗ Clear
Major	10.2.2.17	Device Failed Availability Check: ICMP Ping	5880	Internal	Device	May 29, 20...	5	✓ Acknowledge	✗ Clear

6. After the action completes, click the **View Logs** link if needed. The **Event Actions Log** window displays updated information about the user initiated automation.

Creating a User Initiated Automation

For an automation action to be visible on the **Tools** pane, the following three things must be true:

- **Organization**. The event must occur for the aligned organization specified in the automation policy.
- **Aligned Devices**. The event must occur on the aligned device or devices specified in the automation policy.
- **Aligned Event**. The event must match one of the aligned events specified in the automation policy.

To create a user initiated automation:

1. On the Automation Policy Manager page (Registry > Run Book > Automation, click **[Create]**. The Automation Policy Editor window appears:

The screenshot shows the 'Automation Policy Editor | Creating New Automation Policy' window. It features a top bar with a 'Reset' button. Below the bar, there are four dropdown menus: 'Policy Name' (set to 'Linux CPU'), 'Policy Type' (set to 'User Initiated'), 'Policy State' (set to '[Enabled]'), and 'Organization' (set to 'System'). Below these is an 'Align With' dropdown set to '[Devices]'. The main area is divided into two columns. The left column contains three lists: 'Available Devices' (listing various Linux systems like 'knights_routemix', 'SILO', 'SL_Meraki', etc.), 'Available Events' (listing various Linux events like '[3474] Major: Linux SSH: File System over usage threshold', etc.), and 'Available Actions' (listing 'Snippet [5]: Linux Classification and Automation'). The right column contains three lists: 'Aligned Devices' (listing 'rc_async_snmp', 'NET-SNMP: Linux: RC-snmpsim-SNMP-App-Test', etc.), 'Aligned Events' (listing '[3471] Major: Linux SSH: CPU utilization above threshold'), and 'Aligned Actions' (listing '1. Snippet [5]: Linux Classification and Automation'). At the bottom center is a 'Save' button.

3. On the **Automation Policy Editor** page, complete the following fields:

- **Policy Name**. Name of the automation policy.
- **Policy Type**. Specifies whether the automation policy will search for cleared events or active events, or if this will be a scheduled automation policy. You choices are:

- *User Initiated*. The Automation policy lets the user execute an "ad hoc" automation on an event from the **Events** page, a device from the **Devices** page or a **Device Investigator** page, or a service from the **Service Investigator** page.

NOTE: If you select *User Initiated*, the following fields are hidden: **Policy Priority**, **Criteria Logic**, **Match Logic**, **Match Syntax**, **Repeat Time**, and **Trigger on Child Rollup**.

- *Active Events/User Initiated*. The automation policy enables all of the features of the "Active Events" and the "User Initiated" Policy Types. As a result, this automation policy can be triggered by active events that meet the criteria in the policy, or a user can manually trigger the automation.

NOTE: If you select *Active Events/User Initiated*, see [Creating an Automation Policy](#) for descriptions of the additional fields on the **Automation Policy Editor** page.

- **Policy State**. Specifies whether the policy can be executed (enabled) or cannot be executed (disabled).
- **Organization**. Organization associated with the automation policy. If you select the *System* organization, the behavior of the **Available Devices** and **Available Device Groups** fields is affected.
- **Align With**. Specifies whether to align this automation policy with one or more devices, one or more device groups, or one or more organizations.
 - *Devices*. The **Available Devices** field will appear below, where you can select devices to associate with the automation policy.
 - *Device Groups*. The **Available Device Groups** field will appear below, where you can select device groups to associate with the automation policy.

NOTE: To run user initiated automations with a device group, the device group must use a *static* list of devices, not a *dynamic* list of devices.

- *Policy Organization*. The **Available Devices in Organization** field will appear below, where you can select one or more devices to associate with the automation policy. The list of devices comprises all devices in the organization specified in the **Organization** field.
- **Available Devices**. If you selected *Devices* in the **Align With** field, this field displays a list of all devices in SL1. You can select one or more devices in this field. The selected event(s) and event criteria must occur on one of the selected devices before the automation policy will be executed.

- **To select a device**, select it and click the right-arrow button.
 - **If you do not select any devices**, the automation policy automatically evaluates all devices associated with the organization you selected in the **Organization** field. If you selected **System** in the **Organization** field, the automation policy automatically evaluates all devices in SL1.
 - **If you select specific devices**, the automation policy will evaluate all selected devices.
- **Aligned Devices**. This pane displays a list of all devices aligned with the automation policy. To de-select a device, select it and click the left-arrow button.
- **Available Device Groups**. If you selected **Device Groups** in the **Align With** field, this field displays a list of all device groups in SL1. You can select one or more device groups in this field. The selected event(s) and event criteria must occur on at least one device in one of the selected device groups before the automation policy will be executed.
 - **To select a device group**, select it and click the right-arrow button.
 - **If you do not select any device groups**, the automation policy automatically evaluates all device groups to which you have access.
 - **If you select specific device groups**, the automation policy will evaluate all selected device groups.
- **Aligned Device Groups**. This pane displays a list of all device groups aligned with this automation policy. To de-select a device group, select it and click the left-arrow button.
- **Available Devices in Organization**. If you selected **Policy Organization** in the **Align With** field, this field displays only devices from the organization selected in the **Organization** field. You can select one or more devices in this field. The selected event(s) and event criteria must occur on one selected device before the automation policy will be executed.
 - **To select a device**, select it and click the right-arrow button.
 - **If you do not select any devices**, the automation policy automatically evaluates all devices associated with the organization you selected in the **Organization** field.
 - **If you select specific devices**, the automation policy will evaluate all selected devices.
- **Aligned Devices**. This pane displays a list of all devices aligned with this automation policy. To de-select a device, select it and click the left-arrow button.
- **Aligned IT Services**. This pane displays a list of all IT Services aligned with this automation policy. To de-select an IT Service, select it and click the left-arrow button.
- **Available Events**. Displays a list of all defined events in SL1. You can select one or more events in this field. One of the selected events and event criteria must occur on one selected device before the automation policy will be executed. **To select an event**, select it and click the right-arrow button. This pane also displays the ID number for each aligned event policy to ensure you select the relevant policy.
- **Aligned Events**. This pane displays a list of all events aligned with this automation policy, along with the ID number of the aligned event policy. To de-select an event, select it and click the left-arrow button.

NOTE: If a triggering event (that is, an event specified in the **Aligned Events** field is not aligned with a device (but is instead aligned with an organization), and you have also selected one or more **Aligned Actions** that must be executed on a Data Collector, SL1 will 1) Not execute the action policy; 2) Create a log entry in the audit log for the organization aligned with the triggering event, noting that the criteria in the automation policy were met, but that the action policy was not executed. This does not apply to Action Policies created on an All-In-One Appliance.

- **Available Actions.** Displays a list of all action policies in SL1. (Action policies are defined in Registry > Run Book > Actions.) You can select one or more action policies in this field. If the selected event(s) and event criteria occur on the selected devices or for the selected IT Services, the selected action policies will be executed. To select an action policy, select it and click the right arrow-button.
- **Aligned Actions.** This pane displays a list of all action policies aligned with this automation policy.
 - **To de-select an action policy**, select it and click the left-arrow button.
 - **To change the order in which one or more action policies are executed**, select the action policy and use the up-arrow or down-arrow to move the policy within the list.

NOTE: If you selected multiple action policies in the automation policy, the action policies will be executed in the order specified in the **Aligned Actions** field. To change the order of one or more action policies, select the action policy and use the up-arrow or down-arrow to move the policy within the list.

- **[Save].** Saves a new automation policy or saves changes to an existing automation policy.
- **[Save As].** If you supply a new value in the **Policy Name** field, saves the current automation policy, including any edits, as a new policy with a new name.

4. Click the **[Save]** button to save the new automation policy or save changes to an existing automation policy.

Scheduling an Automation Policy

You can use an Automation Schedule to automatically trigger Run Book Automations based on time and day, or to restrict a Run Book Automation from running during certain time windows. The actions are executed according to the schedule, regardless of event status, or you can manually execute a scheduled automation policy at any time.

For example, you can use an automation schedule to:

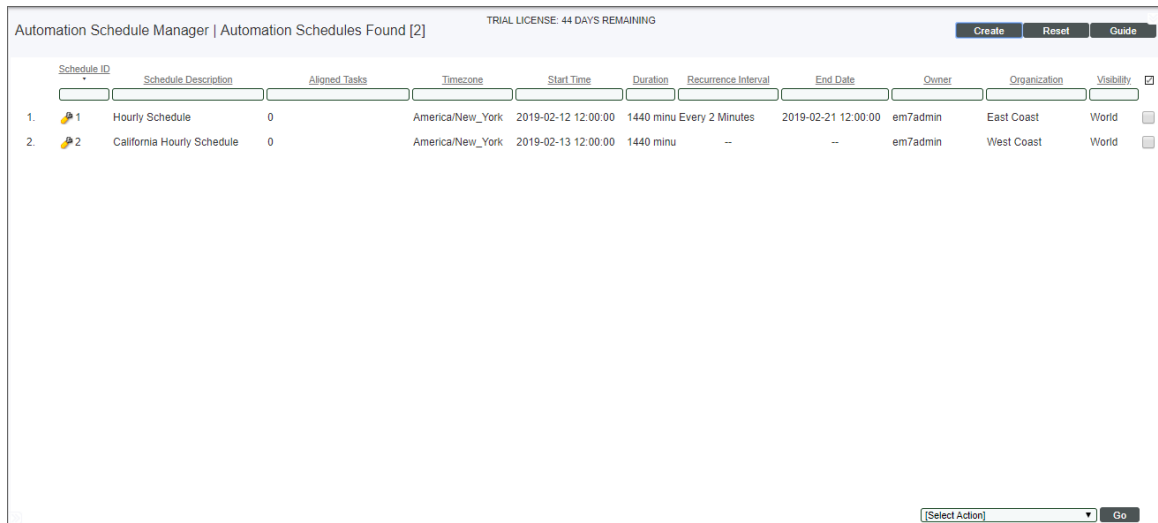
- Run a specific Run Book Automation for a given point in time (such as, tonight at midnight).
- Run a specific Run Book Automation at an interval (such as, every day at 6:00 p.m.).
- Restrict a Run Book Automation from triggering a support event during normal work hours (such as, 8:00 to 5:00).

Creating an Automation Schedule

You must create an Automation Schedule on the **Automation Schedule Manager** page before you can use it with an automation policy.



To create a schedule for an automation:

1. Navigate to the **Automation Schedule Manager** page (Registry > Run Book > Schedules).



Automation Schedule Manager | Automation Schedules Found [2] TRIAL LICENSE: 44 DAYS REMAINING

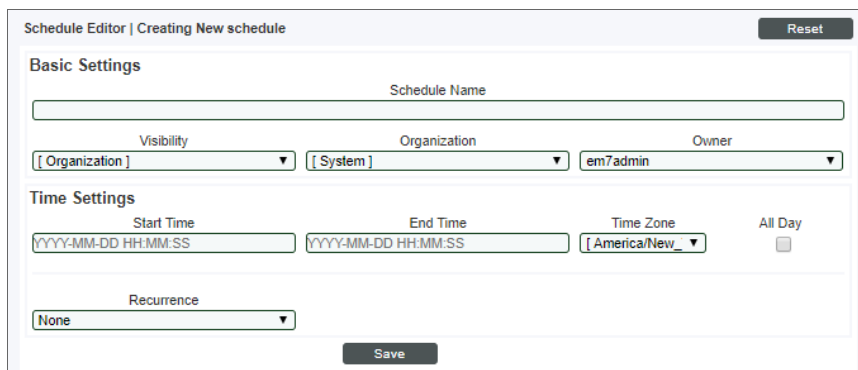
Create Reset Guide

Schedule ID	Schedule Description	Aligned Tasks	Timezone	Start Time	Duration	Recurrence Interval	End Date	Owner	Organization	Visibility
1.  1	Hourly Schedule	0	America/New_York	2019-02-12 12:00:00	1440 minu	Every 2 Minutes	2019-02-21 12:00:00	em7admin	East Coast	World <input type="checkbox"/>
2.  2	California Hourly Schedule	0	America/New_York	2019-02-13 12:00:00	1440 minu	--	--	em7admin	West Coast	World <input type="checkbox"/>

[Select Action] Go

NOTE: After an automation schedule has been associated with an automation policy, you can click the + icon next to the schedule in the **Automation Schedule Manager** page to expand a list of all automation tasks that are associated with the schedule. A task can be associated with more than one schedule, so if you disable a task, it is disabled for *all* schedules associated with that task. You align a task with a schedule when you [create the scheduled automation policy](#).

2. Click the **[Create]** button. A new **Schedule Editor** modal appears:



Schedule Editor | Creating New schedule Reset

Basic Settings

Schedule Name

Visibility Organization Owner

[Organization] [System] em7admin

Time Settings

Start Time End Time Time Zone All Day ☐

YYYY-MM-DD HH:MM:SS YYYY-MM-DD HH:MM:SS [America/New_York]

Recurrence

None

Save

3. In the **Schedule Editor** modal, complete the following fields:

Basic Settings

- **Schedule Name.** Type a name for the schedule.
- **Visibility.** Select the visibility level for the schedule. You can select one of the following:
 - *Private.* The schedule is visible only to the owner selected in the **Owner** field.
 - *Organization.* The schedule is visible only to the organization selected in the **Organization** field.
 - *World.* The schedule is visible to all users.
- **Organization.** If Visibility is set to "Organization", select the name of the organization with which this schedule is associated.
- **Owner.** Select the owner of the schedule. The default value is the username of the user who created the schedule.

Time Settings

- **Start Time.** Click in the field and select the date and time you want the schedule to start.

NOTE: If you want this automation schedule to be valid for a single point in time, do not enter an *End Time*.

- **End Time.** (Optional) If specifying a time range during which Run Book Automations associated with this schedule will run, or if specifying a time range during which Run Book Automations associated with this schedule will be restricted, select the date and time you want the schedule to end.
- **Time Zone.** Select the region or time zone for the scheduled start time.

NOTE: If you want SL1 to automatically adjust for daylight savings time (if applicable), then you must select a named region (such as *America/New York*) in the **Time Zone** field. If you select a specific time zone (such as *EST*) or a specific time offset (such as *GMT-5*), then SL1 will not automatically adjust for daylight savings time.

- **All Day.** If you want this schedule to be valid for a single day, enter a *Start Time* and select this checkbox. The *End Time* selection will be grayed out.

- **Recurrence.** Select whether you want the schedule to occur once or on a recurring basis. You can select one of the following:

- *None.* The schedule occurs only once.
- *By Interval.* The schedule recurs at a specific interval.

If you select *By Interval*, specify the interval in frequency number, then select the time interval (*Minutes, Hours, Days, Weeks, or Months*). For example:

- If you specify "6 Hours", then the schedule recurs every six hours from the time listed in the **Start Time** field.
- If you specify "10 Days", then the schedule recurs every 10 days from the date listed in the **Start Time** field.
- If you specify "2 Weeks", then the schedule recurs every two weeks, on the same day of the week as the **Start Time**.
- If you specify "3 Months" the ticket recurs every three months, on the same day of the month as the **Start Time**.

- *<Dynamic>.* The system will offer a dynamic option based on your entries in the fields above. For example, if you have created an automation schedule for date that is a first Monday of the month, your dynamic option would be *Every 1st Monday*. Use this for recurring Run Book Automations that you want to run on a particular day of the month.

- **Recur Until.** Specifies when the schedule stops recurring. You can select one of the following:
 - *No Limit.* The schedule recurs indefinitely until you disable it.
 - *Specified Date.* The schedule recurs until a specific date and time. If you select *Specified Date*, you must select a date and time in the **Last Recurrence** field.
- **Last Recurrence.** Click in the field and select the date and time you want the schedule to stop recurring.

4. Click **[Save]** to save the new schedule.

This is an example of an automation schedule for a one-time, ad hoc test:

The screenshot shows the 'Schedule Editor | Editing Schedule [2]' window. It has a 'Reset' button in the top right corner. The interface is divided into two main sections: 'Basic Settings' and 'Time Settings'.

Basic Settings:

- Schedule Name:** A text field containing 'Ad hoc test'.
- Visibility:** A dropdown menu showing '[Organization]'.
- Organization:** A dropdown menu showing '[System]'.
- Owner:** A dropdown menu.

Time Settings:

- Start Time:** A text field containing '2020-08-12 12:00'.
- Time Zone:** A dropdown menu showing '[UTC]'.
- Recurrence:** A dropdown menu showing 'None'.

At the bottom of the 'Time Settings' section, there are two buttons: 'Save' and 'Save As'.

This is an example of an automation schedule for a non-recurrent test within a date range:

The screenshot shows a 'Schedule Editor' window with a blue header bar containing the text 'Schedule Editor | Editing Schedule [1]' and a 'Reset' button. The main content area is divided into two sections: 'Basic Settings' and 'Time Settings'. In 'Basic Settings', there is a 'Schedule Name' field with the value 'Support Availability Test', and three dropdown menus for 'Visibility' (set to '[Organization]'), 'Organization' (set to '[System]'), and 'Owner'. The 'Time Settings' section includes 'Start Time' (2020-08-10 12:00), 'End Time' (2020-08-14 12:00), 'Time Zone' (set to '[UTC]'), and an 'All Day' checkbox which is unchecked. Below these is a 'Recurrence' dropdown menu set to 'None'. At the bottom of the form are 'Save' and 'Save As' buttons.

Creating an Automation Policy Limited by Schedule

After you create a schedule for the automation on the **Automation Schedule Manager** page (Registry > Run Book > RunBook Schedules), you can create an event-driven automation policy that is limited to run based on an automation schedule.

To create an event-driven automation policy that is limited to run within an automation schedule:

1. Navigate to the **Automation Policy Manager** page (Registry > Run Book > Automation).

- Click the **[Create]** button. The **Automation Policy Editor** page appears:

- In the **Automation Policy Editor** page, supply a value in each of the following fields:

- **Policy Name.** Name of the automation policy.
- **Policy Type.** Select *Active Events*.
- **Policy State.** Specifies whether the policy can be executed (Enabled) or cannot be executed (Disabled).
- **Organization.** Organization associated with the automation policy. If you select the *System* organization, the behavior of the **Available Devices** and **Available Device Groups** fields is affected.

NOTE: The organization you select must match the organization of the Automation Schedule you specify in the criteria.

- **Criteria Logic.** Specify criteria for the schedule you want to use to limit the automation policy.
 - **Time/Schedule.** Specifies the timespan during which the automation policy can execute the aligned actions. The choices for scheduled automations are:

- *and the following schedule is active.* The automation policy can execute the aligned actions during the timespan specified in the selected schedule.
 - *and the following schedule is NOT active.* The automation policy can execute the aligned actions during any time except the timespan specified in the selected schedule.
- *Schedule.* Select an available schedule in this field.
- **Align With.** Specifies whether to align this automation policy with one or more devices, one or more device groups, or one or more organizations.
 - *Devices.* The **Available Devices** field will appear below, where you can select devices to associate with the automation policy.
 - *Device Groups.* The **Available Device Groups** field will appear below, where you can select device groups to associate with the automation policy.
 - *Policy Organization.* The **Available Devices in Organization** field will appear below, where you can select one or more devices to associate with the automation policy. The list of devices comprises all devices in the organization specified in the **Organization** field.
- **Available Devices.** If you selected *Devices* in the **Align With** field, this field displays a list of all devices in SL1. You can select one or more devices in this field. The selected event(s) and event criteria must occur on one of the selected devices before the automation policy will be executed.
- **Aligned Devices.** This pane displays a list of all devices aligned with the automation policy. To de-select a device, highlight it and click the left-arrow button.
- **Aligned Device Groups.** This pane displays a list of all device groups aligned with this automation policy. To de-select a device group, highlight it and click the left-arrow button. Note that all devices contained in a device group are aligned with the automation policy when you align a device group.
- **Available Devices in Organization.** If you selected *Policy Organization* in the **Align With** field, this field displays only devices from the organization selected in the **Organization** field. You can select one or more devices in this field. The selected event(s) and event criteria must occur on one selected device before the automation policy will be executed.
- **Aligned Devices.** This pane displays a list of all devices from the specified organization that are aligned with this automation policy. To de-select a device, highlight it and click the left-arrow button.
- **Available Actions.** Displays a list of all action policies in SL1. Action policies are defined in Registry > Run Book > Actions. You can select one or more action policies to run on your schedule. To select an action policy, highlight it and click the right arrow-button.
- **Aligned Actions.** This pane displays a list of all action policies aligned with this automation policy.
 - *To de-select an action policy,* highlight it and click the left-arrow button.
 - *To change the order in which one or more action policies are executed,* highlight the action policy and use the up-arrow or down-arrow to move the policy within the list.

4. Click the **[Save]** button to save the new automation policy.

Creating an Automation Policy to Run on a Schedule

After you create an automation schedule on the **Automation Schedule Manager** page (Registry > Run Book > Schedules), you can create an automation policy to run on a schedule.

To create an automation policy that runs based on an automation schedule:

1. Navigate to the **Automation Policy Manager** page (Registry > Run Book > Automation).

- Click the **[Create]** button. The **Automation Policy Editor** page appears.

- In the Automation Policy Editor page, supply a value in each of the following fields:
 - Policy Name.** Name of the automation policy.
 - Policy Type.** Select *Scheduled*.
 - Policy State.** Specifies whether the automation policy can be executed (Enabled) or cannot be executed (Disabled).
 - Organization.** Organization associated with the automation policy. The organization should be the same as the one associated with the automation schedule you want to use.
 - Align With.** Specifies whether to align this automation policy with one or more devices, one or more device groups, or one or more organizations. Based on your setting, you must then specify the Devices, Device Groups, or Device in Organization in the field provided, as listed below.
 - Devices.* The *Available Devices* field will appear below, allowing you to select devices to associate with the automation policy.
 - Device Groups.* The *Available Device Groups* field will appear below, allowing you to select device groups to associate with the automation policy.
 - Policy Organization.* The *Available Devices in Organization* field will appear below, allowing you to select one or more devices to associate with the automation policy. The list of devices comprises all devices in the organization specified in the Organization field.

- **Available Schedules.** Displays a list of all automation schedules from the **Automation Schedule Manager** page that are not time-limited, that is, that do not have an set *End Time*. You can select one or more schedules in this field. To select an automation schedule, highlight it and click the right-arrow button.
- **Aligned Schedules.** This pane displays a list of all automation schedules aligned with this automation policy. To de-select an automation schedule, highlight it and click the left-arrow button. To change the order in which one or more automation schedules are evaluated, highlight the action policy and use the up-arrow or down-arrow to move the policy within the list. If you selected multiple automation schedules in the automation policy, the automation schedules will be evaluated in the order specified in the **Aligned Schedules** field.

In the example below, we have created an automation policy to run daily CPU diagnostics on our "Windows Automation" device group using the Windows PowerShell: Daily Run CPU Diagnostics schedule we created. We selected Aligned Actions based on the tasks we want to happen during the automation run.

The screenshot shows the 'Automation Policy Editor | Creating New Automation Policy' window. At the top, there are fields for 'Policy Name' (Daily Windows PowerShell CPU Diag), 'Policy Type' (Scheduled), 'Policy State' ([Enabled]), and 'Organization' (EMC). Below these is an 'Align With' dropdown set to 'Device Groups'. The main area is divided into three sections: 'Available Device Groups', 'Available Schedules', and 'Available Actions'. In the 'Available Device Groups' list, 'Windows Automation' is selected and moved to the 'Aligned Device Groups' list. In the 'Available Schedules' list, 'Ad hoc test' is selected and moved to the 'Aligned Schedules' list. In the 'Available Actions' list, three actions are selected and moved to the 'Aligned Actions' list: 'Execute Remote PowerShell Request [101]: Windows CPL', 'Snippet [5]: Automation Utilities: Calculate Memory Size for', and 'Snippet [5]: Datacenter Automation: Format Output as HTML'. A 'Save' button is at the bottom.

The automation schedule we created runs every day at 12:00 (America/NewYork timezone) with no end date. This automation schedule allows our automation policy to continue until we disable it.

The screenshot shows the 'Schedule Editor | Editing Schedule [4]' window. It has a 'Reset' button in the top right. The 'Basic Settings' section includes a 'Schedule Name' field with the text 'Windows PowerShell: Daily Run CPU Diagnostics', and three dropdown menus for 'Visibility' (set to '[Organization]'), 'Organization' (set to '[Windows]'), and 'Owner' (set to 'em7admin'). The 'Time Settings' section includes a 'Start Time' field (2020-08-14 12:00), a 'Time Zone' dropdown (set to '[America/New_York]'), a 'Recurrence' dropdown (set to 'By Interval'), an 'Interval' field (set to '1') and a unit dropdown (set to 'Days'), a 'Recur Until' dropdown (set to 'No Limit'), and a 'Last Recurrence' field (placeholder: 'YYYY-MM-DD HH:MM:SS'). At the bottom are 'Save' and 'Save As' buttons.

Manually Executing a Scheduled Automation Policy

When you create a scheduled automation policy, SL1 will execute that automation policy according to the schedule, regardless of event status. However, you can also manually execute the scheduled automation policy at any time.

To manually execute a scheduled automation policy:

1. Navigate to the **Automation Policy Manager** page Registry > Run Book > Automation).
2. Locate the scheduled automation policy you want to manually execute and click its lightning bolt icon (⚡). A confirmation message appears.
3. Click **[OK]** to continue. Depending on the policy, one of the following will happen:
 - If the scheduled automation policy is enabled and has at least one schedule aligned with it, the policy will execute immediately.
 - If the policy is disabled or does not have a schedule aligned with it, SL1 displays an error message and the policy will not execute.

"Clear" Policies

In an automation policy, the **Policy Type** field specifies whether the policy will be evaluated against active events or against cleared events.

If you create an automation policy with a **Policy Type** of *Clear*:

- The automation policy will be evaluated only for cleared events.
- The automation policy will contain only options for matching severity (**Criteria Logic** fields), matching ticket created or not created status (**Criteria Logic** fields), and matching text in an event message (**Match Logic** and **Match Syntax** fields).
- The automation policies will run only once (when the event is cleared) for any given event.

Aligning an Automation Policy with the System Organization

In an automation policy, the **Organization** field specifies the organization to associate with the policy and tells the automation policy which devices to evaluate. If you select the *System* organization in the **Organization** field, the behavior of the **Available Devices** field is affected.

- If you selected *Devices* in the **Align With** field, the **Available Devices** field is displayed in the **Automation Policy Editor** page.
- In the **Available Devices** field, you can select one or more devices. The selected event(s) and event criteria must occur on at least one of the selected devices before the automation policy will be executed.
 - *If you do not select any devices*, the automation policy automatically evaluates all devices associated with the organization you selected in the **Organization** field.
 - *If you do not select any devices and you selected System in the Organization field*, the automation policy automatically evaluates **all devices in SL1**.

Ordering Actions in an Automation Policy

You can align multiple action policies with a single automation policy. In addition, you can specify the order in which the SL1 system executes those aligned action policies.

Automation Policy Editor | Editing Automation Policy [8] Reset

Policy Name

Policy Type

Policy State

Policy Priority

Organization

AWS: Disable EC2 and EBS Instances by E

[Active Events]

[Disabled]

[Default]

[System]

Criteria Logic

Match Logic

Match Syntax

[Severity >=]

[Healthy,]

[and no time has elapsed]

[since the first occurrence,]

[and event is NOT cleared]

[and all times are valid]

Hourly Schedule

Repeat Time

Align With

[Only once]

[Device Groups]

☐ Include events for entities other than devices (organizations, assets, etc.)

☒ Trigger on Child Rollup

Available Device Groups

Aligned Device Groups

Servers

»

«

AWS EBS Volumes

AWS EC2 Instances

Available Events

Aligned Events

[3283] Critical: AKCP: AC Voltage sensor detects no current

[3292] Critical: AKCP: DC Voltage sensor High Critical

[3293] Critical: AKCP: DC Voltage sensor Low Critical

[3282] Critical: AKCP: Dry Contact Sensor Low Critical

[3288] Critical: AKCP: Smoke Detector Alert!

[3286] Critical: AKCP: Water Sensor has detected water

»

«

[1698] Notice: Component Device Record Created

Available Actions

Aligned Actions

SNMP Trap [1]: EM7 Event Trap

Snippet [5]: AWS: Disable Instance By Tag

Snippet [5]: AWS: Discover from EC2 IP

Snippet [5]: AWS: Get EC2 Instance Configuration

Snippet [5]: AWS: Merge Physical with Component

Snippet [5]: AWS: Vanish Terminated EC2 Instances

»

«

1. Snippet [5]: AWS: Get EC2 Instance Configuration

2. Snippet [5]: AWS: Disable Instance By Tag

↑

↓

Save Save As

Action policies can use the variable `%_EM7_RESULT_%` to retrieve the results from the previously executed action policy. Therefore, it is important that you understand the dependencies between action policies before you specify the order in which aligned action policies are executed.

For details on the variable `%_EM7_RESULT_%`, see [Using the Result of a Previous Action](#).

Automation Policies and Event Masks and Event Correlation

In SL1, events can be grouped together in a suppression group using event correlation or event masks. These grouped events can affect run book criteria.



If you selected the checkbox **Trigger on Child Rollup**, both the parent and all the child events in a suppression group can trigger the automation policy.

If you do not select the checkbox **Trigger on Child Rollup**, the default behavior is:

- For event correlation, only the parent event can trigger the automation policy.
- For event masks, only the event with the highest severity can trigger the automation policy. If multiple events have the highest severity, only the event with the highest severity and the earliest timestamp can trigger the automation policy.

Events Not Displayed on the Events Page that Might Affect Automation Policies

There are four types of events that might not be displayed on the **Events** page. Two of them have an effect on Automation Policies:

- **Topology Events.** In SL1, event correlation or topology suppression means the ability to build parent-child relationships between events. When events are correlated, only the parent event is displayed on the **Events** page. The child events are rolled up and nested under the parent event and are displayed only if you click on the magnifying-glass icon (). For the parent event, the count column will be incremented to indicate the number of correlated child events.
- **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. On the **Events** page, masked events are nested under the event with the highest severity. The magnifying-glass icon () appears to the left of the event. When you click on the magnifying-glass icon, the nested events are displayed.

The first time an event triggers an automation policy, SL1 will check to see if that event is the parent event of a suppression group due to topology events or an event mask. If the event is part of a suppression group, SL1 will trigger the automation policy only if the event is the parent event in the suppression group. Only that single event will trigger the automation policy; other events in the suppression group will not trigger the automation policy. For all future instances, only that event with the highest severity will trigger the automation policy.

Example

- Suppose you have a high-security project that requires hardware to be extremely responsive.
- Suppose this project uses Cisco network hardware.
- Suppose you want to notify key personnel immediately if the Cisco network hardware is too slow.
- You could define an automation policy that specifies the Cisco hardware to monitor and the event that is triggered when speeds are too slow.
 - The event is called "Critical: Cisco: Configuration Interface Speed to Slow".
- You could align the automation policy with an action policy that sends an email to key personnel. The action policy could send these emails to the handheld devices for these key personnel.
- The action policy is called "Email_sysadmins".


Our example automation policy might look like this:

The screenshot shows the 'Automation Policy Editor | Creating New Automation Policy' interface. The policy is named 'notify_hw_interface_speeds'. It is of type '[Active Events]', is '[Enabled]', has a priority of '[Default]', and is associated with the organization 'System'. The criteria logic is '[Severity >=]' with a value of 'Healthy'. The match logic is '[Text search]'. The repeat time is 'Every 1 minute until satisfied' and it is aligned with '[Devices]'. The 'Include events for entities other than devices (organizations, assets, etc.)' checkbox is unchecked. The 'Hourly Schedule' dropdown is set to 'Trigger on Child Rollup'. The 'Available Devices' list includes 'East Coast', 'ScienceLogic, Inc.: EM7 All-In-One: gmstack02', 'System', 'ScienceLogic, Inc.: EM7 Admin Portal: sebi-ap-15', 'ScienceLogic, Inc.: EM7 Admin Portal: tr-ap-33-148', and 'ScienceLogic, Inc.: EM7 All-In-One: AA-AIO-33-177'. The 'Aligned Devices' list includes 'System', 'Cisco Systems: 7609S: 7609S-NPE3.cisco.com', and 'Cisco Systems: CUCM Server: CUCM10-01.qa.sciencelogic.local'. The 'Available Events' list includes '[2253] Major: Cisco: FRU Control Config Operation Status for Fan Tray not UP', '[2255] Major: Cisco: FRU Control Config Operation Status for Power not ON', '[2251] Major: Cisco: FRU Control Configuration Operation Status for Module not OK', '[363] Major: Cisco: TP: Call Terminated-Configuration', '[435] Major: Cisco: TP: Call Terminated-Unsupported Protocol Configuration', and '[418] Major: Cisco: TP: TFTP Config File Issue'. The 'Aligned Events' list includes '[3215] Critical: Cisco: Configuration (CE Series) Interface Speed too slow'. The 'Available Actions' list includes 'Send Email [0]: Send Email Automation Runbook Test', 'Send Email [0]: Send Email Automation Runbook Test', 'SNMP Trap [1]: EM7 Event Trap', 'Snippet [5]: AWS: Disable Instance By Tag', 'Snippet [5]: AWS: Discover from EC2 IP', and 'Snippet [5]: AWS: Get EC2 Instance Configuration'. The 'Aligned Actions' list includes '1. Send Email [0]: Send Email Automation Runbook Test'. A 'Save' button is at the bottom.

- We specified that the automation policy:
 - Should act upon active events.
 - Is enabled.
 - Is associated with the organization "System".
 - Will be triggered by the specified event when the event has a severity greater than "Healthy".
 - Will be triggered as soon as the specified event occurs.
 - The policy will continue to trigger the action every 1 minute until the event is cleared.
 - Will be triggered when the selected event occurs on at least one of the selected Cisco devices.
 - Will be triggered when the event "Critical: Cisco: Configuration Interface Speed to Slow" occurs on the selected Cisco devices.
 - Will be triggered at all times.
- We specified that when all the criteria in the automation policy are met, the action policy "Send Email" will be executed.

Editing an Automation Policy

You can edit any parameters of an existing automation policy. To do so:

1. Navigate to the **Automation Policy Manager** page (Registry > Run Book > Automation). In the **Automation Policy Manager** page, find the automation policy you want to edit. Click its wrench icon ().



























Automation Policy Manager | Automation Policies Found [22]

TRIAL LICENSE: 43 DAYS REMAINING

Create

Reset

Guide

Automation Policy Name *	ID	Policy State	Policy Priority	Organization	Devices	Events	Actions	Edited By	Last Edited	
									All	
1.  AWS: Disable EBS Instances by EC2 Tag	9	Disabled	Default	System	1 group	1	2	em7admin	2018-09-24 15:23:39	
2.  AWS: Disable EC2 and EBS Instances by EC2 Tag	8	Disabled	Default	System	2 groups	1	2	em7admin	2018-09-24 15:23:39	
3.  AWS: Disable or Discover EC2 Instances	10	Disabled	Default	System	1 group	1	3	em7admin	2018-09-24 15:23:39	
4.  AWS: Discover EC2 Instances	11	Disabled	Default	System	1 group	1	2	em7admin	2018-09-24 15:23:39	
5.  AWS: Merge with EC2	13	Disabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:39	
6.  AWS: Vanish Terminated EC2 Instances	12	Disabled	Default	System	1 group	1	1	em7admin	2018-09-24 15:23:39	
7.  Cisco: ACI Device Class Realignment	16	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	
8.  Cisco: ACI Tenant Device Creation	14	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	
9.  Cisco: ACI Tenant Device Rename	15	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:43	
10.  Cisco: AppDynamics Application Discovery	22	Enabled	Default	System	All	2	1	em7admin	2019-01-02 15:19:29	
11.  Cisco: CSP Cluster Creation	1	Enabled	Default	System	All	1	2	em7admin	2018-09-24 15:23:08	
12.  Cisco: CSP Component Alignment	3	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:08	
13.  Cisco: CSP Component to Physical Merge	2	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:08	
14. Cisco: CUCM Root Device update	7	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:31	
15. Cisco: VOS Cluster Status Alignment	5	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:13	
16. Cisco: VOS Component to Physical Merge	6	Enabled	Default	System	All	1	1	em7admin	2018-09-24 15:23:13	

Select Action

Go

- The **Automation Policy Editor** modal page appears, populated with values from the selected automation policy.

Automation Policy Editor | Editing Automation Policy [9] Reset

Policy Name: AWS: Disable EBS Instances by EC2 Tag

Policy Type: [Active Events]

Policy State: [Disabled]

Policy Priority: [Default]

Organization: [System]

Criteria Logic: [Severity >=] [Healthy,]

Match Logic: [Text search]

Match Syntax: []

Repeat Time: [Only once]

Align With: [Device Groups]

☐ Include events for entities other than devices (organizations, assets, etc.)

☒ Trigger on Child Rollup

Available Device Groups:

- AWS EC2 Instances
- Servers

Aligned Device Groups:

- AWS EBS Volumes

Available Events:

- [3283] Critical: AKCP: AC Voltage sensor detects no current
- [3292] Critical: AKCP: DC Voltage sensor High Critical
- [3293] Critical: AKCP: DC Voltage sensor Low Critical
- [3282] Critical: AKCP: Dry Contact Sensor Low Critical
- [3288] Critical: AKCP: Smoke Detector Alert!
- [3286] Critical: AKCP: Water Sensor has detected water

Aligned Events:

- [1698] Notice: Component Device Record Created

Available Actions:

- Send Email [0]: Send Email Automation Runbook Test
- Send Email [0]: Send Email Automation Runbook Test
- SNMP Trap [1]: EM7 Event Trap
- Snippet [5]: AWS: Disable Instance By Tag
- Snippet [5]: AWS: Discover from EC2 IP
- Snippet [5]: AWS: Get EC2 Instance Configuration

Aligned Actions:

- 1. Snippet [5]: AWS: Get EC2 Instance Configuration
- 2. Snippet [5]: AWS: Disable Instance By Tag

Save Save As

- You can edit the values in one or more fields. For a description of each field, see the previous section on [creating an automation policy](#).
- Click the **[Save]** button to save your changes to the automation policy.

Deleting One or More Automation Polices

From the **Automation Policy Manager** page (Registry > Run Book > Automation), you can delete an automation policy. To do so:

- Navigate to the **Automation Policy Manager** page (Registry > Run Book > Automation).
- In the **Automation Policy Manager** page, find the automation policy you want to delete. Select its checkbox (☐)
- Select the checkbox for each automation policy you want to delete.
- Go to the **Select Action** field in the lower right of the page. Select *Delete Policies*. Click the **[Go]** button.
- Each selected automation policy is removed from SL1.

Chapter



3

Action Policies

Overview

This chapter describe how to create an action policy. An **action policy** is an action that can be automatically triggered in SL1 when certain criteria are met.

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

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

This chapter covers the following topics:

<i>What is an Action Policy?</i>	52
<i>Viewing the List of Action Policies</i>	53
<i>Filtering the List of Action Policies</i>	55
<i>Creating an Action Policy</i>	56
<i>Creating a Custom Action Type</i>	58
<i>Creating an Action Policy that Sends an Email Notification</i>	62
<i>Creating an Action Policy that Sends an SNMP Trap</i>	64
<i>Varbinds</i>	67
<i>Creating an Action Policy that Creates a New Ticket</i>	71
<i>Creating an Action Policy that Sends an SNMP Set</i>	72
<i>Creating an Action Policy that Executes an SQL Query</i>	74
<i>Creating an Action Policy that Updates an Existing Ticket</i>	76

Creating an Action Policy that Sends an AWS SNS Message	77
Creating an Action Policy that Runs an Integration Service Application	81
Creating an Action Policy that Sends an HTTP Request	83
Creating an Action Policy that Uses a Custom Action Type	84
Using the Results of a Previous Action	85

What is an Action Policy?

An **action policy** is an action that can be automatically triggered in SL1 when certain criteria are met. The triggers are defined in an automation policy (Registry > Run Book > Automation). For details on automation policies, see the section on [Automation Policies](#).

An action policy can perform one of the following tasks:

- Send an email message to a pre-defined list of users and/or external contacts.
- Send an SNMP trap from SL1 to an external device.
- Write an SNMP value to an existing SNMP object on an external device.
- Create a new ticket (using ticket templates defined in the **Ticket Templates** page [Registry > Ticketing > Templates]).
- Update an existing ticket. An action policy can change the status and/or severity of an existing ticket and/or add a note to an existing ticket. For this action policy to trigger successfully, a ticket must be associated with the event that triggered the action.

NOTE: For more details on ticket templates, see the chapter on ticket templates in the ***Ticketing*** manual.

- Query a database.
- Run a custom python script, called a **snippet**.
- Send a Message to a Topic ARN (Amazon Resource Name). All subscribers to the Topic ARN will receive the message.
- Run an Integration Service application.
- Send an HTTP request.

This chapter will describe how to create each type of action policy.

- If you want to trigger multiple actions when certain event criteria are met, you can define your automation policy to include multiple action policies.
- In an automation policy that will trigger multiple actions, you can specify the order in which the action policies are executed.
- In addition, the result of each action is available to the next executed action policy and can be accessed with the variable `%_EM7_RESULTS_%`. You can define an action policy that uses the results of the previous action policy.

Viewing the List of Action Policies

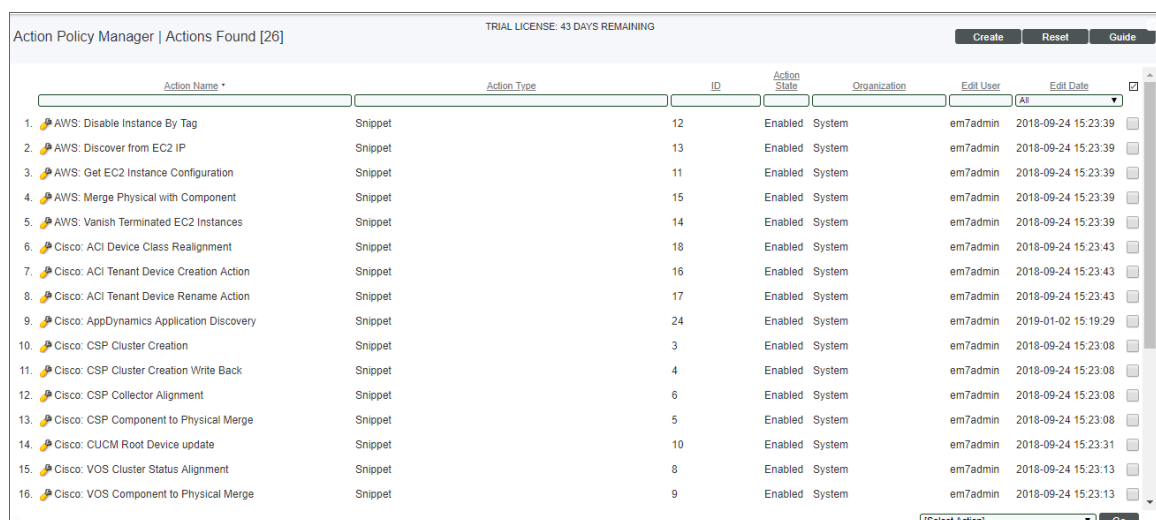
The **Action Policy Manager** page (Registry > Run Book > Actions) displays a list of all existing action policies.

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

TIP: To sort the list of action 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 **Edit Date** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

To view the list of action policies:

1. Navigate to the **Action Policy Manager** page (Registry > Run Book > Actions).



Action Name *	Action Type	ID	Action State	Organization	Edit User	Edit Date
1. AWS: Disable Instance By Tag	Snippet	12	Enabled	System	em7admin	2018-09-24 15:23:39
2. AWS: Discover from EC2 IP	Snippet	13	Enabled	System	em7admin	2018-09-24 15:23:39
3. AWS: Get EC2 Instance Configuration	Snippet	11	Enabled	System	em7admin	2018-09-24 15:23:39
4. AWS: Merge Physical with Component	Snippet	15	Enabled	System	em7admin	2018-09-24 15:23:39
5. AWS: Vanish Terminated EC2 Instances	Snippet	14	Enabled	System	em7admin	2018-09-24 15:23:39
6. Cisco: ACI Device Class Realignment	Snippet	18	Enabled	System	em7admin	2018-09-24 15:23:43
7. Cisco: ACI Tenant Device Creation Action	Snippet	16	Enabled	System	em7admin	2018-09-24 15:23:43
8. Cisco: ACI Tenant Device Rename Action	Snippet	17	Enabled	System	em7admin	2018-09-24 15:23:43
9. Cisco: AppDynamics Application Discovery	Snippet	24	Enabled	System	em7admin	2019-01-02 15:19:29
10. Cisco: CSP Cluster Creation	Snippet	3	Enabled	System	em7admin	2018-09-24 15:23:08
11. Cisco: CSP Cluster Creation Write Back	Snippet	4	Enabled	System	em7admin	2018-09-24 15:23:08
12. Cisco: CSP Collector Alignment	Snippet	6	Enabled	System	em7admin	2018-09-24 15:23:08
13. Cisco: CSP Component to Physical Merge	Snippet	5	Enabled	System	em7admin	2018-09-24 15:23:08
14. Cisco: CUCM Root Device update	Snippet	10	Enabled	System	em7admin	2018-09-24 15:23:31
15. Cisco: VOS Cluster Status Alignment	Snippet	8	Enabled	System	em7admin	2018-09-24 15:23:13
16. Cisco: VOS Component to Physical Merge	Snippet	9	Enabled	System	em7admin	2018-09-24 15:23:13

2. The **Action Policy Manager** page displays the following about each action policy:

- **Action Name.** Name of the action policy.
- **Action Type.** Action that will be executed by the action policy. Choices are:
 - *Send an Email Notification.* Sends an email message. You can specify the content of the message and the users to whom it will be sent.
 - *Send an SNMP Trap.* Sends an unsolicited SNMP message to an external system, using the ScienceLogic MIB files and predefined variables.
 - *Create a New Ticket.* Creates a new ticket, using the Ticket Templates defined in SL1.
 - *Send an SNMP Set.* Writes a value to an SNMP variable on an external device.
 - *Run a Snippet.* Executes a snippet. A snippet is a custom program, written in Python.
 - *Execute an SQL Query.* Either retrieve values from an external database or write a value to an external database. For distributed systems, the query can be sent from the Database Server or a Data Collector.
 - *Update an Existing Ticket.* Updates an existing ticket. The action can add notes, change the severity, and change the status of the ticket.
 - *Send an AWS SNS.* Sends an SNS Message to a Topic ARN (Amazon Resource Name). All subscribers to the Topic ARN will receive the message.
 - *Run Integration Service Application.* Triggers an Integration Service integration application. When you create an Automation Action using this Action Type, you specify the credential for the Integration Service instance, the application to run, and the parameters to include in the request. This Action Type is available in the *Integration Service Action Type* PowerPack.
 - *Send an HTTP request.* Sends an HTTP request to one or more devices. When you create an Automation Action using this Action Type, you specify the credential or Dynamic Application GUID, a relative URL, and the request payload. This Action Type is available in the *HTTP Action Type* PowerPack.
 - *Custom Action Type.* A Custom Action Type executes a reusable snippet. Unlike the Action Type "Snippet", a Custom Action Type can accept input parameters (in a JSON format) and create output (in a JSON format). A Custom Action Type allows a single snippet to be used in multiple Action Policies, each time with different inputs and different outputs.
- **ID.** Unique numeric identifier, automatically assigned by SL1 to each action policy.
- **Action State.** Specifies whether the policy can be executed by an automation policy (enabled) or cannot be executed (disabled).
- **Organization.** Organization associated with the action policy.
- **Edit User.** User who created or last edited the action policy.
- **Edit Date.** Date and time the action policy was created or last edited.

Filtering the List of Action Policies

The **Action Policy Manager** page (Registry > Run Book > Actions) includes seven filters. You can filter the list of action policies by one or more of the following parameters: action policy name, action type, ID, action state, organization, user who created or last edited the policy, and date the policy was created or last edited. You can specify one or more parameters to filter the list of action policies. Only action policies that meet all of the filter criteria will be displayed in the **Action Policy Manager** page.

The list of action policies is dynamically updated as you select each filter. For each filter except **Edit Date**, you must enter text to match against. SL1 will search for action policies that match the text, including partial matches. Text matches are not case-sensitive. You can use [special characters](#) in each filter.

To filter the list of action policies:

1. Navigate to the **Action Policy Manager** page (Registry > Run Book > Actions).

Action Name *	Action Type	ID	Action State	Organization	Edit User	Edit Date
1. AWS: Disable Instance By Tag	Snippet	12	Enabled	System	em7admin	2018-09-24 15:23:39
2. AWS: Discover from EC2 IP	Snippet	13	Enabled	System	em7admin	2018-09-24 15:23:39
3. AWS: Get EC2 Instance Configuration	Snippet	11	Enabled	System	em7admin	2018-09-24 15:23:39
4. AWS: Merge Physical with Component	Snippet	15	Enabled	System	em7admin	2018-09-24 15:23:39
5. AWS: Vanish Terminated EC2 Instances	Snippet	14	Enabled	System	em7admin	2018-09-24 15:23:39
6. Cisco: ACI Device Class Realignment	Snippet	18	Enabled	System	em7admin	2018-09-24 15:23:43
7. Cisco: ACI Tenant Device Creation Action	Snippet	16	Enabled	System	em7admin	2018-09-24 15:23:43
8. Cisco: ACI Tenant Device Rename Action	Snippet	17	Enabled	System	em7admin	2018-09-24 15:23:43
9. Cisco: AppDynamics Application Discovery	Snippet	24	Enabled	System	em7admin	2019-01-02 15:19:29
10. Cisco: CSP Cluster Creation	Snippet	3	Enabled	System	em7admin	2018-09-24 15:23:08
11. Cisco: CSP Cluster Creation Write Back	Snippet	4	Enabled	System	em7admin	2018-09-24 15:23:08
12. Cisco: CSP Collector Alignment	Snippet	6	Enabled	System	em7admin	2018-09-24 15:23:08
13. Cisco: CSP Component to Physical Merge	Snippet	5	Enabled	System	em7admin	2018-09-24 15:23:08
14. Cisco: CUCM Root Device update	Snippet	10	Enabled	System	em7admin	2018-09-24 15:23:31
15. Cisco: VOS Cluster Status Alignment	Snippet	8	Enabled	System	em7admin	2018-09-24 15:23:13
16. Cisco: VOS Component to Physical Merge	Snippet	9	Enabled	System	em7admin	2018-09-24 15:23:13

2. The **Action Policy Manager** page displays a list of action policies. To sort the list, you can enter a value in one or more of the following headings:
 - **Action Name.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Action Policy Manager** page will display only action policies that have a matching policy name.
 - **Action Type.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Action Policy Manager** page will display only action policies that have a matching action type.
 - **ID.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Action Policy Manager** page will display only action policies that have a matching ID. SL1 automatically assigns this unique, numeric ID to each action policy.

- **Action State.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Action Policy Manager** page will display only action policies that have the specified state (enabled or disabled).
- **Organization.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Action Policy Manager** page will display only action policies that are aligned with a matching organization.
- **Edit User.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Action Policy Manager** page will display only action policies that have a matching username in the **User Edit** field.
- **Edit Date.** Only those action policies that match all of the previously selected fields and have the specified creation date or last-edited date will be displayed. The choices are:
 - *All.* Display all action policies that match the other filters.
 - *Last Minute.* Display only action policies that have been created within the last minute.
 - *Last Hour.* Display only action policies that have been created within the last hour.
 - *Last Day.* Display only action policies that have been created within the last day.
 - *Last Week.* Display only action policies that have been created within the last week.
 - *Last Month.* Display only action policies that have been created within the last month.
 - *Last Year.* Display only action policies that have been created within the last year.

Creating an Action Policy

To create an action policy:

1. Navigate to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. In the **Action Policy Manager** page, click the **[Create]** button.
3. The **Action Policy Editor** modal page appears.

Action Editor

Policy Editor | Creating New Action Reset

Action Name Action State: [Enabled]

Description

Organization: [System] Action Type: Send an Email Notification

Email Subject: %S Event: %M Email Priority: [Normal] Send as Plain Text: ☐

Email Body

```
Severity: %S
First Occurred: %D
Last Occurred: %d
Occurrences: %c
Source: %Z
Organization: %O
Device: %X
Message: %M
```

Available Emails

- em7admin: admin@sciencelogic.com
- jsmith: mantone@sciencelogic.com
- luser: pjones@sciencelogic.com

Assigned Emails

Save

4. In the **Action Policy Editor** page, supply a value in each field.
5. For all types of action policies, the first four fields are the same.
 - **Action Name.** Specify the name for the action policy.
 - **Action State.** Specifies whether the policy can be executed by an automation policy (enabled) or cannot be executed (disabled).
 - **Description.** Allows you to enter a detailed description of the action.
 - **Organization.** Organization to associate with the action policy.
 - **Action Type.** Type of action that will be executed. Your choices are:
 - *Send an Email Notification.* Sends an email message. You can specify the content of the message and the users to whom it will be sent.
 - *Send an SNMP Trap.* Sends an unsolicited SNMP message to an external system, using the ScienceLogic MIB files and predefined variables.
 - *Create a New Ticket.* Creates a new ticket, using the Ticket Templates defined in SL1.
 - *Send an SNMP Set.* Writes a value to an SNMP variable on an external device.
 - *Run a Snippet.* Executes a snippet. A snippet is a custom program, written in Python.

- *Execute an SQL Query*. Either retrieve values from an external database or write a value to an external database. For distributed systems, the query can be sent from the Database Server or a Data Collector.
 - *Update an Existing Ticket*. Updates an existing ticket. The action can add notes, change the severity, and change the status.
 - *Send an AWS SNS Message*. Sends an SNS Message to a Topic ARN (Amazon Resource Name). All subscribers to the Topic ARN will receive the message.
 - *Run Integration Service Application*. Triggers an Integration Service integration application. When you create an Automation Action using this Action Type, you specify the credential for the Integration Service instance, the application to run, and the parameters to include in the request. This Action Type is available in the *ScienceLogic: Integration Service Action Type PowerPack*.
 - *Send an HTTP request*. Sends an HTTP request to one or more devices. When you create an Automation Action using this Action Type, you specify the credential or Dynamic Application GUID, a relative URL, and the request payload. This Action Type is available in the *HTTP Action Type PowerPack*.
 - *Custom Action Type*. A Custom Action Type executes a reusable snippet. Unlike the Action Type "Snippet", a Custom Action Type can accept input parameters (in a JSON format) and create output (in a JSON format). A Custom Action Type allows a single snippet to be used in multiple Action Policies, each time with different inputs and different outputs.
- **[Save]**. Saves a new action policy or saves changes to an existing policy.
 - **[Save As]**. If you supply a new value in the **Action Name** field, saves the current action policy, including any edits, as a new policy with a new name.

6. The remaining fields will vary, depending upon the value you selected in the **Action Type** field.

Creating a Custom Action Type

A **Custom Action Type** executes a reusable snippet. Unlike the Action Type "Snippet", a Custom Action Type can accept input parameters (in a JSON format) and create output (in a JSON format). A Custom Action Type allows a single snippet to be used in multiple Action Policies, each time with different inputs and different outputs.

A Custom Action Type is associated with an Execution Environment. An **execution environment** is an on-demand Python environment that includes the supporting modules, code, scripts, directories, and files (packaged in one or more ScienceLogic Libraries) required by the Custom Action Type. **ScienceLogic Libraries** are packages consisting of metadata and Python files that can be used by the Run Book Actions that use snippets.





You can create and edit Custom Action Types on the **Action Type Manager** page (Registry > Run Book > Action Types). The **Action Type Manager** page displays a list of all Custom Action Types and any PowerPacks that include a Custom Action Type.


TIP: To create a new Custom Action Type based on an existing Custom Action Type, you can change the values in one or more of the following fields, supply a new name for the edited Custom Action Type, and click the **[Save As]** button.

To create a New Custom Action Type:

1. Navigate to the **Action Type Manager** page (Registry > Run Book > Action Types).

Action Type Manager [BETA] | Action Types Found [2] TRIAL LICENSE: 43 DAYS REMAINING Create Reset Guide

	Name	Version	ID	State	PowerPack	Organization	Edit User	Edit Date	
1.	 Sleep for 2 seconds	2.0	101	Enabled	--	System	em7admin	2019-02-13 14:41:32	
2.	 Timed Action	1.0	100	Enabled	--	System	em7admin	2019-02-13 14:39:24	

[Select Action]  Go

2. On the **Action Type Manager** page, click the **[Create]** button. The Action Type Editor page appears:

The screenshot shows the 'Action Type Editor | Creating a New Action Type' interface. At the top right is a 'Reset' button. Below the title bar are several input fields and dropdowns: 'Name' (containing 'Timed Action'), 'Version' (containing '1.0'), 'State' (a dropdown menu showing '[Enabled]'), 'Organization' (a dropdown menu showing '[System]'), 'Description' (an empty text box), and 'Execution Environment' (a dropdown menu showing '[-- Default Environment]'). Below these are two side-by-side text areas for 'Input Parameters Definition' and 'Output Parameters Definition'. The 'Input Parameters Definition' area contains a JSON array: `[{ "name": "seconds", "type": "number" }]`. The 'Output Parameters Definition' area contains a JSON object: `{ "type": "number" }`. Below these is a large text area labeled 'Snippet' containing a Python code snippet: `import time
time.sleep(seconds)
EM7_RESULT = seconds`. At the bottom center is a 'Save' button.

3. Complete the following fields:
 - **Name**. Specify the name of the Custom Action Type. Can be any combination of alpha-numeric characters, up to 255 characters in length.
 - **Version**. Version number for the Custom Action Type. Can be any combination of alpha-numeric characters, up to 64 characters in length.
 - **State**. Specifies whether the Custom Action Type can be executed by an action policy (Enabled) or cannot be executed (Disabled).
 - **Organization**. The organization associated with the Custom Action Type.
 - **Description**. A description of the action type. Can be any combination of alpha-numeric characters, up to 255 characters in length.
 - **Execution Environment**. Select from the list of available Execution Environments. The default execution environment is System.
 - **Input Parameters Definition**. A JSON structure that specifies each input parameter. Each parameter definition includes its name, data type, and whether the input is optional or required for this Custom Action Type. For example:

```
[{"name": "param", "type": "string", "required": true}]
```

NOTE: Input parameters must be defined as a JSON structure, even if only one parameter is defined.

NOTE: Currently, the only supported input data types are "number", "string", and "boolean".

- **Output Parameters Definition.** A JSON structure that specifies the output parameter. The parameter definition must include its name and data type. For example:

```
[{"name": "success", "type": "boolean"}]
```

NOTE: The output parameter definition is limited to a single parameter.

- **Snippet.** Specify the python code that will be executed when SL1 runs the action policy associated with this Custom Action Type. For example:

```
EM7_RESULT = {"success": True, "data": param}
```

4. Click the **[Save]** button to save the new action type.

Examples:

Here is an example Custom Action Type called "Timed Action":

- **Name.** Timed Action.
- **Version.** 1.0
- **State.** Enabled
- **Organization.** System
- **Description.**
- **Execution Environment.** System
- **Input Parameters Definition.**

```
[{"name": "seconds", "type": "number" }]
```

- **Output Parameters Definition.**

```
{ "type": "number" }
```

- **Snippet.**

```
import time
time.sleep(seconds)
EM7_RESULT = seconds
```

Here is an Action Policy called "Sleep for 2 Seconds" that uses the Custom Action Type called "Timed Action":

- **Action Name.** Sleep For 2 Seconds
- **Action State.** Enabled
- **Description.**
- **Organization.** System
- **Action Type.** Timed Action (1.0)
- **Execution Environment.** Default
- **Action Run Context.** Database
- **Input Parameters.**

```
{ "seconds": 2 }
```

Creating an Action Policy that Sends an Email Notification

In the **Action Policy Editor** page, if you selected the **Action Type** of *Send an Email Notification*, the new action policy will send an email message. You can specify the content of the email message and the users to whom the email message will be sent. If the action is aligned with an automation policy (i.e., if the action policy is included in the definition of an automation policy), and the criteria in the automation policy are met, the email message will be sent.

An action policy that sends an email notification is useful when you must immediately inform key personnel about event conditions.

NOTE: When an automation policy executes actions, the time stamps for the actions will use the time zone defined in the **System Timezone** field (System > Settings > Behavior page). However, the timestamp for the Event Action Log window will display the user's local time zone, as defined in the **Account Information** page (Preferences > Account > Information). For more information, see "My Contact Information" in the Introduction to SL1 > User Preferences section of the user manual.

NOTE: In the **Email Subject** and **Email Body** fields, you can use one or more of the variables from the [list of variables](#). The value of each variable will be retrieved from the event that triggered the automation policy.

NOTE: In the **Behavior Settings** page (System > Settings > Behavior), make sure that the value in the **Interface URL** does not include a trailing forward slash (/). When SL1 generates URLs for tickets or events (and includes those URLs in email messages), the trailing forward slash causes problems with the generated URL.

To define an action policy that sends an email notification, you must supply values in the general fields, as specified in the [section on Creating an Action Policy](#) and also supply values in the following fields:

The screenshot shows the 'Action Editor' window with the title bar 'Close / Esc'. The main area is titled 'Policy Editor | Creating New Action' and includes a 'Reset' button. The configuration fields are as follows:

- Action Name:** Email_sysadmins
- Action State:** [Enabled]
- Description:** (Empty text field)
- Organization:** [System]
- Action Type:** Send an Email Notification
- Email Subject:** %S Event: %M
- Email Priority:** [Normal]
- Send as Plain Text:** (Unchecked checkbox)
- Email Body:**

```
Severity: %S
First Occurred: %D
Last Occurred: %d
Occurrences: %c
Source: %Z
Organization: %O
Device: %X
```
- Available Emails:**
 - lvaruolo: lvaruolo@sciencelogic.com
 - mcooley: mcooley@sciencelogic.com
 - mhussain: mhussain@sciencelogic.com
 - mluebke: mluebke@sciencelogic.com
 - mpanciera: mpanciera@sciencelogic.com
 - npeters: npeters@sciencelogic.com
 - rdanner: rdanner@sciencelogic.com
 - rsandwick: rsandwick@sciencelogic.com
- Assigned Emails:**
 - bleyland: bleyland@sciencelogic.com
 - mantone: mantone@sciencelogic.com

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

- **Email Subject.** This will be the subject text in the outgoing email message. By default, the subject will be:

%S Event: %M.

where %S is the event's severity and %M is the message that appears on the **Events** page when the event occurs.
- **Email Priority.** You can select *High*, *Normal*, or *Low*. However, be aware that email clients each handle priority differently.
- **Send as Plain Text.** Select this checkbox if you want the email sent as plain text, without any special formatting.

- **Email Body.** The body of the outgoing email message. You can include additional variables from the [list of variables](#) in the email body. By default, the body will be:

Severity: %S

First Occurred: %D

Last Occurred: %d

Occurrences: %c

Source: %Z

Organization: %O

Device: %X

Message: %M

Sent by Automation Action: %N

View this event at: %H

NOTE: If you want to specify that the email be sent as an HTML message, include "<html> <body>" at the very beginning and "</body> </html>" at the very end of the **Email Body** field.

- **Available Emails.** List of all email addresses associated with users and external contacts. You can select one or more email addresses to align with the action. To select an email address, highlight and then click the right-arrow button. The email address will then appear in the **Assigned Emails** pane. If the action is associated with an automation policy, and the criteria in the automation policy are met, the SL1 system will send an email to the users and external contacts in the **Assigned Emails** pane.
- **Assigned Emails.** If the action is associated with an automation policy, and the criteria in the automation policy are met, SL1 will send an email message to the selected email address(es).

Creating an Action Policy that Sends an SNMP Trap

In the **Action Policy Editor** page, if you selected the **Action Type** of *Send an SNMP Trap*, the new action policy will send an unsolicited SNMP message to a device. If the action is associated with an automation policy, and the criteria in the automation policy are met, the SL1 system sends the SNMP trap to the specified device. When you select this type action type, you must manually build the trap that will be sent. You do so in the **Action Policy Editor**.

An SNMP trap is a message is initiated by a network device or network application and sent to a network management system. For example, a router could send a message if one of its redundant power supplies fails or a printer could send an SNMP trap when it is out of paper.

An action policy that sends an SNMP trap is useful when you want to integrate SL1 with an existing network management system. When certain event conditions are met (as defined in the automation policy), SL1 can build an SNMP trap to pass the event information to another network management system.

Using the Default ScienceLogic MIBs to Build an SNMP Trap

When you create an action policy that sends an SNMP trap, you must manually build the trap that will be sent. You build the trap in the **Action Policy Editor** page. In the action policy, you assign an OID number to the trap. One or more variables can be included in the trap. These variables are called **varbinds**. A varbind is referenced by an OID number, has a data type, and stores a dynamic value. You also define the varbinds in the **Action Policy Editor** page. For each varbind in the trap, you define the OID number, data type, and value.

If the receiver of the trap will perform actions based on the trap, best practice is to define a MIB file and send it to the receiver. This allows the receiver to decode and act upon the trap.

Default Traps from SL1

In most cases, you can use the default ScienceLogic MIB files to build SNMP traps from SL1. When you use the ScienceLogic MIB files, you are not required to define your own MIB files. You can simply export the ScienceLogic MIB files and send them to the trap receiver. When building traps in the **Action Policy Editor** page, you can then use the trap OIDs and varbind OIDs defined in the ScienceLogic MIB files, and the receiver will know how to decode each trap.

You can view the MIB files in the **MIB Compiler** page (System > Tools > MIB Compiler).

- **SCIENCELOGIC-COMMON-MIB**. Defines the root OID for ScienceLogic.com (19567) and the products associated with SL1.
- **SCIENCELOGIC-EVENT-MIB**. Defines varbinds for all the event information that can be included in a trap.
- **SCIENCELOGIC-TRAP-MIB**. Defines two basic types of traps, severity-based traps, or event-type traps. Both types of traps can contain one, multiple, or all varbinds from the SCIENCELOGIC-EVENT-MIB.

If you choose to use the default ScienceLogic MIB files, you must configure the external system to receive traps from SL1. The MIB file SCIENCELOGIC-TRAP-MIB defines two types of event-based traps:

- **Severity-based traps**. These traps specify that an event of a certain severity has occurred. The trap contains details on the event, including the event message and the element associated with the event.
- **Event Type-based Traps**. These traps specify the event's policy ID. The trap contains details on the event, including the event message, event severity, and the element associated with the event. This type of trap allows you to define a unique trap OID for each event definition in SL1.

You must configure the receiving system to look for the traps.

- If you will send **event severity-based** traps:
 - You must configure the receiving system to look for traps with the following OIDs:

Event Severity	OID
Critical event	.1.3.6.1.4.1.19567.2.1.0.0.1
Major event	.1.3.6.1.4.1.19567.2.1.0.0.2
Minor event	.1.3.6.1.4.1.19567.2.1.0.0.3
Notice event	.1.3.6.1.4.1.19567.2.1.0.0.4
Healthy event	.1.3.6.1.4.1.19567.2.1.0.0.5

- You must then define your traps (in the **Action Policy Editor** page) using these OIDs. When you specify the **Trap OID**, use these OIDs.
- If you will send **event type-based** traps:
 - You must configure the receiving system to look for traps with the following OIDs:

.1.3.6.1.4.1.19567.2.1.0.2.1.event_policy_ID
 - If you want the receiving system to accept and act on all of these traps, you can tell the receiving system to look for all traps that begin with the OID .1.3.6.1.4.1.19567.1.0.2.1.
 - If you want the receiving system to perform different actions depending upon the type of event, you can use the event_policy_ID at the end of each trap OID to sort and separate the traps by type of event.
 - You must then define your traps (in the **Action Policy Editor** page) using the OIDs .1.3.6.1.4.1.19567.2.1.0.2.1.event_policy_ID. When specifying the **Trap OID**, you can use the %3 variable like this:

.1.3.6.1.4.1.19567.2.1.0.2.1.%3

SL1 will append the current event's policy ID to the trap OID. (The current event will be the event that triggered the action policy. This event is specified in the automation policy.)

Varbinds

If you want to use an already defined MIB file and already defined OIDs, you can use the ScienceLogic MIB files SCIENCELOGIC-TRAP-MIB and the SCIENCELOGIC-EVENT-MIB and then dynamically assign values to the OIDs in those files. You can view the MIB files in the **MIB Compiler** page (System > Tools > MIB Compiler).

If you use the ScienceLogic MIB files, specifically the SCIENCELOGIC-EVENT-MIB files, you can include one or more of the following variables (called **varbinds**) in each outgoing trap. You can assign values to these variables using the event variables described in the appendix on [Variables](#).

Description	OID	Type	Associated Event Variable
Event ID	.1.3.6.1.4.1.19567.2.1.1.1.1	Integer	%e
Severity of the event, in numeric format. Possible values are 0 = healthy 1 = notice 2 = minor 3 = major 4 = critical	.1.3.6.1.4.1.19567.2.1.1.1.2	Integer	%s
Source of the event. Possible values are: syslog=1 internal=2 trap=3 dynamic=4 email=7 other=8	.1.3.6.1.4.1.19567.2.1.1.1.3	Integer	%z

Description	OID	Type	Associated Event Variable
Type of element that this event is tied to. Possible values are: organization=0 device=1 asset=2 network=4 interface=5 vendor=6 account=7 virtual interface=8 device group=9 IT service=10 ticket=11	.1.3.6.1.4.1.19567.2.1.1.1.4	Integer	%l (one)
Unique element ID. For example, if the elementType is device, the elementID corresponds to the ScienceLogic device ID.	.1.3.6.1.4.1.19567.2.1.1.1.5	Integer	%x
Element name from SL1. Examples of element names are device hostname and organization name.	.1.3.6.1.4.1.19567.2.1.1.1.6	String	%X
Network address of an element. Typically this is an IP address.	.1.3.6.1.4.1.19567.2.1.1.1.7	String	N/A
Unique organization ID.	.1.3.6.1.4.1.19567.2.1.1.1.8	Integer	%o (lowercase "oh")
Organization Name	.1.3.6.1.4.1.19567.2.1.1.1.9	String	%O (uppercase "oh")
Event description (from event's definition)	.1.3.6.1.4.1.19567.2.1.1.1.10	String	%M

Description	OID	Type	Associated Event Variable
Type of sub-element that this event is tied to. Possible values for organizations are: news feed=0 Possible values for devices are: cpu=1 disk=2 filesystem=3 memory=4 swap=5 component=6 interface=7 software=8 process=9 port=10 service=11 content=12 mail=13	.1.3.6.1.4.1.19567.2.1.1.1.11	Integer	%2 (two)
Unique sub-element ID. For example, if the subElementType is disk, the subElementID corresponds to the disk ID.	.1.3.6.1.4.1.19567.2.1.1.1.12	Integer	%y
Name of sub-element associated with the event	.1.3.6.1.4.1.19567.2.1.1.1.13	String	%Y

Example Trap

The following is an example of a trap that could be built with an action policy. This trap is event-type based (note the OID):

```
Trap Received: (.1.3.6.1.4.1.19567.2.1.0.2.1.217) | Trap Detail : eventID: 32755;
eventSeverity: 5; eventSource: 2; elementType: 1; elementID: 119; elementName:
webserver01; elementAddress: 192.168.11.30; roaID: 0; roaName: System; eventMessage:
CPU usage now below threshold (load now: 2%); subElementType: 0; subElementID: 0;
subElementName;;
```

Creating the Action Policy

To define an action policy that sends an SNMP trap to an external device, you must supply values in the general fields, as specified in the section on [Creating an Action Policy](#) and also supply values in the following fields:

The screenshot shows the 'Action Editor' window with the title 'Policy Editor | Creating New Action'. It contains several input fields and buttons. The 'Action Name' field is set to 'Event Trap' and 'Action State' is set to '([Enabled]'. The 'Description' field is empty. The 'Organization' is set to '([System]' and 'Action Type' is 'Send an SNMP Trap'. The 'Trap Host' is 'localhost' and 'Trap Credential' is 'SNMP Public V1'. The 'Trap OID' is '1.3.6.1.4.10267.2.1.5.2.1.53'. Below these are sections for 'New Varbind' and 'Current Varbinds'. The 'New Varbind' section has fields for 'Varbind OID' (1.3.6.1.4.10267.2.1.1.1.1), 'Varbind Value Type' (SNMP Integer), and 'Varbind Value'. The 'Current Varbinds' list contains one entry: '1.3.6.1.4.10267.2.1.1.1.1: = 1e'. Buttons for 'Save', 'Reset', and arrow controls are also visible.

- **Trap Host.** IP address of the external device to which you want to send a trap.
- **Trap Credential.** SNMP credential that allows SL1 to send information to the external device. The list of credentials is filtered to include only those credentials to which you have access.

If this field has already been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the list in this field; you will not be able to re-align the device with the *Restricted Credential*.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the **Trap Credential** field. For more information, see the **Discovery and Credentials** manual.

- **Trap OID.** Object identifier for the trap. If you are using the default ScienceLogic MIB files to build traps, see [Default Traps from the ScienceLogic platform](#) to determine which OID to enter in this field.
- **Varbind OID.** Object identifier (in dotted decimal notation) of the variable.
- **Varbind Value Type.** Data type contained in the variable.
- **Varbind Value.** Value to assign to the variable. You can use the event variables to assign values to the trap variables. This ensures that values from the event specified in the automation policy are included in the trap.
- Supply values in the **Varbind OID**, **Varbind Value Type**, and **Varbind Value**, then click the right-arrow button (>>) to add the varbind to the **Current Varbinds** pane. Repeat this step for each variable you want to include in the trap. If you are using the default ScienceLogic MIB files to build traps, see the section on [Varbinds](#) to determine the **Varbind OID**, **Varbind Value Type**, and **Varbind Value**.
- Each defined variable will appear in the **Current Varbinds** pane. To edit a varbind, highlight it in the **Current Varbinds** pane and click the left-arrow button (<<). The **Varbind OID**, **Varbind Value Type**, and **Varbind Value** fields will be populated with values from the selected varbind.

NOTE: In the *Trap OID* field, *Varbind OID* field, and the *Varbind Value* field, you can use the variables described in the appendix on [Variables](#). The value of each variable will be retrieved from the event that triggered the automation policy.

Creating an Action Policy that Creates a New Ticket

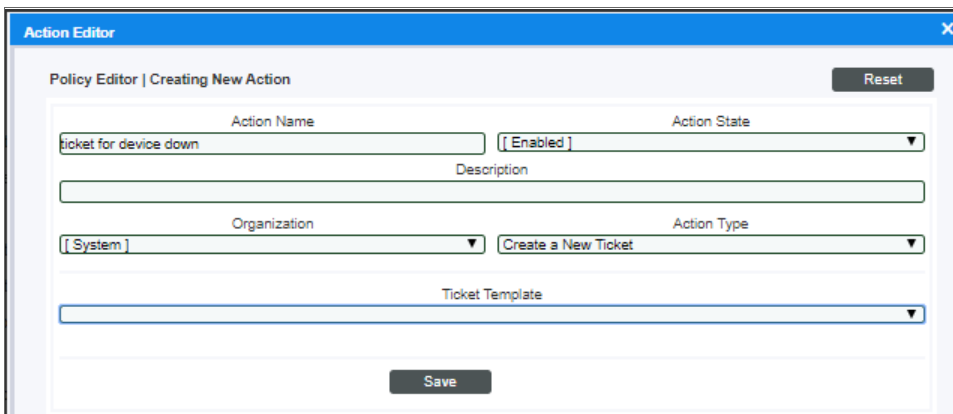
In the **Action Policy Editor** page, if you selected the **Action Type** of *Create a New Ticket*, the new action policy will generate a ticket in SL1. The value in each ticket field is supplied by a ticket template. Ticket templates are defined in the **Ticket Templates** page (Registry > Ticketing > Templates page.) If the action is associated with an automation policy, and the criteria in the automation policy are met, SL1 will generate a ticket.

NOTE: For more details on ticket templates, see the chapter on ticket templates in the *Ticketing* manual .

An action policy that automatically generates a ticket is useful when you want to immediately assign a task based on event conditions. When certain event conditions are met (as defined in the automation policy), SL1 can automatically create a ticket that describes the task to be performed and specifies who should perform that task.

To ensure that the generated ticket includes data from the event triggered in the automation policy, you can define a ticket template that uses event variables. These variables are described in the appendix on [Variables](#) and can be used in the **Description** and **Notes** fields of the ticket template.

To define an action policy that creates a ticket, you must supply values in the general fields, To define an action policy that sends an email notification, you must supply values in the general fields, as specified in the section on [Creating an Action Policy](#), and also supply values in the following fields:

The screenshot shows a web-based 'Action Editor' window. The title bar is blue with the text 'Action Editor' and a close button. The main content area is titled 'Policy Editor | Creating New Action' and includes a 'Reset' button in the top right. The form contains several fields: 'Action Name' with the value 'ticket for device down', 'Action State' with a dropdown menu showing '[Enabled]', a 'Description' text area, 'Organization' with a dropdown menu showing '[System]', 'Action Type' with a dropdown menu showing 'Create a New Ticket', and 'Ticket Template' with a dropdown menu. A 'Save' button is located at the bottom center of the form.

- **Ticket Template.** From this field, you can select from a list of ticket templates. Ticket templates are defined in the **Ticket Templates** page (Registry > Ticketing > Templates). All ticket templates defined with a **Feature Use of Automation** will appear in this drop-down list. Each of these ticket templates is listed in the **Ticket**

Template field by ID and name. The ticket template will populate the fields for the ticket that is created by the action policy.

NOTE: For more details on ticket templates, see the chapter on ticket templates in the *Ticketing* manual.

Creating an Action Policy that Sends an SNMP Set

The Action Type of *Send an SNMP Set* writes a value to an SNMP variable on an external device. In the action policy, you can specify the variable to write to and the value to write. If the action policy is associated with an automation policy, and the criteria in the automation policy are met, SL1 will write a value to the variable on the external device.

In the **Action Policy Editor** page, you can specify the SNMP variable to change and the value to assign to the SNMP variable.

For increased flexibility and connectivity, you can specify whether the SNMP Set should be executed by the Database Server or by the Data Collector. In some cases, a device might not accept connections from the Database Server or may not be "visible" from the Database Server. In these situations, you can specify that the SNMP Set be executed by the Data Collector.

NOTE: For SL1 systems that are using an All-In-One Appliance, you cannot choose to execute a policy on an Database Server or an Data Collector. All policies will be executed on the All-In-One Appliance.

An action policy that automatically changes the value of an SNMP variable on an external device is useful when you want to perform some automatic steps on the device to resolve a problem. For example, the external device could run a script that is triggered when the value of an SNMP variable is set to "5". You could also use such an action policy to create a custom status or a custom message and store that custom status or custom message in an SNMP variable.

NOTE: Before you can write a value to an SNMP variable on an external device, you must be aware of the SNMP structure on the external device and the list of SNMP variables on the external device.

To define an action policy that changes an SNMP variable on an external device, you must supply values in the general fields, as specified in the section on [Creating an Action Policy](#), and also supply values in the following fields:

- **SNMP Host.** IP address of the external device where you want to write an SNMP value.
- **SNMP Credential.** SNMP credential that allows SL1 to send information to the external device. The list of credentials is filtered to include only those credentials to which you have access.

If this field has already been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the list in this field; you will not be able to re-align the device with the *Restricted Credential*.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the **SNMP Credential** field. For details, see the **Discovery and Credentials** manual .

- **Action Run Context.** This option is not available on All-In-One Appliances. Specifies whether the action will be executed on the Database Server or on the Data Collector. The Choices are:
 - *Database.* Execute the action from the Database Server.
 - *Collector.* Execute the action from the Data Collector associated with the device. This is useful when a device doesn't accept connections from the Database Server or may not be "visible" from the Database Server.

NOTE: If the triggering event (that is, the event specified in the automation policy that triggered this action policy) is not aligned with a device, and you select *Collector* in the **Action Run Context** field, SL1 will 1) Not execute the action policy; 2) Create a log entry in the audit log for the organization aligned with the triggering event, noting that the criteria in the automation policy were met, but that the action policy was not executed.

- **SNMP OID.** Object identifier for the variable on the external device to which you want to write a value.
- **SNMP Value Type.** Data type contained in the variable.
- **SNMP Value.** Value to assign to the variable.

NOTE: In the **SNMP Host** field, the **SNMP OID** field, and the **SNMP Value** field, you can use one or more of the variables described in the appendix on [Variables](#). The value of each variable will be retrieved from the event that triggered the automation policy.

Creating an Action Policy that Executes an SQL Query

In the **Action Policy Editor** page, if you selected the **Action Type** of *Execute an SQL Query*, the new action policy will execute an SQL query against an external database on an external device. The SQL query can either retrieve values from an external database or write values to an external database. If the action policy is aligned with an automation policy (i.e., if the action policy is included in the definition of an automation policy), and the criteria in the automation policy are met, SL1 will execute the query.

In the **Action Policy Editor** page, you specify the database you want to query and the SQL query to execute.

An action policy that automatically executes an SQL query is useful when you want to integrate event information from SL1 with an external application that is database-based. For example, suppose you want an event to trigger a ticket on an external ticketing system. Suppose the ticketing system is database-based. If you know the database and table structure on the external ticketing system, you could use an action policy to manually create a ticket in the external database.

For increased flexibility and connectivity, you can specify whether the SQL query should be executed by the Database Server or by the Data Collector. In some cases, a device might not accept connections from the Database Server or may not be "visible" from the Database Server. In these situations, you can specify that the SQL query be executed by the Data Collector.

NOTE: For SL1 systems that are using an All-In-One Appliance, you cannot choose to execute a policy on a Database Server or a Data Collector. All policies will be executed on the All-In-One Appliance.

To define an action policy that executes an SQL query on an external database, you must supply values in the general fields, as specified in the section on [Creating an Action Policy](#), and also supply values in the following fields:

- **Database Credential.** Credential that allows SL1 to send a query to the external database. The database to query is specified in the credential. The list of credentials is filtered to include only those credentials to which you have access.

If this field has already been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the list in this field; you will not be able to re-align the device with the *Restricted Credential*.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the **Database Credential** field. For details, see the **Discovery and Credentials** manual.

- **Action Run Context.** This option is not available on All-In-One Appliances. Specifies whether the action will be executed on the Database Server or on the Data Collector. The choices are:
 - *Database.* Execute the action from the Database Server.
 - *Collector.* Execute the action from the Data Collector associated with the device. This is useful when a device doesn't accept connections from the Database Server or may not be "visible" from the Database Server.
- **SQL Query.** SQL query to execute.

NOTE: In the **SQL Query** field, you can use the variables described in the appendix on [Variables](#). The value of each variable will be retrieved from the event selected in the automated policy.

NOTE: SL1 automatically performs an "auto-commit" action for each query, to save the change to the database. You are not required to create a separate "commit" clause for the queries in an action policy.

NOTE: If you clicked the **Code Highlighting** in the **Account Preferences** page (Preferences > Account > Preferences), the code in the **SQL Query** field appears with syntax highlighting.

Creating an Action Policy that Updates an Existing Ticket

The Action Type of *Update an Existing Ticket* edits an existing ticket in SL1. The action can change the status, severity, and/or add a note to an existing ticket. The existing ticket must be associated with the event that triggers the automation policy that executes the action policy. This means that a user manually created the ticket from an instance of an event or that another Run Book Action Policy created the ticket. If the *Update an Existing Ticket* action is associated with an automation policy, and the criteria in the automation policy are met, SL1 will edit the ticket.

An action policy that automatically edits a ticket is useful when you want to automate tasks in your escalation processes. For example, you could define an automation policy that specifies if an event is still active after a certain time period (that is, the event has not been cleared), increase the severity of the ticket. Conversely, you could define an automation policy that automatically resolves the ticket associated with an event when that event is cleared.

In the **Action Policy Editor** page, if you selected the **Action Type** of *Update an Existing Ticket*, you must supply values in the fields, as specified in the section on [Creating an Action Policy](#), and also supply values in the following fields:

- **Set Ticket Status.** Specifies the status to assign to the ticket. Choices are:
 - *Don't Change Status*
 - *Open*
 - *Working*
 - *Pending*
 - *Resolved*
- **Set Ticket Severity.** Specifies how the severity of the ticket will be modified, or a specific severity to assign to the ticket. Choices are:
 - *Don't Change Severity*
 - *Increment Severity*
 - *Decrement Severity*
 - *Healthy*
 - *Notice*

- *Minor*
- *Major*
- *Critical*

- **Add Ticket Note.** Specifies text to add to the ticket as a note, like notes added with the **Notepad Editor**.

NOTE: For details on Ticket Status, Ticket Severity, and adding a note to a ticket, see the chapter on *Creating and Editing Tickets* in the **Ticketing** Manual.

Creating an Action Policy that Sends an AWS SNS Message

The Action Type of "Send an AWS SNS message" sends an SNS (Amazon Simple Notification Service) message to a Topic ARN (Amazon Resource Name). All subscribers to the Topic ARN will receive the message.

An action policy that sends an AWS SNS message is useful when you already have access to an AWS account through discovery and monitoring and would like to use the AWS ARN publish/subscribe model to send event notifications to users.

Setting up a Topic ARN in AWS

This information is provided as a courtesy to help you configure the action policy successfully. Use the following procedure to prepare an AWS Topic ARN. For details, refer to the Amazon Web Services documentation (<https://docs.aws.amazon.com/>).

1. From your AWS account, create a new SNS topic (**Amazon SNS > Topics > Create Topic**). Enter a *Topic Name*.

- a. Set the access policy to the least restrictive for testing, as shown.

▼ Access policy - optional
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. [Info](#)

Choose method

☒ **Basic**
Use simple criteria to define a basic access policy

☐ **Advanced**
Use a JSON object to define an advanced access policy.

Define who can publish messages to the topic

☐ **Only the topic owner**
Only the owner of the topic can publish to the topic

☒ **Everyone**
Anybody can publish

☐ **Only the specified AWS accounts**
Only the specified AWS account IDs can publish to the topic

Define who can subscribe to this topic

☐ **Only the topic owner**
Only the owner of the topic can subscribe to the topic

☒ **Everyone**
Any AWS account can subscribe to the topic

☐ **Only the specified AWS accounts**
Only the specified AWS account IDs can subscribe to the topic

☐ **Only requesters with certain endpoints**

JSON preview

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:Publish",
        "SNS:RemovePermission",
        "SNS:SetTopicAttributes",
        "SNS>DeleteTopic",
        "SNS:ListSubscriptionsByTopic",

```

- b. Click **Create Topic**. Note the *Topic ARN ID*, as you will need this to set up the message and the action policy.
2. From the SNS console, create a subscription to the Topic ARN (**Amazon SNS > Subscriptions > Create Subscription**).
- a. Click **Create subscription**.
- b. Enter the **Topic ARN ID**.
- c. Select "Email" as the *Protocol*.
- d. Enter a valid email address as the *Endpoint*.
- e. Click **Create subscription**.
3. Confirm your subscription in the email confirmation sent from AWS.

Creating the Action Policy for AWS SNS

In the **Action Policy Editor** page, if you selected the **Action Type** of *Send an AWS SNS message*, you must supply values in the required fields, as specified in the section on [Creating an Action Policy](#), and also supply values in the following AWS SNS fields:

- **SNS Subject**. This field is optional. This field specifies the subject line for the SNS message. This field cannot exceed 100 characters and cannot contain newline characters or any special characters. You can include variables in this field.
- **SNS Credential**. Select a credential of type "SOAP/XML" that will allow SL1 to access the specified **Topic ARN** and **Region**.
- **Topic ARN**. The Topic ARN to which you want to send the SNS message. All subscribers to the Topic ARN will receive the SNS message.

- **Region Name.** AWS region with which the Topic ARN is associated.
- **SNS Body.** The body of the SNS message. You can include variables in this field.

The screenshot shows the 'Action Editor' window in the AWS IAM console. The title bar says 'Action Editor'. Inside, the header reads 'Policy Editor | Editing Action [37]' with a 'Reset' button on the right. The form contains the following fields:

- Action Name:** 'RBA Base Pack: SNS Notification SILOPOV'
- Action State:** '[Enabled]' (dropdown)
- Description:** (empty text box)
- Organization:** '[System]' (dropdown)
- Action Type:** 'Send an AWS SNS message'
- SNS Subject:** '%S event on %X in org %O'
- SNS Credential:** 'AWS POV' (dropdown)
- Topic ARN:** 'arn:aws:sns:us-east-1:211723050304:SILOPOV'
- Region Name:** '[us-east-1: US East (Northern Virginia)]' (dropdown)
- SNS Body:** A large text area containing the following message template:


```
Severity: %S
First Occurred: %D
Last Occurred: %d
Occurrences: %c
Source: %Z
Organization: %O
Device: %X

Message: %M

Sent by Automation Action: %N

View this event at: %H
```

At the bottom of the form are 'Save' and 'Save As' buttons.

Using the Action Policy in an Automation Policy for AWS SNS

In the **Automation Policy Editor**, create an automation policy that runs the action policy you created for AWS SNS messages.

1. Enter a **Policy Name** that describes this automation.
2. Align the action policy you created with the automation policy in the **Aligned Actions** field.
3. Set the **Repeat Time** to "Every 30 seconds until satisfied" to test the automation.

Automation Policy Editor | Editing Automation Policy [56] Reset

Policy Name: SNSPOV Auto Policy Type: [Active Events] Policy State: [Enabled] Policy Priority: [Default] Organization: [AWS-POV]

Criteria Logic: [Severity >=] [Notice,] [and no time has elapsed] [since the first occurrence,] [and event is NOT cleared] [and all times are valid] Midnight Express

Match Logic: [Text search] Match Syntax: Repeat Time: [Every 30 seconds until satisfied]

Align With: [Devices]

☐ Trigger on Child Rollup ☐ Include events for entities other than devices (organizations, assets, etc.)

Available Devices: AWS-POV
AWS: Account: AIDAJVY6ZLTGAB5JNQ5WS
AWS: Availability Zone - Central: ca-central-1a
AWS: Availability Zone - Central: ca-central-1b

Aligned Devices: (All devices)

Available Events: [3178] Critical: AKCP: AC Voltage sensor detects no cur
[3187] Critical: AKCP: DC Voltage sensor High Critical
[3188] Critical: AKCP: DC Voltage sensor Low Critical
[3177] Critical: AKCP: Dry Contact Sensor Low Critical

Aligned Events: (All events)

Available Actions: SNMP Trap [1]: EM7 Event Trap
SNMP Trap [1]: EM7 Event Trap
SNMP Trap [1]: RBA Base Pack: Send Trap
Create Ticket [2]: RBA Base Pack: Create Ticket

Aligned Actions: 1. Send AWS SNS [8]: RBA Base Pack: SNS Notifi

Save Save As

4. Click **[Save]**.
5. Check your Email inbox for a message received from AWS SNS. You might also need to check your Spam or Junk mailboxes, if you do not receive the message in your inbox within a few minutes.

Check that the event appears in your Events viewer and that the automation policy ran successfully. An example is shown below:

```
2019-03-28 07:35:02
Automation Policy SNSPOV Auto action RBA Base Pack: SNS Notification SILOPOV ran Successfully
Message:Sent AWS SNS:
Severity: CRITICAL
First Occurred: 2019-03-28 04:46:36 UTC
Last Occurred: 2019-03-28 11:32:06 UTC
Occurrences: 82
Source: Dynamic
Organization: AWS-POV
Device: dhcp20.auto.sciencelogic.local
Message: SLCORE01 high frequency is 31779 behind (threshold: 3000)
Sent by Automation Action: RBA Base Pack: SNS Notification SILOPOV
View this event at: http://poc.demo.sciencelogic.com/em7/index.em7?exec=events&q_type=aid&q_arg=95958&q_sev=1&q_sort=0&q_oper=0
Result:{}
```

If the automation policy did not run successfully, you might see something like the following in the event. Troubleshoot as necessary.

```
2019-03-28 07:41:40
Automation Policy POV: Send SNS Message action POV - Send AWS SNS ran Unsuccessfully
Message:Snippet (20) executed with incident: iraceback (most recent call last):
File "/opt/em7/backend/silo_common/automation/exec_snippet.py", line 73, in execute_snippet
File "", line 30, in
File "/opt/em7/lib/python/boto-2.34.0-py2.7.egg/boto/sns/connection.py", line 290, in publish
return self._make_request('Publish', params, '/', 'POST')
File "/opt/em7/lib/python/boto-2.34.0-py2.7.egg/boto/sns/connection.py", line 765, in _make_request
raise self.ResponseError(response.status, response.reason, body)
BotoServerError: BotoServerError: 403 Forbidden
{"Error":{"Code":"AuthorizationError","Message":"User: arn:aws:iam:121940133279:user/SL1-User is not authorized to perform: SNS:Publish on resource: arn:aws:sns:us-east-1:121940133279:POCAlerts","Type":"Sender"},"RequestId":"849bba70-87da-5360-b951-ef6632ee39fd"}
Result:None
```

6.

Creating an Action Policy that Runs an Integration Service Application

The *Integration Service Action Type* PowerPack includes the "Run Integration Service Application" action type. You can use this action type to build an automation action that triggers an Integration Service application. When you create an automation action using this action type, you must specify the credential for the Integration Service instance, the application to run, and the parameters to include in the request.

This automation action does not wait for the Integration Service application to complete. If the Integration Service API responds, the output of the automation action is the JSON response from the API, formatted as a string.

NOTE: This action type is not compatible with the formatting actions in the *Datacenter Automation Utilities* PowerPack.

You can create a new automation action that runs an Integration Service application using the "Run Integration Service Application" action type. To do this, select "Run Integration Service Application" in the Action Type drop-down list when you create a new automation action.

The following figure shows an example of a custom action that uses the "Run Integration Service Application" action type to run IS diagnostics:

The screenshot shows the 'Action Editor' window with the title 'Policy Editor | Editing Action [492]'. The interface includes a 'Reset' button in the top right. The main configuration area contains several fields:

- Action Name:** 'Run IS Diagnostics'
- Action State:** '[Enabled]' (dropdown menu)
- Description:** (empty text field)
- Organization:** '[System]' (dropdown menu)
- Action Type:** 'Run Integration Service Application (1.0)'
- Execution Environment:** '[-- Default Environment]' (dropdown menu)
- Action Run Context:** '[Database]' (dropdown menu)
- Input Parameters:** A large text area containing a JSON object:


```
{
  "credential_id": "162",
  "application_name": "is_system_diagnostics",
  "params": "{}",
  "include_event": false
}
```

At the bottom of the window are 'Save' and 'Save As' buttons.

This action accepts the following parameters in JSON:

Parameter	Input Type	Description
credential_id	integer	The ID of the credential that can be used to connect to the Integration Service API.
include_event	boolean	Controls whether the EM7_VALUES dictionary is included as a parameter in the request to run the Integration Service application.
application_name	string	Contains the name of the application to execute.
params	string	A string representation of a JSON object. This string will be passed as additional parameters to the Integration Service application. This field can contain substitution values that match the keys in EM7_VALUES.

Creating an Action Policy that Sends an HTTP Request

The *HTTP Action Type* PowerPack includes the "Make an HTTP Request" action type. You can use this action type to build an automation action that sends an HTTP request, using a SOAP/XML credential and specific to one or more devices.

You can create a new automation action that sends an HTTP request using the "Make an HTTP Request" action type. To do this, select "Make an HTTP Request" in the Action Type drop-down list when you create a new automation action.

The following figure shows an example of a custom action that uses the "Make an HTTP Request" action type to set the Event Mask to 5 minutes:

The screenshot displays the 'Action Editor' window with the title 'Policy Editor | Editing Action [491]'. The interface includes a 'Reset' button in the top right corner. The main configuration area is divided into several sections:

- Action Name:** 'Set Event Mask to 5 Minutes'
- Action State:** '[Enabled]' (dropdown menu)
- Description:** (empty text field)
- Organization:** '[System]' (dropdown menu)
- Action Type:** 'Make an HTTP Request (1.0)'
- Execution Environment:** '[-- Default: HTTP Action Type]' (dropdown menu)
- Action Run Context:** '[Database]' (dropdown menu)
- Input Parameters:** A JSON object displayed in a text area:

```
{
  "credential_id":161,
  "dynapp_guid":"",
  "relative_url":"/api/device/%x",
  "payload":{"event_suppress_mask\\":\\"00:05:00\\"}"
}
```

At the bottom of the editor, there are 'Save' and 'Save As' buttons.

This action accepts the following parameters in JSON:

Parameter	Input Type	Description
credential_id	integer	The ID of the SOAP/XML credential that will be used to make the request.
dynapp_guid	integer	If the credential_id parameter is set to zero, the dynapp_guid parameter is used. The credential that will be used is the one aligned to the specified Dynamic Application (using the GUID to look up the Dynamic Application) on the device associated with the triggering event.
relative_url	string	Specifies the relative portion of the URL. This string will be appended to the URL from the credential.
payload	string	A string representation of a JSON object. This JSON object will be sent as the body of the HTTP request. This field can contain substitution values that match the keys in EM7_VALUES.

Creating an Action Policy that Uses a Custom Action Type

If your organization has defined Custom Action Types, you can select them when creating an Action Policy.

A **Custom Action Type** executes a reusable snippet. Unlike the Action Type "Snippet", a Custom Action Type can accept input parameters (in a JSON format) and create output (in a JSON format). A Custom Action Type allows a single snippet to be used in multiple Action Policies, each time with different inputs and different outputs.

A Custom Action Type is associated with an Execution Environment. An **execution environment** is an on-demand Python environment that includes the supporting modules, code, scripts, directories, and files (packaged in one or more ScienceLogic Libraries) required by the Custom Action Type. **ScienceLogic Libraries** are packages consisting of metadata and Python files that can be used by the Run Book Actions that use snippets.

In the **Action Policy Editor** page, if you selected a custom action type in the **Action Type** field, you must supply values in the fields, as specified in the section on [Creating an Action Policy](#), and also supply values in the following fields:

The screenshot shows the 'Action Editor' window with the title 'Policy Editor | Creating New Action'. It contains several form fields and buttons:

- Action Name:** A text input field.
- Action State:** A dropdown menu with '[Enabled]' selected.
- Description:** A text input field.
- Organization:** A dropdown menu with '[System]' selected.
- Action Type:** A dropdown menu with 'Timed Action (1.0)' selected.
- Execution Environment:** A dropdown menu with '[-- Default Environment]' selected.
- Action Run Context:** A dropdown menu with 'Database' selected.
- Input Parameters:** A large text area for defining input parameters.
- Buttons:** 'Reset' (top right) and 'Save' (bottom center).

- **Execution Environment.** Specify the execution environment for the Action Policy. If you select "Default", the Action Policy will use the Execution Environment specified in the definition of the Custom Action Type.
- **Action Run Context.** This option is not available on ScienceLogic All-In-One appliances. Specifies whether the action will be executed on the ScienceLogic Database server or on the ScienceLogic Data Collection server. The choices are:
 - *Database.* Execute the action from the ScienceLogic Database Server.
 - *Collector.* Execute the action from the ScienceLogic Data Collection server associated with the device. This is useful when a device doesn't accept connections from the ScienceLogic Database Server or may not be "visible" from the ScienceLogic Database Server.
- **Input Parameters.** Specifies the name and value of the input parameter, in *name:value* format:

```
{ "name_of_parameter": value }
```

Using the Results of a Previous Action

When you define an action policy, you can use the result from an action that was previously triggered by the same automation policy. To do this, you can use one of the following two variables:

- **%_EM7_RESULT_%.** Action Policies can include the variable `%_EM7_RESULT_%` to retrieve the results from the previously executed action policy. The value of the variable is available only to the very next action policy in an automation policy. For example, if an automation policy includes three action policies, the results from

the first action policy are available only to the second action policy. The third action policy cannot access the results of the first action policy.

- **em7_result_list**. This variable allows you to include the results from any Action Policy that was executed by the same Automation Policy. For more information on how to use this variable, see [Using the em7_result_list Variable](#).

You can use these two variables in the following fields:

- In the subject or body of an email message, sent with an action policy of type *Email Notification*.
- To populate an OID contained in an outbound trap, sent with an action policy of type *Send an SNMP Trap*.
- In the **Description** field or in a **Note** in a ticket template. The ticket template must be triggered by an action policy of type *Create a New Ticket*.
- To populate an OID contained in an SNMP Set command. The SNMP Set must be triggered by an action policy of type *Send an SNMP Set*.
- As part of an SQL query, triggered by an action policy of type *Execute an SQL Query*.
- In a ticket note added by an action policy of type *Update an existing ticket*.
- In an SNS Message to a Topic ARN (Amazon Resource Name).

Using the em7_result_list Variable

The variable **em7_result_list** allows you to include the results from a previous Action Policy in the current Action Policy. The value of the variable is available only to other actions in the same automation policy. For example, if an automation policy includes three action policies, you could include the **em7_result_list** variable in the third action policy and retrieve the results from the first action policy and use them in the third action policy. To specify the action policy for which you want to retrieve the results, you include the index number for that action policy. Index numbers start at zero ("0"). The syntax for the **em7_result_list** variable is:

{em7_result_list[i]}

where *i* represents the index number.

For example:

```
{em7_result_list[2]}
```

would display the results of the third action policy.

For all Action Policies except of type *Execute an SQL Query*, **em7_result_list** returns the result of the specified action.

For Action Policies of *Execute an SQL Query*, **em7_result_list** returns:

- returned data, if the query was a SELECT query.
- Row Count.
- Last Row ID (if cursor was used in query).
- Messages (if cursor was used in query).

You can include the **em7_result_list** variable:

- In the subject or body of an email message, sent with an action policy of type *Email Notification*.
- To populate an OID contained in an outbound trap, sent with an action policy of type *Send an SNMP Trap*.
- In the **Description** field or in a **Note** in a ticket template. The ticket template must be triggered by an action policy of type *Create a New Ticket*.
- To populate an OID contained in an SNMP Set command. The SNMP Set must be triggered by an action policy of type *Send an SNMP Set*.
- As part of an SQL query, triggered by an action policy of type *Execute an SQL Query*.
- In a ticket note added by an action policy of type *Update an existing ticket*.
- In an SNS Message to a Topic ARN (Amazon Resource Name).

For example, suppose your Automation Policy included three Action Policies.

- Action Policy "0" is of type *Run a Snippet* and executes a traceroute on the device associated with the triggering event.
- Action Policy "1" is of type *Run a Snippet* and executes a ping on the device associated with the triggering event.
- Action Policy "2" is of type *Create a New Ticket* and will include the results of the previous two action policies. In the ticket template specified in the Create a New Ticket action, you could include the following in the Notes in Attachments section. This data would appear in the newly created ticket:

Results of the traceroute:

```
{em7_result_list[0]}
```

Results of the PING:

```
{em7_result_list[1]}
```

Asset Information:

Make: %W

Model: %w

Tag: %v

Chapter



4

Snippet Actions

Overview

This chapter describes how to create an action policy that executes a snippet, which is a custom-written Python program.

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

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

This chapter covers the following topics:

<i>Creating an Action Policy that Executes a Snippet</i>	89
<i>Writing Snippet Code</i>	91

Creating an Action Policy that Executes a Snippet

In the **Action Policy Editor** page, if you selected the **Action Type** of *Run a Snippet*, the new action policy will execute a custom-written Python program. If the action policy is aligned with an automation policy (i.e., if the action policy is included in the definition of an automation policy), and the criteria in the automation policy are met, SL1 will execute the Snippet.

For increased flexibility and connectivity, you can specify whether the Snippet should be executed by the Database Server or by the Data Collector. In some cases, a device might not accept connections from the Database Server or may not be "visible" from the Database Server. In these situations, you can specify that the Snippet be executed by the Data Collector.

NOTE: For SL1 systems that are using an All-In-One Appliance, you cannot choose to execute a policy on a Database Server or a Data Collector. All policies will be executed on the All-In-One Appliance.

An action policy that executes a Snippet is useful when you want to run detailed network diagnostics on a device. For example, if SL1 generates an event saying that a device is not responding to ping, you could run a Snippet that performs a traceroute and specify that SL1 execute the Snippet from the Data Collector server. You would then execute a traceroute from the Data Collector to the device, store the results in the variable `%_EM7_RESULT_`, and use that variable to pass the results to another action policy.

An action policy that executes a Snippet is useful when you want to perform some automated steps on the device to resolve a problem. For example, when a specific event is triggered, you could run a Snippet that turns on debugging on the remote device and copies the logs to another remote device.

NOTE: Snippets are developed using the Python programming language. To create a Snippet Action Policy, you must be familiar with the programming techniques and data structures of the Python language.

In the **Action Policy Editor** page, if you select the **Action Type** of *Run a Snippet*, you must supply values in the fields specified in [Action Policies](#) and also in the following fields:

The screenshot shows the 'Action Editor' window with the 'Policy Editor | Creating New Action' tab. The form contains the following fields and values:

- Action Name:** (Empty text field)
- Action State:** [Enabled] (Dropdown menu)
- Description:** (Empty text field)
- Organization:** [System] (Dropdown menu)
- Action Type:** Run a Snippet (Dropdown menu)
- Snippet Credential:** (None) (Dropdown menu)
- Action Run Context:** Database (Dropdown menu)
- Execution Environment:** [-- Default Environment] (Dropdown menu)
- Snippet Code:** (Large empty text area)
- Buttons:** Reset (top right), Save (bottom right)

- **Snippet Credential.** Credential that allows SL1 to execute the Snippet code on the external device. Usually, these are credentials of type "Basic". The list of credentials is filtered to include only those credentials to which you have access.

If this field has already been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the list in this field; you will not be able to re-align the device with the *Restricted Credential*.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the **Snippet Credential** field.

- **Action Run Context.** This option is not available on All-In-One Appliances. Specifies whether the action will be executed on the Database Server or on the Data Collector. The Choices are:

- **Database.** Execute the action from the Database Server.
- **Collector.** Execute the action from the Data Collector associated with the device. This is useful when a device doesn't accept connections from the Database Server or may not be "visible" from the Database Server.
- **Execution Environment.** Select the execution environment to which you want to align the action. An execution environment is an on-demand Python environment that contains the supporting modules, code, scripts, directories, and files (packaged in ScienceLogic Libraries) for the snippet. An execution environment includes its own installation directories, doesn't share libraries with other environments, and allows granular control of dependencies, versions, and permissions. The default execution environment is *System*. For more information, see the **ScienceLogic Libraries** manual.
- **Snippet Code.** Python code for the Snippet.

NOTE: If you selected **Code Highlighting** in the **Account Preferences** page (Preferences > Account > Preferences), the code in the **Snippet Code** field appears with syntax highlighting.

Writing Snippet Code

The following sections describe the functions and variables that are available to python code for automation actions of type "snippet".

Snippet Functions

SL1 automatically imports the module **em7_snippets**. This module includes the following functions that you can use within your Snippet code:

- **logger = em7_snippets.logger(filename = 'pathname for log file')**

This function opens a log file to which your snippet can write messages. For example:

```
logger=em7_snippets.logger(filename='/tmp/mylog')
```

Your snippet code can write messages to the log file using the syntax:

```
logger.debug ("message")
```

- **em7_snippets.generate_alert(message, xid, xtype, yid, ytype, yname, value, threshold).**

This function allows you to generate an alert from a Snippet action policy. You can define an event based on the alert; the event must have a **Source** of *API* and use pattern matching to match the alert. The arguments for the function are:

- **message.** Required argument. The message text for the alert.

- **xid**. Required argument. The entity to associate with the alert. Supply the numeric ID of an entity. For example, if you supply '1' in the **xtype** argument, supply a device ID in this argument.
- **xtype**. Specifies the type of ScienceLogic element associated with the alert. Supply one of the following integer values:
 - 0. Organization
 - 1. Device
 - 2. Asset
 - 4. Network
 - 5. Interface
 - 6. Vendor
 - 7. User Account
 - 8. Virtual Interface
 - 9. Device Group
 - 10. IT Service
 - 11. Ticket
- **yid** = *value*. The sub-entity to associate with the alert. Supply the numeric ID of a sub-entity. For example, if you supply '3' in the **ytype** argument, supply a file system ID in this argument.
- **ytype** = *value*. Optional argument. The type of sub-entity for which you specified an ID in the **yid** argument. Supply one of the following integer values:
 - 9. News Feed (if **xtype** is 0) or Process (if **xtype** is 1).
 - 1. CPU. Can be specified only if **xtype** is 1 (Device).
 - 2. Disk. Can be specified only if **xtype** is 1 (Device).
 - 3. File System. Can be specified only if **xtype** is 1 (Device).
 - 4. Memory. Can be specified only if **xtype** is 1 (Device).
 - 5. Swap. Can be specified only if **xtype** is 1 (Device).
 - 6. Hardware Component. Can be specified only if **xtype** is 1 (Device).
 - 7. Interface. Can be specified only if **xtype** is 1 (Device).
 - 10. Port. Can be specified only if **xtype** is 1 (Device).
 - 11. Windows Service. Can be specified only if **xtype** is 1 (Device).
 - 12. Web Content. Can be specified only if **xtype** is 1 (Device).
 - 13. Email Monitor. Can be specified only if **xtype** is 1 (Device).
- **yname** = *value*. Optional argument. The name of the sub-entity for which you specified an ID in the **yid** argument.

- **value**= *string*. Optional argument. A value that will be passed with the alert message. This value is available in the %V substitution character for event policies.
- **threshold**= *string*. Optional argument. A threshold value that will be passed with the alert message. This threshold value is available in the %T substitution character for event policies.

For example:

```
em7_snippets.generate_alert('Attempted File System Cleanup', '60', '1', '150',  
'3')
```

will generate an alert with the message "Attempted File System Cleanup" associated with the file system with ID 150 on the device with ID 60.

Snippet Variables

A Snippet can use the following global Snippet variables:

- **EM7_LAST_RESULT**. Variable that contains the results from the previous Action Policy.
- **EM7_RESULT**. Variable in which to store the results from the current Snippet Action Policy. This variable is used to populate the variable `%_EM7_RESULT_`.
- A Snippet can access the standard replacement variables (described in the appendix on [Variables](#)) by using the global dictionary **EM7_VALUES**. The syntax is:

```
EM7_VALUES['variable']
```

For example, to access the variable that contains a device's IP address:

```
EM7_VALUES['%a']
```

- **EM7_ACTION_CRED**. Variable that contains a [dictionary of values](#) from the credential for this action policy, specified in the **Snippet Credential** field.
- **EM7_DEVICE_CRED**. Variable that contains a [dictionary of values](#) from the credential used to discover the device where the event occurred (that is, the event specified in the automation policy that triggered the current action policy). If the triggering event is not aligned with a device, this variable does not contain a value.
- **EM7_DYNAMIC_APP_CREDS[Dynamic_Application's_ID]**. Variable that returns a [dictionary of values](#) from the credential associated with the specified Dynamic Application on the device (where the triggering event occurred). The syntax is:

```
EM7_DYNAMIC_APP_CREDS['Dynamic_Application's_ID']
```

For example, to access the dictionary of values for the credential assigned to the Dynamic Application with the ID of "61", you would enter:

```
EM7_DYNAMIC_APP_CREDS['61']
```

This would return the dictionary of values for the credential that allows the Dynamic Application with an ID of "61" to run for the device where the triggering event occurred.

A returned value can be used in a Run Book Automation snippet to set a value. For example, the following statement will set the value in the key "cred_user" to variable "user" within the snippet:

```
user = EM7_DYNAMIC_APP_CREDS['Dynamic_Application's_ID']["cred_user"]
```

Credential Dictionary Structure

Several elements in the credential dictionary are common to all credential types, and each credential type (other than Basic/Snippet) has unique elements that appear only in the credential dictionary for that credential type. The following elements are common to every type of credential dictionary:

- **cred_id**. Integer. Unique credential ID.
- **cred_type**. Integer. Type of credential .
 - 1 SNMP
 - 2 DB
 - 3 HTTP/XML
 - 4 LDAP
- **cred_host**. String. Host name or IP address (%D substitution string).
- **cred_port**. Integer. TCP/IP port for connections.
- **cred_pwd**. String. Password (encrypted in the database, stored as clear text in the dictionary).
- **cred_user**. String. Username.
- **cred_timeout**. Integer. Timeout in milliseconds.

The following elements are unique for SNMP credentials:

- **snmp_version**. Integer. SNMP version, values 1, 2, 3.
- **snmp_ro_community**. String. Read-only community string.
- **snmp_rw_community**. String. Read/Write community string.
- **snmp_retries**. Integer. Number of retries.
- **snmpv3_auth_proto**. String. V3 auth. protocol,. Can be either MD5 or SHA.
- **snmpv3_sec_level**. String. V3 security. Can be noAuthNoPriv, AuthNoPriv, or AuthPriv.
- **snmpv3_priv_proto**. String. V3 privacy protocol. Can be : DES or AES.
- **snmpv3_priv_pwd**. String. V3 password encrypted in the database and stored as clear text in the dictionary.
- **snmpv3_context**. String. V3 context.

The following elements are unique for Database credentials:

- **db_type**. Integer.
 - 1 MySQL
 - 2 MSSQL
 - 3 Oracle
 - 4 Postgress
 - 5 DB2
 - 6 Sybase
 - 7 Informix
 - 8 Ingress).

- **db_name**. String. Initial database name.
- **db_sid**. String. Database SID (Oracle only).
- **db_connect**. String. Database connect string (Oracle only).

The following elements are unique for SOAP/XML credentials:

- **curl_url**. String. URL.
- **curl_proxy_ip**. String. Proxy server IP address.
- **curl_proxy_port**. Integer. Proxy server TCP/IP port.
- **curl_proxy_acct**. String. Proxy server account.
- **curl_proxy_passwd**. String. Proxy server password.
- **curl_encoding**. String. Encoding method (eg text/xml).
- **curl_post_or_get**. Integer. HTTP method 0 – GET, 1 - POST.
- **curl_http_version**. HTTP version: 10 = 1.0, 11 = 1.1.
- **curl_request_sub_1**. String. Substitution value to substitute into Snippet code.
- **curl_request_sub_2**. String. Substitution value to substitute into Snippet code.
- **curl_request_sub_3**. String. Substitution value to substitute into Snippet code.
- **curl_request_sub_4**. String. Substitution value to substitute into Snippet code.
- **curl_headers**. List of Strings. Each string is a HTTP key/value pair.
- **curl_opts**. Dictionary of Curl options comprising a series of pairs of string key and corresponding string value.

Using the Results of Previous Actions

The variable **EM7_LAST_RESULT_LIST** allows you to use the results from a previous Action Policy in the current Action Policy. The results of an action are available only to other actions in the same automation policy. For example, if an automation policy includes three action policies, you could pass the results from the first action policy to the third action policy. To specify the action policy for which you want to retrieve the results, you include the index number for that action policy. Index numbers start at zero ("0").

Each index in the **EM7_LAST_RESULT_LIST** variable is a list object with the following structure:

```
('success', 'type', 'result', 'metrics', 'message')
```

Where:

- **success**. Contains "True" if the specified Action Policy was successful and "False" if the specified Action Policy was not successful. To assign this value to a local variable, the syntax is:

```
success = EM7_LAST_RESULT_LIST[i].success
```

where *success* is the variable in which to store the returned value and *i* is the index number for the Action Policy, for example "1" for the second Action Policy.

- **type.** Numeric ID for the action type. Possible values are:

- 0. Send An Email Notification
- 1. Send an SNMP Trap
- 2. Create a New Ticket
- 3. Send an SNMP Set
- 5. Run a Snippet
- 6. Execute an SQL Query
- 7. Update an Existing Ticket

To assign this value to a local variable, the syntax is:

```
type = EM7_LAST_RESULT_LIST[i].type
```

where *type* is the variable in which to store the returned value and *i* is index number for the Action Policy, for example "1" for the second Action Policy.

- **result.** Returns the result of the specified Action Policy and is usually a Python **dict** object. To assign this value to a local variable, the syntax is:

```
result = EM7_LAST_RESULT_LIST[i].result
```

where *result* is the variable in which to store the returned value and *i* is the index number for the Action Policy, for example "1" for the second Action Policy.

- **metrics.** Returns metrics about the specified Action Policy.

- If the specified Action Policy is not of type "Run a Snippet", this value will be NONE.
- If the specified Action Policy is of type "Run a Snippet", this value contains the following list structure:

```
('start_time', 'end_time', 'duration', 'mem', 'cpu_sys', 'cpu_user')
```

To assign this value to a local variable, the syntax is:

```
metrics = EM7_LAST_RESULT_LIST[i].metrics.end_time
```

where *metrics* is the variable in which to store the returned value and *i* is the index number for the Action Policy, for example "1" for the second Action Policy.

This syntax returns the "end_time" metric. To view another metric, substitute its name for "end_time". The name of each metric is listed above, in the description of the data structure.

- **message.** An informational message. If the success parameter returns False, this parameter returns the error message. To assign this value to a local variable, the syntax is:

```
message = EM7_LAST_RESULT_LIST[i].message
```

where *message* is the variable in which to store the returned value and *i* is the index number for the Action Policy, for example "1" for the second Action Policy.

For example, suppose we included the following Snippet code in an action of type "Run a Snippet". Suppose our current Action (the one that includes the code) is the fourth action in the Automation Policy. Suppose we want to gather information about the third action (which has an index of "2"). Suppose the third action created a new ticket. Suppose the snippet included the following local variable assignment statements:

```
success = EM7_LAST_RESULT_LIST[2].success  
  
type = EM7_LAST_RESULT_LIST[2].type  
  
result = EM7_LAST_RESULT_LIST[2].result  
  
metrics = EM7_LAST_RESULT_LIST[2].metrics  
  
message = EM7_LAST_RESULT_LIST[2].message
```

The contents of the local variables might be:

```
success: true  
  
type: 2  
  
result: {'tid': 814}  
  
metrics: metrics is None  
  
message: Created ticket 814
```

Chapter



5

Examples

Overview

This chapter contains examples of Run Book Automations that you can use as templates for your own automations.

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

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

This chapter covers the following topics:

<i>Action Policy that Sends an Email Message</i>	100
<i>Action Policy that Sends an SNMP Trap to an External Server</i>	102
<i>Action Policy that Creates a Ticket</i>	105
<i>Action Policy that Writes an SNMP Value to an External Server</i>	110
<i>Action Policy that Sends an SQL Query to an External Server</i>	110
<i>Action Policy that Executes a Snippet and Triggers a New Alert</i>	113
<i>Action Policy that Executes a Snippet and Sends the Results to a Second Action Policy</i>	116

Action Policy that Sends an Email Message

Automation Policy

For this example, our example automation policy might look like this:

The screenshot shows the 'Automation Policy Editor | Creating New Automation Policy' interface. The policy is named 'cisco_config_email'. It is configured with the following settings:

- Policy Name:** cisco_config_email
- Policy Type:** [Active Events]
- Policy State:** [Enabled]
- Policy Priority:** [Default]
- Organization:** System
- Criteria Logic:** [Severity >=] Notice, and no time has elapsed, [since the first occurrence,], [and event is NOT cleared], and all times are valid, Hourly Schedule
- Match Logic:** [Text search]
- Match Syntax:** (empty)
- Repeat Time:** [Only once]
- Align With:** [Devices]
- Trigger on Child Rollup:** (unchecked)
- Include events for entities other than devices (organizations, assets, etc.):** (unchecked)

The interface also shows three lists of available items and their aligned counterparts:

- Available Devices:** East Coast, ScienceLogic, Inc.: EM7 All-In-One: gmstack02, System, Cisco Systems: 7609S: 7609S-NPE3.cisco.com, Cisco Systems: CUCM Server: CUCM10-01.qa.sciencelogic.local, ScienceLogic, Inc.: EM7 Admin Portal: sebi-ap-15
- Aligned Devices:** (All devices)
- Available Events:** CPU has, [1851] Minor: Dell PowerConnect: CPU has exceeded threshold, [470] Minor: Enterasys: CPU has exceeded threshold, [1993] Minor: Fortinet: CPU has exceeded threshold, [77] Minor: Foundry: CPU has exceeded threshold, [478] Minor: Host Resource: CPU has exceeded threshold, [3349] Minor: HP Procurve: CPU has exceeded threshold
- Aligned Events:** [2238] Minor: Cisco: CPU has exceeded threshold
- Available Actions:** Send Email [0]: Send Email Automation Runbook Test, Send Email [0]: Send Email Automation Runbook Test, SNMP Trap [1]: EM7 Event Trap, Snippet [5]: AWS: Disable Instance By Tag, Snippet [5]: AWS: Discover from EC2 IP, Snippet [5]: AWS: Get EC2 Instance Configuration
- Aligned Actions:** 1. Send Email [0]: Send Email Automation Runbook Test

A 'Save' button is located at the bottom right of the form.

- We specified that the automation policy:
 - Should act upon active events.
 - Is enabled.
 - Is associated with the organization "System".
 - Will be triggered when the specified event has a severity equal to or greater than "Notice".

- Will be triggered as soon as the specified event occurs.
 - The policy will trigger the action only once for each instance of the event.
 - Will be triggered at any time.
 - Will be triggered when the selected event occurs on at least one of the selected Cisco devices.
 - Will be triggered when the event "Cisco: CPU has exceeded threshold" occurs on at least one of the selected Cisco devices.
- We specified that when all the criteria in the automation policy are met, the action policy "automatic_email" will be executed.

Action Policy

The action policy called "automatic_email" looks like this:

The screenshot shows the 'Action Editor' window with the title bar 'Action Editor' and a close button. The main content area is titled 'Policy Editor | Action Added | Editing Action [19]' and includes a 'Reset' button. The configuration is as follows:

- Action Name:** automatic_email
- Action State:** [Enabled]
- Description:** Email Message Policy
- Organization:** [System]
- Action Type:** Send an Email Notification
- Email Subject:** %S Event: %M
- Email Priority:** [Normal]
- Send as Plain Text:** ☐
- Email Body:**

```
Severity: %S
First Occurred: %D
Last Occurred: %d
Occurrences: %c
Source: %Z
Organization: %O
Device: %Y
```
- Available Emails:**
 - banderton: banderton@sciencelogic.com
 - bleylard: bleyland@sciencelogic.com
 - em7admin: admin@sciencelogic.com
 - ttesterson: ttesterson@sciencelogic.com
 - [Monteith, Bill]: bmonteith@mail.com
- Assigned Emails:**
 - charmander: char@mander.com

At the bottom, there are 'Save' and 'Save As' buttons.

- We specified that this action policy:
 - Is enabled.
 - Will act upon events and devices aligned with the System organization.
 - Will send an email notification in response to an automation policy.
 - Will include the default Email Subject and Email Body.
 - Will label email messages with Normal priority.
 - Will send an email message to cha@rmande.com.

Sent Email

Suppose the criteria in our automation policy "cisco_config_email" was met and that the trigger event "Cisco: CPU has exceeded threshold" occurred on the device "CustB_2821-1.cisco.com".

Suppose our action policy "automatic_email" was successfully triggered and executed.

Our action policy will build and send an email message like this:

From: EM7 Event Notifier
 Date: Wednesday, January 20, 2010 8:13 AM
 Subject: MINOR Event: Configuration management trap received

Date: Wed, 20 Jan 2010 13:12:07 +0000

System Event [16285]
 Severity: MINOR
 Device/Context: CustB_2821-1.cisco.com
 Message: CPU has exceeded threshold
 First Occurred: 2010-01-15 22:13:13
 Last Occurred: 2010-01-20 13:08:20

Impacted:

Cause and Resolution:

View this event at:

Action Policy that Sends an SNMP Trap to an External Server

Suppose SL1 must integrate with an existing network management system. To do this, SL1 must forward certain event information to the existing network management server. SL1 could use an SNMP trap to forward event information to another network management server. In this example, we'll use this scenario and send information about each instance of the event "Cisco: CPU has exceeded threshold".

Automation Policy

In this example, we'll use a modified version of the Automation Policy we described in [Automation Policies](#).

The screenshot shows the 'Automation Policy Editor' window with the title 'Automation Policy Editor | Policy Added | Editing Automation Policy [35]'. The interface is divided into several sections:

- Policy Metadata:** Policy Name: 'cisco_config_send_trap', Policy Type: '[Active Events]', Policy State: '[Enabled]', Policy Priority: '[Default]', Organization: '[System]'. There is a 'Reset' button in the top right.
- Criteria Logic:** A series of dropdown menus: '[Severity >=]', '[Healthy]', '[and no time has elapsed]', '[since the first occurrence,]', '[and event is NOT cleared]', '[and all times are valid]'. There is also a 'Trigger on Child Rollup' checkbox.
- Match Logic:** '[Text search]' dropdown and an empty text input field.
- Match Syntax:** Empty text input field.
- Repeat Time:** '[Only once]' dropdown.
- Align With:** '[Devices]' dropdown.
- Include events for entities other than devices (organizations, assets, etc.):** An unchecked checkbox.
- Available Devices:** A list box containing 'System', 'Microsoft: Azure Services: Azure Device', 'ScienceLogic: Integration Service: Integration Service Docs', 'ScienceLogic, Inc.: EM7 All-In-One: em7ao', and 'ScienceLogic, Inc.: EM7 All-In-One: em7ao'. There are '»' and '«' buttons next to it.
- Aligned Devices:** A list box containing '(All devices)'.
- Available Events:** A list box containing 'configman', '[3118] Critical: Cisco: Configuration (CE Series) Interface Spee', '[2844] Major: Polycom: DMA: Configuration Manager: No Territ', and '[2148] Minor: Cisco: CPU has exceeded threshold'. There are '»' and '«' buttons next to it.
- Aligned Events:** A list box containing '[2028] Notice: Cisco: ConfigManEvent'.
- Available Actions:** A list box containing 'Send Email [0]: Send Email Automation Runbook Test', 'SNMP Trap [1]: EM7 Event Trap', 'Snippet [5]: AWS: Disable Instance By Tag', 'Snippet [5]: AWS: Discover from EC2 IP', and 'Snippet [5]: AWS: Get EC2 Instance Configuration'. There are '»' and '«' buttons next to it.
- Aligned Actions:** A list box containing '1. SNMP Trap [1]: EM7 Event Trap'. There are '↑' and '↓' buttons next to it.
- Buttons:** 'Save' and 'Save As' buttons at the bottom.

- We specified that the automation policy:
 - Should act upon active events.
 - Is enabled.
 - Is associated with the organization "System".
 - Will be triggered when the specified event has a severity greater than "Healthy".
 - Will be triggered as soon as the specified event occurs.
 - The policy will trigger the action only once.
 - Will be triggered at any time.
 - Will be triggered when the selected event occurs on at least one of the selected Cisco devices.

- Will be triggered when the event "Cisco: ConfigManEvent" occurs on at least one of the selected Cisco devices.
- We specified that when all the criteria in the automation policy are met, the action policy "send_event_trap" will be executed.

Action Policy

The action policy called "send_event_trap" looks like this:

- We specified that this action policy:
 - Is enabled.
 - Will act upon events and devices aligned with the System organization.
 - Will send an SNMP trap in response to an automation policy.
 - Will send the trap to the trap host at 192.168.30.30.
 - Will use the credential "EM7 Default V2" to send the trap to the trap host at 192.168.30.30.
 - Will send an **event type-based trap**, using the OID .1.3.6.1.4.1.19567.2.1.0.2.1.event_policy_ID. We use the variable %3, so that EM7 will append the current event's policy ID to the trap OID. (The current event will be the event that triggered the action policy. This event is specified in the automation policy.)
 - Includes all the **EM7 varbinds** in the trap.

Sent Trap

Suppose the criteria in our automation policy "cisco_config_send_trap" was met and that the trigger event "Cisco: ConfigManEvent" occurred on the device "CustB_2821-1.cisco.com".

Suppose our action policy "send_event_trap" was successfully triggered and executed.

Our action policy will build and send an event trap like this:

```
Trap Received: (.1.3.6.1.4.1.19567.2.1.0.2.1.403) | Trap Detail : eventID: 12500;
eventSeverity: 2; eventSource: 3; elementType: 1; elementID: 48; elementName: CustB_
2821-1.cisco.com; elementAddress: 10.20.30.43; roaID: 0; roaName: System;
eventMessage: Configuration management trap received; subElementType: 0;
subElementID;; subElementName;;
```

Action Policy that Creates a Ticket

Suppose we want to automatically create a ticket in response to a specific set of event conditions. We will use a modified version of the automation policy used in the examples above. Suppose that each time an event occurs, we immediately want to create a high priority ticket that specifies the emergency actions that must be performed. In this example, we'll automatically create a ticket about each instance of the event "Critical: APC: UPS Battery Capacity".

Automation Policy

In this example, we'll use a modified version of the Automation Policy we described in [Automation Policies](#).

Automation Policy Editor | Creating New Automation Policy

Reset

Policy Name

battery_capacity_create_ticket

Policy Type

[Active Events]

Policy State

[Enabled]

Policy Priority

[Default]

Organization

System

Criteria Logic

[Severity >=]

Major,

and no time has elapsed

[since the first occurrence,]

[and event is NOT cleared]

and all times are valid

Hourly Schedule

Match Logic

[Text search]

Match Syntax

Repeat Time

[Only once]

Align With

[Devices]

☐ Trigger on Child Rollup

☐ Include events for entities other than devices (organizations, assets, etc.)

Available Devices

cisc

East Coast

West Coast

Aligned Devices

System

Cisco Systems: 7609S: 7609S-NPE3.cisco.com

Cisco Systems: CUCM Server: CUCM10-01.qa.sciencelogic.local

Available Events

battery ca

Aligned Events

[1729] Critical: APC: UPS Battery Capacity

Available Actions

Send Email [0]: Send Email Automation Runbook Test

Send Email [0]: Send Email Automation Runbook Test

SNMP Trap [1]: EM7 Event Trap

Create Ticket [2]: Create a Ticket

Snippet [5]: AWS: Disable Instance By Tag

Snippet [5]: AWS: Discover from EC2 IP

Aligned Actions

1. Create Ticket [2]: Create a Ticket

Save

- We specified that the automation policy:
 - Should act upon active events.
 - Is enabled.
 - Is associated with the organization "System".
 - Will be triggered when the specified event has a severity equal to or greater than "Major".
 - Will be triggered as soon as the specified event occurs.
 - The policy will trigger the action only once for each instance of the event.
 - Will be triggered at any time.
 - Will be triggered when the selected event occurs on the selected device.
 - Will be triggered when the event "Critical: APC: UPS Battery Capacity" occurs on the selected device.
- We specified that when all the criteria in the automation policy are met, the action policy "create_ticket" will be executed.

Action Policy

The action policy called "create_ticket" looks like this:

The screenshot shows the 'Action Editor' window with a red title bar. Inside, the 'Policy Editor | Editing Action [77]' tab is active. The form contains the following fields:

- Action Name:** create_ticket
- Action State:** [Enabled] (dropdown menu)
- Description:** (empty text field)
- Organization:** [System] (dropdown menu)
- Action Type:** Create a New Ticket
- Ticket Template:** [Rollback Configuration on Device %X] (dropdown menu)

At the bottom of the form are two buttons: 'Save' and 'Save As'. A 'Reset' button is located in the top right corner of the editor area.

- We specified that this action policy:
 - Is enabled.
 - Will act upon events and devices aligned with the System organization.
 - Will create a new ticket in response to an automation policy.
 - Will use the ticket template "Rollback Configuration on Device %X" to create the ticket.

Ticket Template

The Ticket Template "Rollback Configuration on Device %X" looks like this:

The screenshot displays the 'Template Editor' interface for creating or editing a ticket template. The top navigation bar includes 'Template Editor | Created template | Editing Template [1] | Click Save to' followed by buttons for 'Actions', 'New', 'Reset', and 'Guide'. The 'Properties' section on the left shows the 'Description' as 'Rollback Configuration on Device %x', 'Organization' as '[System]', and 'Element' as 'System'. The 'Ticket Properties' section contains fields for 'Template Name', 'Ticket Description', 'Ticket State', 'Severity' (set to '[Sev 3 / Minor]'), 'Category' (set to 'Abuse'), 'Source' (set to '[Automated]'), 'Queue' (set to '[Change Management]'), and 'Assigned User' (set to '[em7admin]'). Below these fields is a rich text editor with a toolbar containing icons for bold, italic, underline, strikethrough, text color, background color, bulleted list, numbered list, link, unlink, image, and code. The text area contains the following content: 'Someone of some event altered the configuration on this device. Roll back configuration to test-known-good.', 'Event occurred on device %X.', and 'See detail of event at \$H.'. At the bottom of the editor are 'Save' and 'Save As' buttons.

- We specified that the ticket template :
 - Will create a ticket that includes the name of the affected device in the description.
 - Will create a ticket that is associated with the organization "System".
 - Will create a ticket that has a severity of "Minor".
 - Will create a ticket that will be placed in the "Monitoring" ticket queue.
 - Will create a ticket that will be assigned to the user "em7admin".
 - Will create a ticket that will have a category of "Abuse".

- Will create a ticket that will have a source of "Automation".
- Will appear as a choice in action policies.
- Will be triggered as soon as the specified event occurs.
- Will create a ticket that includes note text that reads:

Someone or some event altered the configuration on this device. Roll back configuration to last-known-good.
 Event occurred on device *device_name*.
 See detail of event at *link for event*.

Resulting Ticket

Suppose that the trigger event "UPS Battery Capacity has Degraded Below Threshold" occurred on the device "10.20.30.76".

Our action policy will build a ticket like this:

Ticket Editor | Created ticket | Active Ticket [226]

Actions
New
Reset
Guide

Properties
Logs
Automation
Message
Custom
Test By Lak

Description
Rollback Configuration on Device 10.20.30.76
Ticket Age
1 sec

Organization
[System]
[ScienceLogic Support | support@sciencelogic.com | (703)-354-1010 | ID: 0]
Created On/By
2013-04-26 11:40:33 | em7admin

Element
System
Modified Age
1 sec

Modified On/By
2013-04-26 11:40:33 | em7admin

Ticket Properties

Ticket Description
Rollback Configuration on Device 10.20.30.76
Sub-Organization
[None]
Ticket State
[Test]
Status
[Open]

Severity
[Sev 3 / Minor]
Category
[Abuse]
Source
[Automated]
Queue
[Asset Management]
Assigned User
[em7admin]

Notes & Attachments

Maximize
Descending
New Note

#1) Date [2013-04-26 11:40:33] | User [em7admin] | Address [192.168.35.25] | Cloak [Enabled]
Someone or some event altered the configuration on this device. Roll back configuration to last-known-good.

Event occurred on device 10.20.30.76.

See detail of event at http://em7.mydomain.com/em7/index.em7?exec=events&q_type=aid&q_arg=23361&q_sev=1&q_sort=0&q_oper=0.

Save
Resolve

Action Policy that Writes an SNMP Value to an External Server

You can create an action policy that writes an SNMP value (using the SNMP Set command). You might want to use this type of action policy to perform the following types of tasks:

- **Change the value of an OID in response to an event.** For example, we could use a Dynamic Application to create an alert. That alert could examine an OID for a specific value (for example, an OID that specifies whether a device will send traps or not). If the OID did **not** have a specific value, we could trigger an event. We could create an automation policy that looked for occurrences of the new event. We could define an action policy that performs an SNMPSet and writes the desired value to the OID (for example, assigns a value that allows the device to send traps). When the new event occurred, we could change the value of the OID.
- **Trigger a script on an external device.** When a specified event occurs (for example, an event that informs us that a network device is not running), we could trigger an automation policy. This automation policy could trigger an action policy that performs an SNMPSet. We could change the value of an OID on the affected external device. The external device must include a script that is also monitoring the value of the changed OID. The script could be triggered when the OID changes. For example, the script might restart the device.

Action Policy that Sends an SQL Query to an External Server

Suppose you want to create a custom Quick Report that displays the number of automation policies that are executed and the date and time each execute occurs. However, by default, SL1 does not log this information to the system logs or access logs.

To solve this problem, you could create an SQL action that automatically creates a log entry in the audit logs in the database each time an automation policy is executed. You could then include this action in each automation policy, so that SL1 automatically creates a log entry in the database each time an automation policy is executed.

You could later write a custom Quick Report to retrieve, format, and display the log entries from the database.

Automation Policy

For our example, we'll use a modification of the previous automation policy that sends an email ("cisco_config_email"). Our modification will include an email action and also include an action that use SQL to log the instance of the email action.

The screenshot shows the 'Automation Policy Editor' interface. The title bar reads 'Automation Policy Editor | Policy Added | Editing Automation Policy [23]' with a 'Reset' button on the right. The form is divided into several sections:

- Policy Metadata:** Policy Name: 'cisco_config_email_and_log'; Policy Type: '[Active Events]'; Policy State: '[Enabled]'; Policy Priority: '[Default]'; Organization: '[System]'.
- Criteria Logic:** A series of dropdowns: '[Severity >=]', '[Notice,]', '[and 5 minutes has elapsed]', '[since the first occurrence,]', '[and event is NOT cleared]', '[and all times are valid]', and 'Hourly Schedule'.
- Match Logic:** '[Text search]'.
- Match Syntax:** An empty text field.
- Repeat Time:** '[Only once]'.
- Align With:** '[Devices]'.
- Include events for entities other than devices (organizations, assets, etc.):** An unchecked checkbox.
- Trigger on Child Rollup:** An unchecked checkbox.
- Available Devices:** A list with 'East Coast' and 'System' highlighted. Below are 'ScienceLogic, Inc.: EM7 All-In-One: gmstack02' and 'ScienceLogic, Inc.: EM7 Admin Portal: sebi-ap-15'.
- Aligned Devices:** A list containing 'System', 'Cisco Systems: 7609S: 7609S-NPE3.cisco.com', and 'Cisco Systems: CUCM Server: CUCM10-01.qa.sciencelogi'.
- Available Events:** A list with '[3288] Critical: AKCP: Smoke Detector Alert!', '[3286] Critical: AKCP: Water Sensor has detected water', '[1741] Critical: APC: Diagnostic Test Failed', and '[1729] Critical: APC: UPS Battery Capacity'.
- Aligned Events:** A list containing '[2238] Minor: Cisco: CPU has exceeded threshold'.
- Available Actions:** A list with 'sq' and 'SQL Query [6]: SQL Query: Log Entry'.
- Aligned Actions:** A list containing '1. Send Email [0]: Send Email Automation Runbook T' and '2. SQL Query [6]: SQL Query: Log Entry'.

At the bottom, there are 'Save' and 'Save As' buttons.

- We specified that the automation policy:
 - Should act upon active events.
 - Is enabled.
 - Is associated with the organization "System".
 - Will be triggered when the specified event has a severity equal to or greater than "Notice".
 - Will be triggered as soon as the specified event occurs.

- The policy will trigger the action only once for each instance of the event.
- Will be triggered at any time.
- Will be triggered when the selected event occurs on at least one of the selected Cisco devices.
- Will be triggered when the event "Cisco: CPU has exceeded threshold" occurs on at least one of the selected Cisco devices.
- We specified that when all the criteria in the automation policy are met, the action policy "automatic_email" will be executed.
- We specified that when all the criteria in the automation policy are met, the action policy "sql_log_entry" will be executed.

Action Policy

The action policy called "sql_log_entry" looks like this:

The screenshot shows the 'Policy Editor | Creating New Action' window. It contains the following fields and values:

- Action Name:** sql_log_entry
- Action State:** [Enabled]
- Description:** SQL Query Policy
- Organization:** [System]
- Action Type:** Execute an SQL Query
- Database Credential:** EM7 Collector Database
- Action Run Context:** Database
- SQL Query:**

```
INSERT INTO master_biz.organizations_log (roa.id, date_edit, source, message)
VALUES ("0", NOW(), "automation engine", "automation engine executed Run Book
automation policy and action policy")
```

A 'Save' button is located at the bottom of the form.

- We specified that this action policy:
 - is enabled.
 - will act upon events and devices aligned with the System organization.
 - will execute an SQL query.
 - will use the credential "MySQLWrite" to connect to the database.
 - will add a new row of data to the table organizations_log in the database master_biz, using following MySQL INSERT command:


```
INSERT INTO master_biz.organizations_log
(roa.id, date_edit, source, message)
VALUES ("0", NOW(), "automation engine", "automation engine executed Run Book
automation policy and action policy")
```

Action Policy that Executes a Snippet and Triggers a New Alert

SL1 includes a sample action policy that executes a Snippet. This example Snippet pings a device, stores the results in a variable, and makes an entry in a ScienceLogic database table. SL1 will check the entries in this database table and try to match the messages to an existing event policy.

NOTE: To use this example action policy to trigger an event, you must define an event policy with an **Event Source** of **API** and a **First Match String** value that will match against the value in the **Message** column in the database **in_api**, in the table **messages**. When a new entry is made to the database **in_api**, in the table **messages**, this triggers SL1 to check the value in the **Message** column against any existing event policies.

The code for the Snippet looks like this (line numbers were added for easy reference and are not included in the code):

```
1) import MySQLdb
2) import subprocess
3) CDB_IP = '192.168.9.90'
4) out, err = subprocess.Popen(['ping', '-c 5', EM7_VALUES['%a']],
stdout=subprocess.PIPE, stderr=subprocess.PIPE).communicate()
5) EM7_RESULT = out
6) if ' 0% packet loss' not in out:
7) conn = MySQLdb.connect(user='root', passwd='em7admin', host=CDB_IP, port=7706)
8) cur = conn.cursor()
9) cur.execute("""INSERT INTO `in_api`.`messages` (`xtype`, `xid`, `message`,
`value`, `message_time`) VALUES (%s, %s, %s, '', NOW())""", (EM7_VALUES['%1'], EM7_
VALUES['%x'], 'Bad connection to %s' % EM7_VALUES['%a']))
10) cur.execute("""COMMIT""")
```

The code performs the following:

- Line 1. Tells the code to use the code in the MySQLdb module. This module allows the code to connect to a MySQL database and execute SQL commands.
- Line 2. Tells the code to use the subprocess module to spawn processes, access stdin and stout for those processes, and retrieve return codes for those processes.
- Line 3. Defines the variable CDB_IP, the IP address of the Database Server (to use this example, supply the IP address of the Database Server in your network).
- Line 4. Uses the subprocess module to run the ping command.
 - Notice that the argument for the ping command is EM7_VALUES[%a]. EM7_VALUES is the global dict that allows a Snippet to access the substitution variables. The substitution variable %a contains the IP address for the device where the event occurred.
 - Notice that the results are stored in the variable **out**.
- Line 5. Stores the value of the variable **out** in the global Snippet variable **EM7_RESULT**. The global Snippet variable EM7_RESULT is used to populate the variable %_EM7_RESULT_%. The value of the variable %_EM7_RESULT_% can be accessed by the next Action Policy.
- Line 6. Defines the criteria for triggering a new event. The code says "If the variable **out** does not contain the value '0% packet loss' perform the following lines of code. If the variable **out** does contain the value '0% packet loss' do not perform the following lines of code."

NOTE: The following lines will enter a row into the database **in_api**, in the table **messages**. This table allows external APIs to trigger an event. When a new entry is made in this database table, it triggers SL1 to try to match the value in the **Message** column with an existing event policy.

- Line 7. Uses the MySQLdb module and the **connect** method to connect to the Database. The connect method passes the user ID, password, IP address of the Database Server, and the port to use to connect to the database.

TIP: In the **connect** method, use the same username and password you would use to connect to the Database through the PHPMysqlAdmin interface, from the **Appliance Manager** page (System > Settings > Appliances).

- Line 8. Uses the **cursor** method to create a cursor object for processing SQL statements.
- Line 9. Uses the **execute** method to execute an SQL statement. In this case, the SQL statement says:
 - Perform an INSERT in the database **in_api**, in the table **messages**.
 - Insert values into the following columns: **xtype, xid, message, value, message time**.
 - For the specified columns, substitute three substitution values (%s in Python), a null value, and the value returned by the **NOW** command.

- Insert into the **xtype** column a substitution value, specifically the value variable **%1** (the entity type for the device).
 - Insert into the **xid** column a substitution value, specifically the value of the variable **%x** (the device ID).
 - Insert into the **message** column a substitution value, specifically the string 'Bad connection to %s', where the Python substitution value (%s) will be replaced with the value of the variable **%a** (the device's IP address).
 - Insert a null value into the **value** column.
 - Insert into the **message time** column the value returned by the **NOW** command (the current date and time).
- Line 10. Uses the **execute** method to execute an SQL statement, specifically to COMMIT the changes to the database **in_api**, in the table **messages**.

To define an event policy based on the alert (database entry) generated by this Snippet, you would perform the following:

1. Navigate to the **Event Policy Manager** page. (Events > Event Policies)
2. In the **Event Policy Manager** page, click the **[Create]** button.
3. The **Event Policy Editor** page is displayed.
4. In the **Event Policy Editor** page, in the **[Policy]** tab, provide the following values:

Event Policy Editor | Create New Event Policy

Policy | Advanced | Suppressions

Event Source: **API** (highlighted with a red box)

Policy Name: _____

Event Message: _____

Operational State: **[Enabled]**

Event Severity: **[Major]** ☐ Use Modifier

Policy Description: _____

Save

- **Event Source.** Select **API**. This tells SL1 to look for new entries in the **in_api.messages** table.

5. In the **Event Policy Editor** page, in the **[Advanced]** tab, provide the following values:

The screenshot shows the 'Event Policy Editor' interface with the 'Advanced' tab selected. The configuration is as follows:

- Policy:** [Disabled]
- Occurrence Count:** [Disabled]
- Occurrence Time:** [Disabled]
- Expiry Delay:** [1 hour]
- Detection Weight:** [0 - First]
- Link-Alert:** (Select Dynamic Object) - Alton: Configuration, Alton: New Flash Enabled, Alton: Primary Power Supply Failure, Alton: Primary Power Supply Healthy, Alton: Redundant Power Supply Failure, Alton: Redundant Power Supply Healthy, APC: Environmental T/H
- Component Type:** [N/A]
- External Event Id:**
- External Category:**
- Match Logic:** [Text Search]
- Use Multi-match:** ☐
- Use Message-match:** ☐
- First Match String:**
- Second Match String:**
- Identifier Pattern:**
- Identifier Format:**
- Override YType:** [None]
- Auto-Clear:** [None Selected]
- Topology Suppression:** [Disabled]
- Category:** [None Selected]

The list of events in the 'Auto-Clear' section includes:

- Healthy: AKCP: AC Voltage sensor now reporting Normal Status [3192]
- Healthy: AKCP: DC Voltage sensor returned to Normal Status [3199]
- Healthy: AKCP: Dry contact sensor now Normal [3190]
- Healthy: AKCP: Smoke detector now Normal Status [3187]
- Healthy: AKCP: Water sensor now Normal [3188]
- Healthy: Alton: Primary Power Supply Healthy [3013]
- Healthy: Alton: Redundant Power Supply Healthy [3015]
- Healthy: APC: Batteries Do Not Need Replacement [1516]
- Healthy: APC: Battery Charge Normal [1524]
- Healthy: APC: Battery Run Time Remaining No Longer Critical [1518]
- Healthy: APC: Calibration Test Completed [1537]
- Healthy: APC: Communication Status Okay [1526]
- Healthy: APC: Diagnostic Test Passed [1534]
- Healthy: APC: Diagnostics Schedule Set [1530]
- Healthy: APC: Percent Battery Remaining No Longer Critical [1520]
- Healthy: APC: Temperature has returned to normal [1539]
- Healthy: APC: UPS Not on Battery [1526]
- Healthy: APC: UPS Not Running on Battery [1522]
- Healthy: APC: Zero Defective Battery Packs [1514]
- Healthy: Automatic Windows Service is now running [3508]
- Healthy: AWS: StorageGateway WorkingStorageUsed Has Returned To Normal [1421]
- Healthy: AWS: API 4xx Error Has Returned To Normal [4658]
- Healthy: AWS: API 5xx Error Has Returned To Normal [4660]

- **First Match String**. Enter a search string that matches the text we entered into the message column of the database table. In this case, we would enter "Bad connection to".
 - In the **Match Logic** field, we also selected **Text Search**, to tell SL1 to search for the text string we entered in the **First Match String** field, and not a regular expression.
6. For additional details on the **Event Policy Editor** page and tabs and creating event policies, see the manual **Events**.
 7. Click the **[Save]** button to save your new event.
 8. The event will be triggered each time a new entry is made to the database **in_api**, in the table **messages**, that contains the text "Bad connection to".

Action Policy that Executes a Snippet and Sends the Results to a Second Action Policy

Suppose that when SL1 generates an event saying that a device is not available, we want to ping the device from a Data Collector. Suppose that we then want to create a ticket that contains the results of the ping, so we can troubleshoot the availability problem. To do this, we could create an automation policy that executes two action policies, one that executes the ping (a Snippet Action Policy) and one that creates a ticket (a Ticket Action Policy).

Automation Policy

Our automation policy would look like this:

Automation Policy Editor | Creating New Automation Policy Reset

Policy Name: Policy Type: Policy State: Policy Priority: Organization:

Criteria Logic:

☐ Trigger on Child Rollup

Match Logic: Match Syntax:

Repeat Time: Align With:
☐ Include events for entities other than devices (organizations, assets, etc.)

Available Devices:
East Coast
ScienceLogic, Inc.: EM7 All-In-One: gmstack02
System
Cisco Systems: 7609S: 7609S-NPE3.cisco.com
Cisco Systems: CUCM Server: CUCM10.01.ga.sciencelogic.com

Aligned Devices:
(All devices)

Available Events:
[1660] Major: AWS: ELB Latency Has Exceeded Threshold
[202] Major: Cisco: TP: Audio Latency Occurred
[4238] Major: Cisco: TP: Endpoint (3-screen) Latency High
[4248] Major: Cisco: TP: Endpoint Latency High
[1071] Major: Cisco: TP: Latency Occurred

Aligned Events:
[1701] Critical: Poller: Availability and Latency checks failed

Available Actions:
Snippet [5]: Cisco: VOS Node Classification and Cluster Crea
Snippet [5]: EM7 Ping Snippet
Snippet [5]: Linux Classification and Automation
Snippet [5]: Microsoft: Windows Server Device Class Alignme
Snippet [5]: Microsoft: Windows Server Restart Automatic Sei

Aligned Actions:
1. Create Ticket [2]: Create a Ticket
2. Snippet [5]: EM7 Ping Snippet

- We specified that the automation policy:
 - Should act upon active events.
 - Is enabled.
 - Is associated with the organization "System".
 - Will be triggered when the specified event has a severity equal to or greater than "Minor".
 - Will be triggered 1 minute after the event occurs and is not cleared.
 - The policy will trigger the action policies once for each occurrence of the event(s).
 - Will be triggered at any time.
 - Will be triggered when the selected event occurs on at least one of the selected devices.
 - Will be triggered when the event "Critical Poller: Availability and Latency checks failed" occurs on at least one of the selected devices (which in this case is all devices).

- We specified that when all the criteria in the automation policy are met, the action policy "ping_device" and then the action policy "Create Ticket: Create Ping Ticket" will be executed, in the order specified.

Snippet Action Policy

The Snippet Action Policy would look like this:

The screenshot shows the 'Action Editor' window with the 'Policy Editor | Creating New Action' tab active. The configuration is as follows:

- Action Name:** ping_device
- Action State:** [Enabled]
- Description:** Snippet Policy
- Organization:** [System]
- Action Type:** Run a Snippet
- Snippet Credential:** Cisco CE Series History
- Action Run Context:** Collector
- Execution Environment:** Cisco: Base Pack
- Snippet Code:**

```
import subprocess
out, err = subprocess.Popen(['ping', '-c 5', EM7_VALUES['%a']],
    stdout=subprocess.PIPE).communicate()
EM7_RESULT = out
```

A 'Save' button is located at the bottom of the form.

This action policy:

- Tells the code to use the **subprocess** module to spawn processes, access stdin and stout for those processes, and retrieve return codes for those processes.
- Uses the **subprocess** module to run the **ping** command.
 - Notice that the argument for the ping command is EM7_VALUES['%a']. EM7_VALUES is the global dictionary that allows a Snippet to access the substitution variables. The substitution variable **%a** contains the IP address for the device where the event occurred.
 - Notice that the results are stored in the variable **out**.
- The value of the variable **out** is stored in the global Snippet variable **EM7_RESULT**. The global Snippet variable EM7_RESULT is used to populate the variable **%_EM7_RESULT_%**. The value of the variable **%_EM7_RESULT_%** can be accessed by the next Action Policy.

Ticket Action Policy

The Ticket Action Policy would look like this:

The screenshot shows a 'Policy Editor' window with a title bar that reads 'Policy Editor | Action Saved | Editing Action [9]' and a 'Reset' button. The main area contains several fields: 'Action Name' with the value 'create_ping_ticket', 'Action State' with a dropdown menu showing '[Enabled]', 'Description' with the value 'Create Ping Ticket', 'Organization' with a dropdown menu showing '[System]', 'Action Type' with the value 'Create a New Ticket', and 'Ticket Template' with a dropdown menu showing '[Connectivity Event: %M]'. At the bottom, there are two buttons: 'Save' and 'Save As'.

- We specified that this action policy:
 - Is enabled.
 - Will act upon events and devices aligned with the System organization.
 - Will create a new ticket in response to an automation policy.
 - Will use the ticket template "Connectivity Event: %M" to create the ticket.

Ticket Template

The Ticket Templates specified in the Create Ticket Action Policy would look like this:

The screenshot shows the 'Template Editor | New Template' interface. At the top, there's a blue header bar with the title and three buttons: 'Actions', 'Reset', and 'Guide'. Below the header, the 'Properties' section contains fields for 'Description' (set to '(New Template)'), 'Organization' (set to '[System]'), and 'Element' (set to 'System'). A 'Feature Use' dropdown is set to '[Ticketing]'. The 'Ticket Properties' section includes fields for 'Template Name' (set to 'Connectivity Template'), 'Ticket Description' (set to 'Connectivity Event %M'), and 'Ticket State' (a dropdown). Below these are several dropdown menus: 'Severity' (set to 'Sev 2 / Major'), 'Category' (set to 'Network'), 'Source' (set to 'Automated'), 'Queue' (set to 'Monitoring'), and 'Assigned User' (set to '[em7admin]'). A rich text editor follows, with a toolbar containing various icons for text formatting and insertion. The editor's content area contains the text: 'Diagnose and resolve availability problem with device.', 'Results of ping from Data Collection Server to device', and '%_EM7_RESULT_%'. At the bottom of the form is a 'Save' button.

- We specified that the ticket template:
 - Will create a ticket that includes the event description (%M) in the description.
 - Will create a ticket that has a severity of "Major".
 - Will create a ticket that is associated with the organization "System".
 - Will create a ticket with the category "Network".
 - Will create a ticket that will be placed in the "Monitoring" ticket queue.
 - Will create a ticket with the source "Automated".

- Will create a ticket that will be assigned to the user "em7admin".
- Will appear as a choice in action policies.
- Will create a ticket that includes note text that reads:

Diagnose and resolve availability problem with device.

Results of ping from Data Collection Server to device:

%_EM7_RESULT_%

Where the variable %_EM7_RESULT_% will contain the results from the previous Snippet Action Policy. In this case, the variable %_EM7_RESULT_% will contain the results from a ping from the Data Collector to the device where the availability event occurred.

Resulting Ticket

The resulting ticket would look like this:

The screenshot shows the 'Ticket Editor' window for an 'Active Ticket [15]'. The interface includes tabs for Properties, Logs, Automation, and Message. The 'Properties' tab is active, displaying the following information:

- Description:** Connectivity Event: Device failed Availability and Latency checks: Both Availability and Latency checks have failed
- Organization:** [System]
- Element:** em7_ao [ScienceLogic, Inc. | EM7 All-in-One | IP: 10.100.100.9 | ID: 578]
- Aligned Event:** [23427] Device failed Availability and Latency checks: Both Availability and Latency checks have failed
- Ticket Age:** 12 secs
- Created On/By:** 2012-01-04 13:33:45 | em7admin
- Modified Age:** 12 secs
- Modified On/By:** 2012-01-04 13:33:45 | em7admin

Below the properties, the 'Ticket Properties' section shows a form with the following fields:

- Ticket Description:** Connectivity Event: Device failed Availability and Latency checks: Both Avail
- Sub-Organization:** [None]
- Ticket State:** [Open]
- Status:** [Open]
- Severity:** [Sev 3 / Major]
- Category:** [Network]
- Source:** [Automated]
- Queue:** [Monitoring]
- Assigned User:** [em7admin]

The 'Notes & Attachments' section shows a single note:

- #1) Date [2012-01-04 13:33:45] | User [em7admin]**
Diagnose and resolve availability problem with device.
Results of ping from Data Collection Server to device:
NameError("name 'EM' is not defined").

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

Appendix



A

Run Book Variables

Overview

This appendix defines the different variables you can use when creating an action policy.

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

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

This appendix covers the following topics:

Run Book Variables	123
--	-----

Run Book Variables

You can include variables when creating an action policy. These variables are listed in the table below.

- In an action policy of type **Send an Email Notification**, you can include one or more of these variables in the fields **Email Subject** and **Email Body**.
- In an action policy of type **Send an SNMP Trap**, you can include one or more of these variables in the **Trap OID** field, **Varbind OID** field, and the **Varbind Value** field.
- In an action policy of type **Create a New Ticket**, you can include one or more of these variables in the **Description** field or the **Note** field of the related Ticket Template.
- In an action policy of type **Send an SNMP Set**, you can include one or more of these variables in the **SNMP OID** field and the **SNMP Value** field.
- In an action policy of type **Run A Snippet**, you can access variables from the global dictionary **EM7_VALUES**.
- In a policy of type **Execute an SQL Query**, you can include one or more of these variables in the **SQL Query** field.

Variable	Source	Description
%A	Account	Username
%N	Action	Automation action name
%g	Asset	Asset serial
%h	Asset	Device ID associated with the asset
%i (lowercase "eye")	Asset	Asset Location
%k	Asset	Asset Room
%K	Asset	Asset Floor
%P	Asset	Asset plate
%p	Asset	Asset panel
%q	Asset	Asset zone
%Q	Asset	Asset punch
%U	Asset	Asset rack
%u	Asset	Asset shelf
%v	Asset	Asset tag
%w	Asset	Asset model
%W	Asset	Asset make
%m	Automation	Automation policy note
%n	Automation	Automation policy name
%F	Dynamic Alert	Alert ID for a Dynamic Application Alert
%I (uppercase "eye")	Dynamic	For events with a source of "dynamic", this variable contains the index value

Variable	Source	Description
	Alert	from SNMP. For events with a source of "syslog" or "trap", this variable contains the value that matches the Identifier Pattern field in the event definition.
%T	Dynamic Alert	Value returned by the Threshold function in a Dynamic Application Alert.
%V	Dynamic Alert	Value returned by the Result function in a Dynamic Application Alert.
%L	Dynamic Alert	Value returned by the label variable in a Dynamic Application Alert.
%a	Entity	IP address
_%category_id	Entity	Device category ID associated with the entity in the event.
_%category_name	Entity	Device category name associated with the entity in the event.
_%class_id	Entity	Device class ID associated with the entity in the event.
_%class_name	Entity	Device class name associated with the entity in the event.
_%parent_id	Entity	For component devices, the device ID of the parent device.
_%parent_name	Entity	For component devices, the name of the parent device.
_%root_id	Entity	For component devices, the device ID of the root device.
_%root_name	Entity	For component devices, the name of the root device.
%1 (one)	Event	Entity type. Possible values are: <ul style="list-style-type: none"> • 0. Organization • 1. Device • 2. Asset • 4. IP Network • 5. Interface • 6. Vendor • 7. Account • 8. Virtual Interface • 9. Device Group • 10. IT Service • 11. Ticket
%2	Event	Sub-entity type. <p>Possible values for organizations are:</p> <ul style="list-style-type: none"> • 9. News feed <p>Possible values for devices are:</p> <ul style="list-style-type: none"> • 1. CPU • 2. Disk • 3. File System

Variable	Source	Description
		<ul style="list-style-type: none"> • 4. Memory • 5. Swap • 6. Component • 7. Interface • 9. Process • 10. Port • 11. Service • 12. Content • 13. Email
%4	Event	Text string of the user name that cleared the event.
%5	Event	Timestamp of when event was deleted.
%6	Event	Timestamp for event becoming active.
%7	Event	<p>Event severity (1 -5), for compatibility with previous versions of SL1 . 1 =critical, 2 =major, 3 =minor, 4 =notify, 5 =healthy.</p> <div> <p>NOTE: When referring to an event, %7 represents severity (for previous versions of SL1). When referring to a ticket, %7 represents the subject line of an email used to create a ticket.</p> </div>
%c	Event	Event counter
%d	Event	Timestamp of last event occurrence.
%D	Event	Timestamp of first event occurrence.
%e	Event	Event ID
%H	Event	URL link to event
%M	Event	Event message
%s	Event	severity (0 - 4). 0=healthy, 1=notify, 2=minor, 3=major, 4=critical.
%S	Event	Severity (HEALTHY - CRITICAL)
%_user_note	Event	Current note about the event that is displayed on the Events page.
%x	Event	Entity ID
%X	Event	Entity name
%y	Event	Sub-entity ID
%Y	Event	Sub-entity name
%Z	Event	Event source (Syslog - Group)
%z	Event	Event source (1 - 8)
%_ext_ticket_ref	Event	For events associated with an external Ticket ID, this variable contains the external Ticket ID.

Variable	Source	Description
%3	Event Policy	Event policy ID
%E	Event Policy	External ID from event policy
%f	Event Policy	Specifies whether event is stateful, that is, has an associated event that will clear the current event. 1 (one)=stateful; 0 (zero)=not stateful.
%G	Event Policy	Event Category
%R	Event Policy	Event policy cause/action text
%_event_policy_name	Event Policy	Name of the event policy that triggered the event.
%B	Organization	Organization billing ID
%b	Organization	Impacted organization
%C	Organization	Organization CRM ID
%o (lowercase "oh")	Organization	Organization ID
%O (uppercase "oh")	Organization	Organization name
%r	System	Unique ID / name for the current SL1 system
%7	Ticket	<p>Subject of email used to create a ticket. If you specify this variable in a ticket template, SL1 will use the subject line of the email in the ticket description or note text when SL1 creates the ticket.</p> <div> <p>NOTE: When referring to a ticket, %7 represents the subject line of an Email used to create a ticket. When referring to an event, %7 represents severity (for previous versions of SL1).</p> </div>
%t	Ticket	Ticket ID
%J	Ticket	Description field from the SL1 ticket.

© 2003 - 2020, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010