AWS Incident Manager Integration

AWS Base Pack Synchronization PowerPack Version 1.0.0

AWS Incident Manager Synchronization PowerPack Version 1.0.0

AWS Incident Manager Automation PowerPack Version 100

Table of Contents

Chapter

1

Introduction to the AWS Incident Manager Synchronization PowerPack

Overview

This chapter describes how you can use the *AWS Incident Manger* Synchronization PowerPack to automatically synchronize SL1 events and Amazon Web Services (AWS) incidents between your AWS and SL1 systems. The integration is bidirectional, from SL1 to AWS.

This Synchronization PowerPack requires a subscription to ScienceLogic Standard solutions.

NOTE: After the 2.1.0 platform release, the *Integration Service* was rebranded as *SL1 PowerFlow*, and the *Automation Builder* was rebranded as *SL1 PowerFlow builder*.

NOTE: The label "SyncPack" is used in place of "Synchronization PowerPack" in the PowerFlow user interface.

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

This chapter covers the following topics:

Prerequisites for this Synchronization PowerPack

This Synchronization PowerPack requires the following:

- A subscription to the SL1 Standard solution
- *AWS Base Synchronization PowerPack*
- *SL1 Base Notifications Synchronization PowerPack*

The following table lists the port access required by PowerFlow and this Synchronization PowerPack:

Source IP	PowerFlow Destination	PowerFlow Source Port	Destination Port	Requirement
PowerFlow	SL1 API	Any	TCP 443	SL1 API Access
PowerFlow	AWS API	Any	TCP 443	AWS API Access

Contents of the Synchronization PowerPack

This section lists the contents of the *AWS Incident Manager* Synchronization PowerPack.

PowerFlow Applications

- ***Bulk Resolve SL1 Events From AWS***. This application collects resolution state data from AWS and resolves corresponding SL1 events.
- ***Create Timeline Event In AWS Incident Manager***. This application collects acknowledged event data from SL1 and creates a timeline event in AWS.
- ***Resolve AWS Incident***. This application resolves an AWS incident that was resolved by a corresponding SL1 event.
- ***Send SL1 Event to AWS Incident Manager***. This application collects event details from SL1 and creates an incident in AWS.

For more information about how to configure these applications, see ***Configuring and Aligning the AWS Incident Manager Applications***.

Configuration Object

- ***AWS Incidents Base Config***. This configuration object can be used as a template after the Synchronization PowerPack is installed on the PowerFlow system. The configuration object includes the following:

- Details for connecting to SL1, including the host, username, and password.
- Details for connecting to AWS, including the region name, access key ID, secret access key ID, and service.
- Details for event and incident response including templates, maps, time, external URL population, and response plans.

Steps

The following steps are included in this Synchronization PowerPack:

- CreateSL1Payload
- Create Timeline Event In AWS Incident Manager
- Get Event Details From SL1 Start AWS Incident
- Get Resolved Incidents And Pass To SL1
- PostUpdateToSL1
- Resolve Incident In AWS Incident Manager

Installing the Synchronization PowerPack

A Synchronization PowerPack file has the **.whl** file extension type. You can download the Synchronization PowerPack file from the ScienceLogic Support site.

NOTE: You must download the *AWS Base Synchronization PowerPack* before downloading the *AWS Incident Manager Synchronization PowerPack*.

Downloading the Synchronization PowerPack

To locate and download the Synchronization PowerPack:

1. Go to the ScienceLogic Support Site.
2. Click the **[Product Downloads]** tab and select *PowerPack*.
3. In the ***Search PowerPacks*** field, search for the Synchronization PowerPack and select it from the search results. The **Release Version** page appears.
4. On the **[PowerPack Versions]** tab, click the name of the Synchronization PowerPack version that you want to install. The **Release File Details** page appears.
5. Click the **[Download File]** button or click the name of the **.zip** file containing the **.whl** file for this Synchronization PowerPack to start downloading the file.

NOTE: Synchronization PowerPacks do not require a specific license. After you download a Synchronization PowerPack, you can import it to your PowerFlow system using the PowerFlow user interface.

NOTE: If you are installing or upgrading to the latest version of this Synchronization PowerPack in an offline deployment, see "Installing or Upgrading in an Offline Environment" in the Synchronization PowerPack release notes to ensure you install any external dependencies.

Importing the Synchronization PowerPack

To import a Synchronization PowerPack in the PowerFlow user interface:

1. On the **SyncPacks** page of the PowerFlow user interface, click **[Import SyncPack]**. The **Import SyncPack** page appears.
2. Click **[Browse]** and select the **.whl** file for the Synchronization PowerPack you want to install.

   TIP: You can also drag and drop a **.whl** file to the **Import SyncPack** page.

3. Click **[Import]**. PowerFlow registers and uploads the Synchronization PowerPack. The Synchronization PowerPack is added to the **SyncPacks** page.

NOTE: You cannot edit the content package in a Synchronization PowerPack published by ScienceLogic. You must make a copy of a ScienceLogic Synchronization PowerPack and save your changes to the new Synchronization PowerPack to prevent overwriting any information in the original Synchronization PowerPack when upgrading.

Installing the Synchronization PowerPack

To activate and install a Synchronization PowerPack in the PowerFlow user interface:

1. On the **SyncPacks** page of the PowerFlow user interface, click the **[Actions]** button (⋮) for the Synchronization PowerPack you want to install and select *Activate & Install*. The **Activate & Install SyncPack** modal appears.

   NOTE: If you try to activate and install a Synchronization PowerPack that is already activated and installed, you can choose to "force" installation across all the nodes in the PowerFlow system.

   TIP: If you do not see the PowerPack that you want to install, click the Filter icon (≡) on the **SyncPacks** page and select *Toggle Inactive SyncPacks* to see a list of the imported PowerPacks.

2. Click **[Yes]** to confirm the activation and installation. When the Synchronization PowerPack is activated, the **SyncPacks** page displays a green check mark icon (✅) for that Synchronization PowerPack. If the activation or installation failed, then a red exclamation mark icon (❗) appears.
3. For more information about the activation and installation process, click the check mark icon (✅) or the exclamation mark icon (❗) in the **Activated** column for that Synchronization PowerPack. For a successful installation, the "Activate & Install SyncPack" application appears, and you can view the Step Log for the steps. For a failed installation, the **Error Logs** window appears.
4. If you have other versions of the same Synchronization PowerPack on your PowerFlow system, you can click the **[Actions]** button (⋮) for that Synchronization PowerPack and select *Change active version* to activate a different version other than the version that is currently running.

Chapter 2

Configuring Applications for the AWS Incident Manager Synchronization PowerPack

Overview

This chapter describes how to set up the PowerFlow applications for the *AWS Incident Manager* Synchronization PowerPack.

This chapter covers the following topics:

Creating and Aligning a Configuration Object in PowerFlow

A ***configuration object*** supplies the login credentials and other required information needed to execute the steps for a PowerFlow application. The **Configurations** page (⚙) of the PowerFlow user interface lists all available configuration objects for that system.

You can create as many configuration objects as you need. A PowerFlow application can only use one configuration object at a time, but you can use (or "align") the same configuration object with multiple applications.

To use this Synchronization PowerPack, you will need to use an existing configuration object in the PowerFlow user interface or create a new configuration object. Next, you need to align that configuration object to the relevant applications.

Creating a Configuration Object

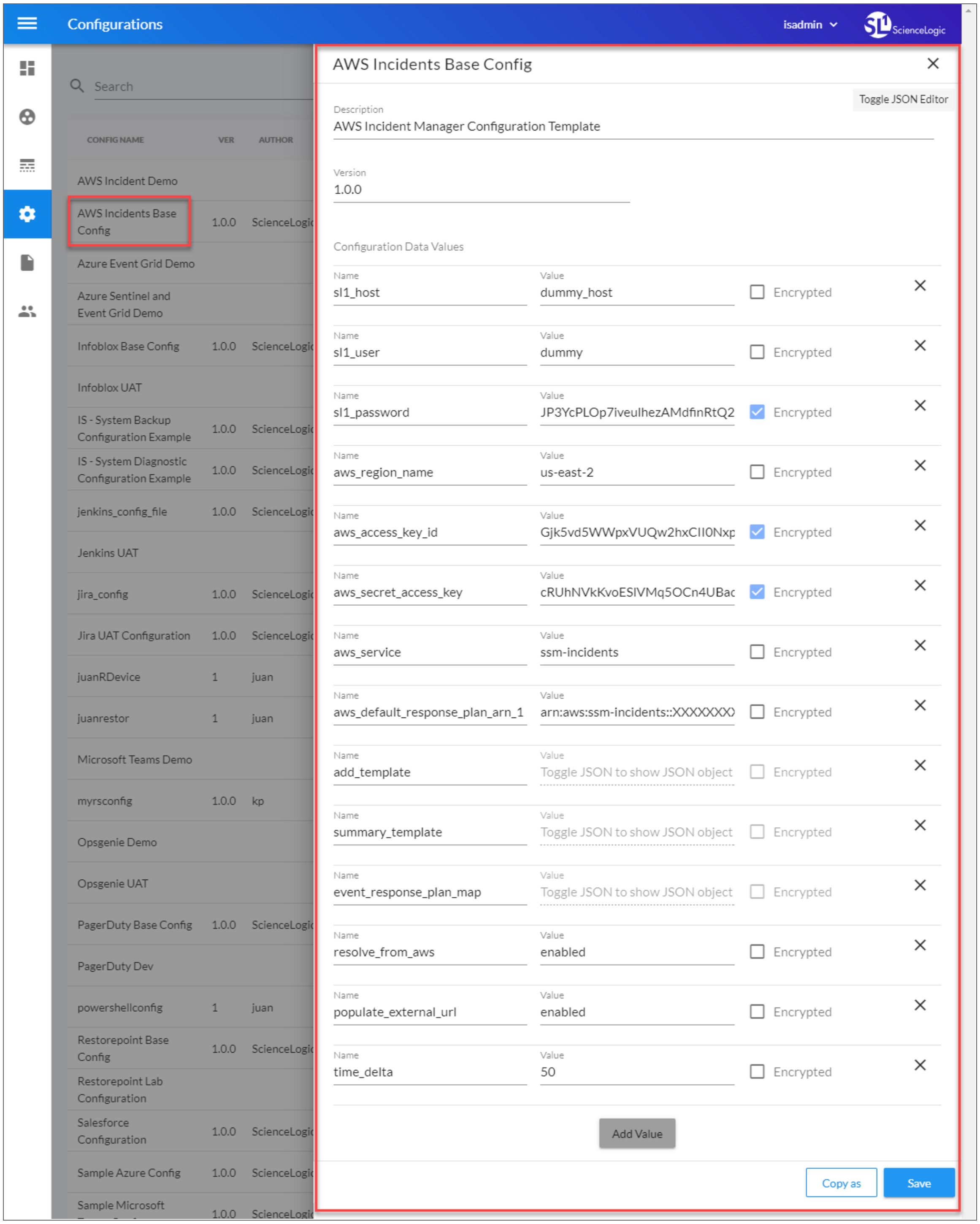
For this Synchronization PowerPack, you can make a copy of the "AWS Incidents Base Config" configuration object, which is the sample configuration file that was installed with the *AWS Incident Manager* Synchronization PowerPack.

TIP: The "AWS Incidents Base Config" configuration object contains all of the required variables. Simply update the variables from that object to match your SL1 and AWS settings.

NOTE: For more information about the AWS terms and concepts in this section, see the AWS documentation.

To create a configuration object based on the "AWS Incidents Base Config" configuration object:

1. In the PowerFlow user interface, go to the **Configurations** page (⚙).
2. Click the **[Actions]** button (⋮) for the "AWS Incidents Base Config" configuration object and select *Edit*. The **Configuration** pane appears:



CONFIG NAME	VER	AUTHOR
AWS Incident Demo		
AWS Incidents Base Config	1.0.0	ScienceLogi
Azure Event Grid Demo		
Azure Sentinel and Event Grid Demo		
Infoblox Base Config	1.0.0	ScienceLogi
Infoblox UAT		
IS - System Backup Configuration Example	1.0.0	ScienceLogi
IS - System Diagnostic Configuration Example	1.0.0	ScienceLogi
jenkins_config_file	1.0.0	ScienceLogi
Jenkins UAT		
jira_config	1.0.0	ScienceLogi
Jira UAT Configuration	1.0.0	ScienceLogi
juanRDevice	1	juan
juanrestor	1	juan
Microsoft Teams Demo		
myrsconfig	1.0.0	kp
Opsgenie Demo		
Opsgenie UAT		
PagerDuty Base Config	1.0.0	ScienceLogi
PagerDuty Dev		
powershellconfig	1	juan
Restorepoint Base Config	1.0.0	ScienceLogi
Restorepoint Lab Configuration		
Salesforce Configuration	1.0.0	ScienceLogi
Sample Azure Config	1.0.0	ScienceLogi
Sample Microsoft	1.0.0	ScienceLogi

AWS Incidents Base Config

Description
AWS Incident Manager Configuration Template

Version
1.0.0

Configuration Data Values

Name	Value	
sl1_host	dummy_host	□ Encrypted
sl1_user	dummy	□ Encrypted
sl1_password	JP3YcPLOp7iveulhezAMdfnRtQ2	☑ Encrypted
aws_region_name	us-east-2	□ Encrypted
aws_access_key_id	Gjk5vd5WWpxVUQw2hxCIl0Nxp	☑ Encrypted
aws_secret_access_key	cRUhNVkKvoESIVMq5OCn4UBac	☑ Encrypted
aws_service	ssm-incidents	□ Encrypted
aws_default_response_plan_arn_1	arn:aws:ssm-incidents::XXXXXXXX	□ Encrypted
add_template	Toggle JSON to show JSON object	□ Encrypted
summary_template	Toggle JSON to show JSON object	□ Encrypted
event_response_plan_map	Toggle JSON to show JSON object	□ Encrypted
resolve_from_aws	enabled	□ Encrypted
populate_external_url	enabled	□ Encrypted
time_delta	50	□ Encrypted

3. Click **[Copy as]**. The **Create Configuration** pane appears.
4. Complete the following fields:

   - ***Friendly Name***. Type a name for the configuration object that will display on the **Configurations** page.
   - ***Description***. Type a brief description of the configuration object.
   - ***Author***. Type the user or organization that created the configuration object.
   - ***Version***. Type a version of the configuration object.

5. In the ***Configuration Data*** field, update the default variable definitions to match your PowerFlow configuration:

   - ***sl1_host***. Type the hostname or IP address of the SL1 system the alerts will synchronize to.
   - ***sl1_user***. Type the username for your SL1 system.
   - ***sl1_password***. Type the password for your SL1 system.
   - ***aws_region_name***. Type the region of your AWS system.
   - ***aws_access_key_id***. Type the access key ID of your AWS system.
   - ***aws_secret_access_key***. Type the secret access key ID of your AWS system.
   - ***aws_service***. Keep the default value.
   - ***aws_default_response_plan_arn_1***. Type the ARN for the default AWS response plan for PowerFlow to use when creating an incident in AWS.
   - ***add_template***. Toggle the JSON editor to define the template to translate SL1 event information to an AWS incident.
   - ***summary_template***. Toggle the JSON editor to define the summary format to translate an SL1 event to an AWS incident.
   - ***event_response_plan_map***. You can configure specific SL1 event criteria to trigger alternative response plans in AWS. To define an alternative response plan, toggle the JSON editor and enter an event property, search key to match to the event, and the ARN for the alternative AWS response plan. For example, if you want to trigger an alternative response plan for an SL1 event that contains "database" in the event message, enter the JSON code as follows:

     ```
     {
     "event_property": "%M",
     "response_plan": "arn:aws:ssm-incidents::XXXXXXXX:response-
     plan/XXXXXXXXX",
     "search_key": "database"
     }
     ```

   - ***resolve_from_aws***. When enabled, this parameter resolves SL1 events from AWS incidents. The default value is 'enabled'. To disable this parameter, change this value to 'disabled'.
   - ***populate_external_url***. The option to add an AWS incident URL to the corresponding SL1 event. The default value is 'enabled'.

- ***time_delta***. Type the time configuration in days to synchronize your AWS incidents and SL1 events. The "Bulk Resolve SL1 Events from AWS" application will only collect incidents that have been updated within the number of days defined in this parameter.

9. Click **[Save]**. You can now align this configuration object with one or more applications.

Aligning a Configuration Object and Configuring PowerFlow Applications

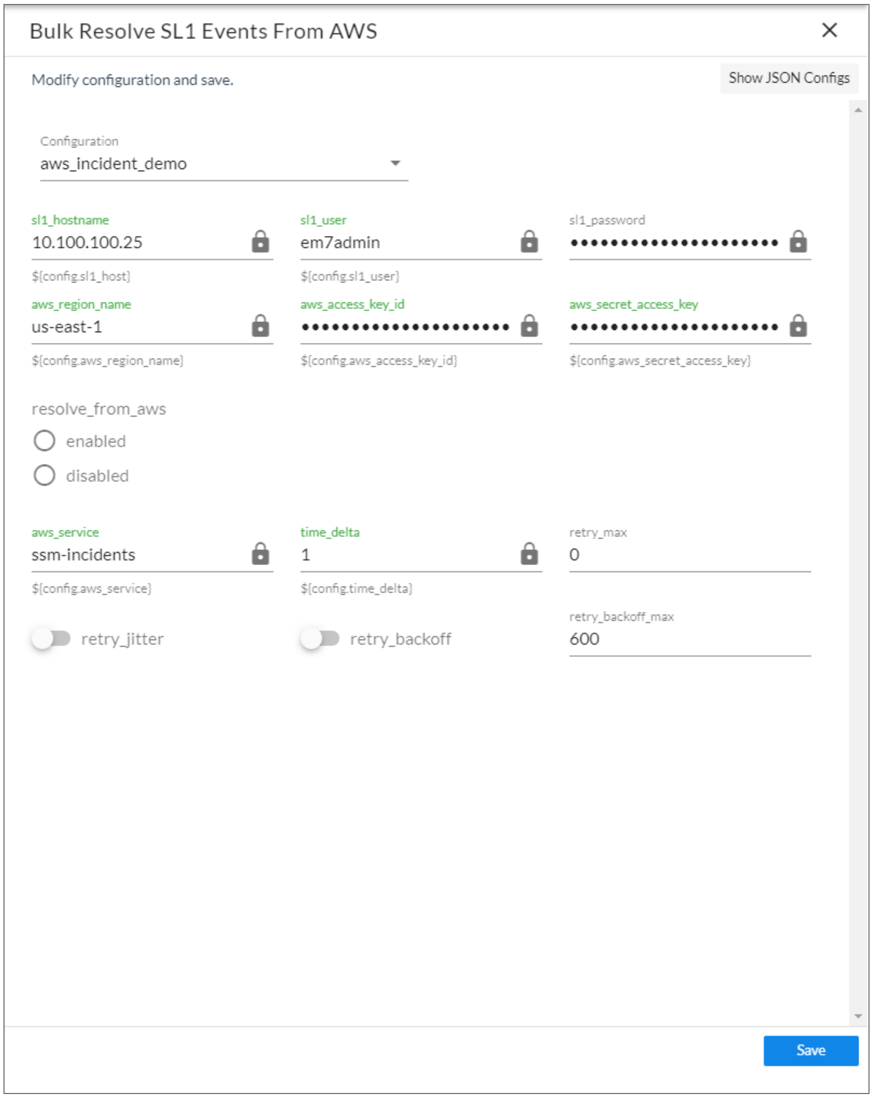
With this Synchronization PowerPack, any status changes made to an SL1 event are sent to AWS to update the corresponding incident. Any status changes to the AWS incident are synced back to the corresponding SL1 event. You will need to align the AWS Incident Manager applications with the relevant configuration object in PowerFlow, and, if needed, update any other fields on the **Configuration** pane for the applications.

To run this Synchronization PowerPack, you must "align" the configuration object to run with the following PowerFlow applications:

- "Bulk Resolve SL1 Events From AWS"
- "Create Timeline Event In AWS Incident Manager"
- "Resolve AWS Incident"
- "Send SL1 Event to AWS Incident Manager"

To align the configuration object with the relevant PowerFlow applications:

1. On the **Applications** page of the PowerFlow user interface, open one of the PowerFlow applications listed above and click **[Configure]** (⚙). The **Configurations** pane for that application appears:



Modify configuration and save.

Configuration
aws_incident_demo

sl1_hostname
10.100.100.25
${config.sl1_host}

sl1_user
em7admin
${config.sl1_user}

sl1_password
••••••••••••••••••••

aws_region_name
us-east-1
${config.aws_region_name}

aws_access_key_id
••••••••••••••••••••
${config.aws_access_key_id}

aws_secret_access_key
••••••••••••••••••••
${config.aws_secret_access_key}

resolve_from_aws
○ enabled
○ disabled

aws_service
ssm-incidents
${config.aws_service}

time_delta
1
${config.time_delta}

retry_max
0

retry_jitter

retry_backoff

retry_backoff_max
600

2. From the ***Configurations*** drop-down, select the configuration object you want to use.

> **NOTE:** The values for **sl1_hostname** and the other parameters that appear in the **Configuration** pane with a padlock icon (🔒) are populated either by the configuration object you aligned with the application or by the Run Book Action. Do not modify these values. If you encounter an error, make sure your Run Book Action is configured properly.

3. Click **[Save]** to align that configuration with the application.
4. Wait until you see the "App & Config modifications saved" pop-up message before proceeding.
5. Repeat this process for the other PowerFlow applications.

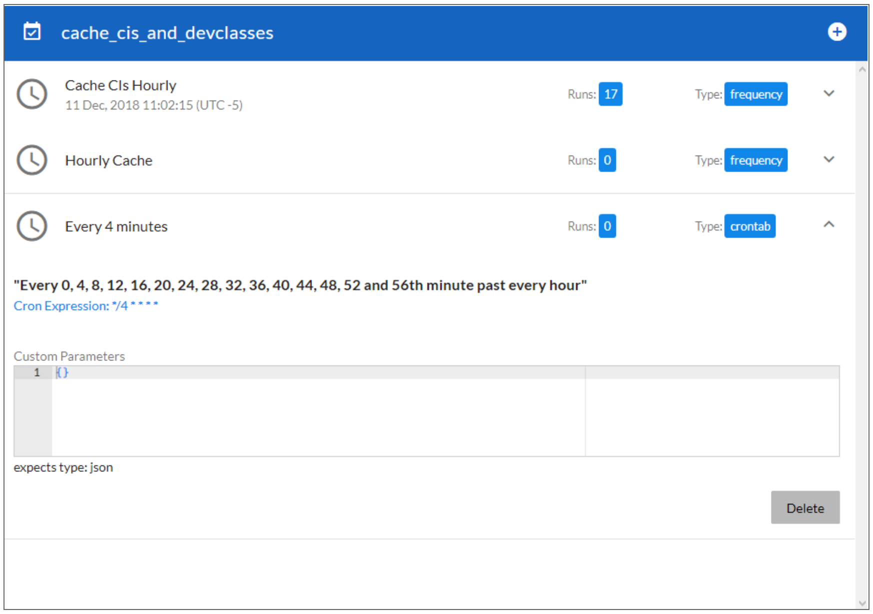
Scheduling PowerFlow Applications

To trigger the "Bulk Resolve SL1 Events From AWS" application, you must schedule the application.

You can create one or more schedules for a single application in the PowerFlow user interface. When creating each schedule, you can specify the queue and the configuration file for that application.

To schedule an application:

1. On the **Applications** page (▤), click the **[Schedule]** button for the application you want to schedule. The **Schedule** window appears, displaying any existing schedules for that application:



cache_cis_and_devclasses

Cache CIs Hourly
11 Dec, 2018 11:02:15 (UTC -5)
Runs: 17 Type: frequency

Hourly Cache
Runs: 0 Type: frequency

Every 4 minutes
Runs: 0 Type: crontab

"Every 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52 and 56th minute past every hour"
Cron Expression: */4 * * * *

Custom Parameters

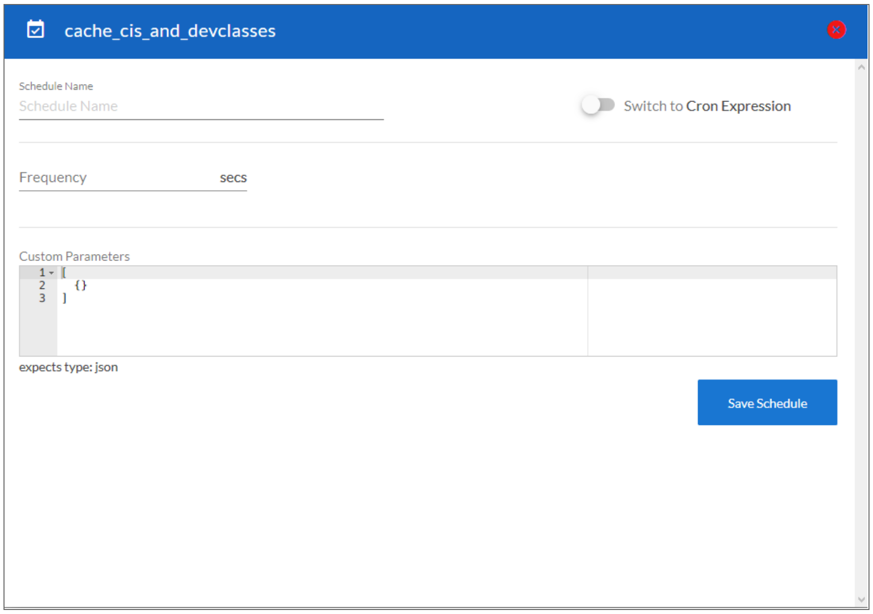
```
{}
```

expects type: json

Delete

NOTE: If you set up a schedule using a cron expression, the details of that schedule display in a more readable format in this list. For example, if you set up a cron expression of ***/4 * * * ***, the schedule on this window includes the cron expression along with an explanation of that expression: "*Every 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, and 56th minute past every hour*".

2. Select a schedule from the list to view the details for that schedule.
3. Click the + icon to create a schedule. A blank **Schedule** window appears:

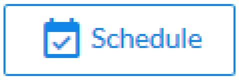


```
[
  {}
]
```

4. In the **Schedule** window, complete the following fields:

   - ***Schedule Name***. Type a name for the schedule.
   - ***Switch to***. Use this toggle to switch between a cron expression and setting the frequency in seconds.
     - ***Cron expression***. Select this option to schedule the application using a cron expression. If you select this option, you can create complicated schedules based on minutes, hours, the day of the month, the month, and the day of the week. As you update the cron expression, the **Schedule** window displays the results of the expression in more readable language, such as *Expression:* "*Every 0 and 30th minute past every hour on the 1 and 31st of every month*", based on */30 * * /30 * *.
     - ***Frequency in seconds***. Type the number of seconds per interval that you want to run the application.
   - ***Custom Parameters***. Type any JSON parameters you want to use for this schedule, such as information about a configuration file or mappings.

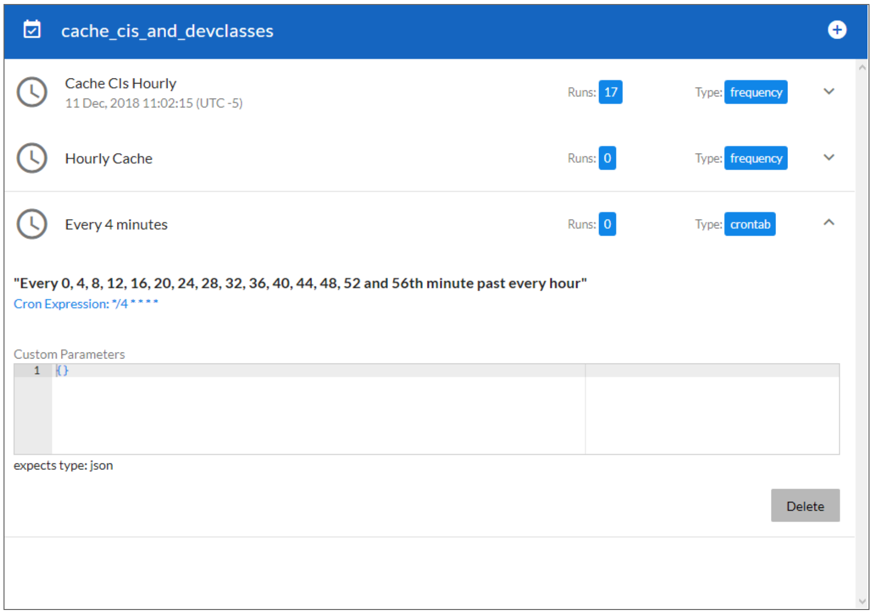
5. Click **[Save Schedule]**. The schedule is added to the list of schedules on the initial **Schedule** window. Also, on the **Applications** page, the word "Scheduled" appears in the **Scheduled** column for this application, and the **[Schedule]** button contains a check mark:



NOTE: After you create a schedule, it continues to run until you delete it. Also, you cannot edit an existing schedule, but you can delete it and create a similar schedule if needed.

To view or delete an existing schedule:

1. On the **Applications** page, click the **[Schedule]** button for the application that contains a schedule you want to delete. The **Schedule** window appears.
2. Click the down arrow icon (⌄) to view the details of an existing schedule:



cache_cis_and_devclasses

Cache CIs Hourly
11 Dec, 2018 11:02:15 (UTC -5) — Runs: 17 — Type: frequency

Hourly Cache — Runs: 0 — Type: frequency

Every 4 minutes — Runs: 0 — Type: crontab

"Every 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52 and 56th minute past every hour"
Cron Expression: */4 * * * *

Custom Parameters

```
1 {}
```

expects type: json

3. To delete the selected schedule, click **[Delete]**. The schedule is removed.

NOTE: When either multiple SL1 instances or multiple AWS instances are involved with PowerFlow, you should create an individual configuration object for each SL1 or AWS instance. Next, create an individual schedule for each configuration object. Each schedule should use a configuration object that is specific to that single SL1 or AWS instance. Creating copies of a PowerFlow application from a Synchronization PowerPack for the purpose of distinguishing between domains is not supported, and will result in issues on upgrades.

Chapter 3

Introduction to the AWS Incident Manager Automation PowerPack

Overview

This chapter describes how to use the automation policies and automation actions found in the *AWS Incident Manager Automation* PowerPack.

This PowerPack requires a subscription to ScienceLogic Standard solutions.

This chapter covers the following topics:

What is the AWS Incident Manager Automation PowerPack?

The *AWS Incident Manager Automation* PowerPack includes automation policies and actions that bidirectionally align incidents and events triggered and updated in Amazon Web Services (AWS) and SL1.

IMPORTANT: You must install and configure the *AWS Incident Manager Synchronization* PowerPack version 1.0.0 and *AWS Base Pack Synchronization* PowerPack version 1.0.0 before using the AWS Incident Manager Automation PowerPack.

Installing the AWS Incident Manager Automation PowerPack

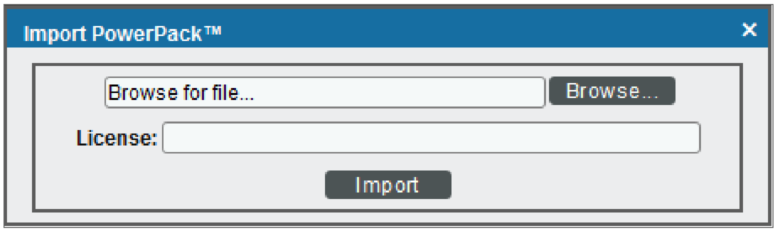
Before completing the steps in this manual, you must import and install the latest version of the *AWS Incident Manager Automation* PowerPack.

NOTE: The *AWS Incident Manager Automation* PowerPack requires SL1 version 10.1.0 or later. For details on upgrading SL1, see the appropriate SL1 Release Notes.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter

4

Configuring Automation Action Credentials

Overview

This chapter describes how to configure the credential required by the automation actions in the *AWS Incident Manager Automation* PowerPack.

This chapter covers the following topics:

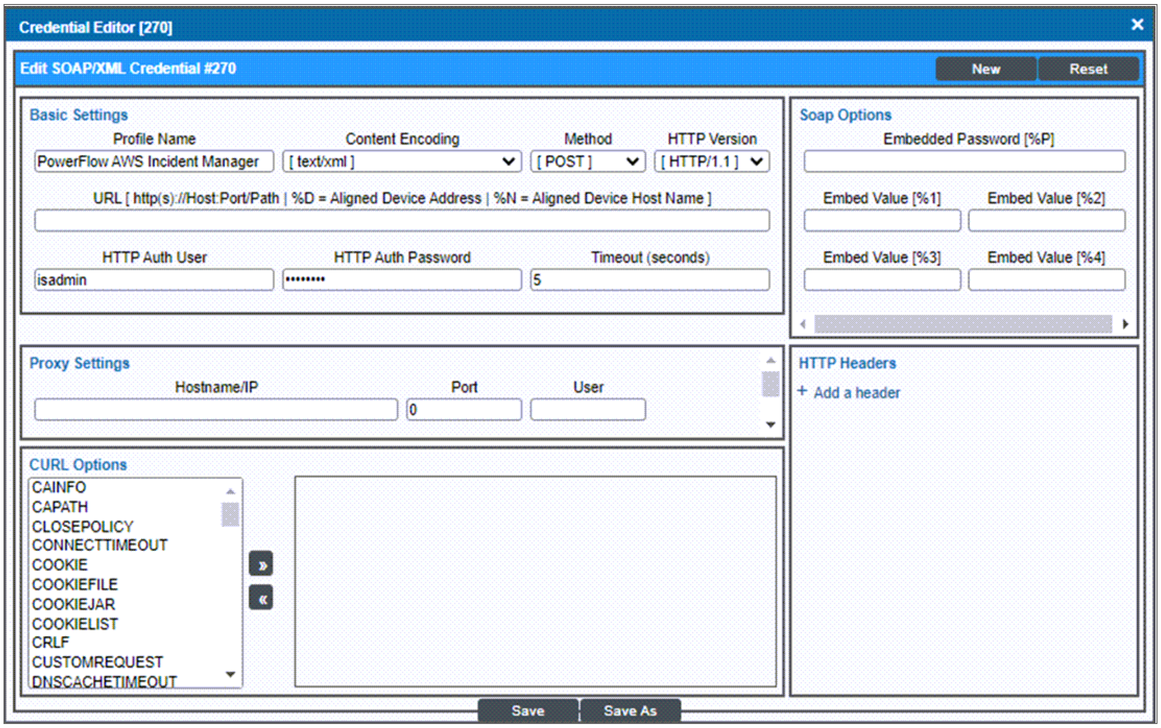
Creating a SOAP/XML Credential to Access SL1 PowerFlow

After you have integrated your AWS and PowerFlow systems, you must create a SOAP/XML credential so that the automation actions included in the PowerPack can access your PowerFlow system. The *AWS Incident Manager Automation* PowerPack includes a template for a SOAP/XML credential that you can edit for use with your PowerFlow system.

To define a SOAP/XML credential using the example credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Click the wrench icon (🔧) for the **PowerFlow AWS Incident Manager** credential. The **Credential Editor** modal window appears:



Credential Editor [270]

Edit SOAP/XML Credential #270

Profile Name: PowerFlow AWS Incident Manager

Content Encoding: [text/xml]

Method: [POST]

HTTP Version: [HTTP/1.1]

HTTP Auth User: isadmin

HTTP Auth Password: ••••••••

Timeout (seconds): 5

Port: 0

3. Supply values in the following fields:

   - ***Profile Name***. Type a new name for the credential.
   - ***URL***. Type the URL for your SL1 PowerFlow system.
   - ***HTTP Auth User***. Type the username for your SL1 PowerFlow user account.
   - ***HTTP Auth Password***. Type the password for your SL1 PowerFlow user account.

4. Click the **[Save As]** button to save the new SOAP/XML credential.

5. SL1 assigns the credential an ID number. Take note of the ID number that appears in the **Credential Editor** heading, as you will need this when editing the input parameters of the automation actions included in the *AWS Incident Manager Automation*PowerPack.

Chapter

5

Editing the AWS Incident Manager Automation Actions

Overview

This manual describes how to edit the automation actions included in the *AWS Incident Manager Automation* PowerPack so that the automation actions can communicate with your PowerFlow system.

This chapter covers the following topics:

Editing the AWS Incident Manager Automation Actions

The *AWS Incident Manager Automation* PowerPack includes automation actions that use the "Run Integration Service Application" action type to trigger the PowerFlow applications that trigger, acknowledge, and resolve incidents and events between SL1 and AWS. You can specify the credential ID in the ***Input Parameters*** field in the **Action Policy Editor** modal.

After you edit the action and trigger the event policy, the new event log will be added to the respective device on the **Event Console** page.

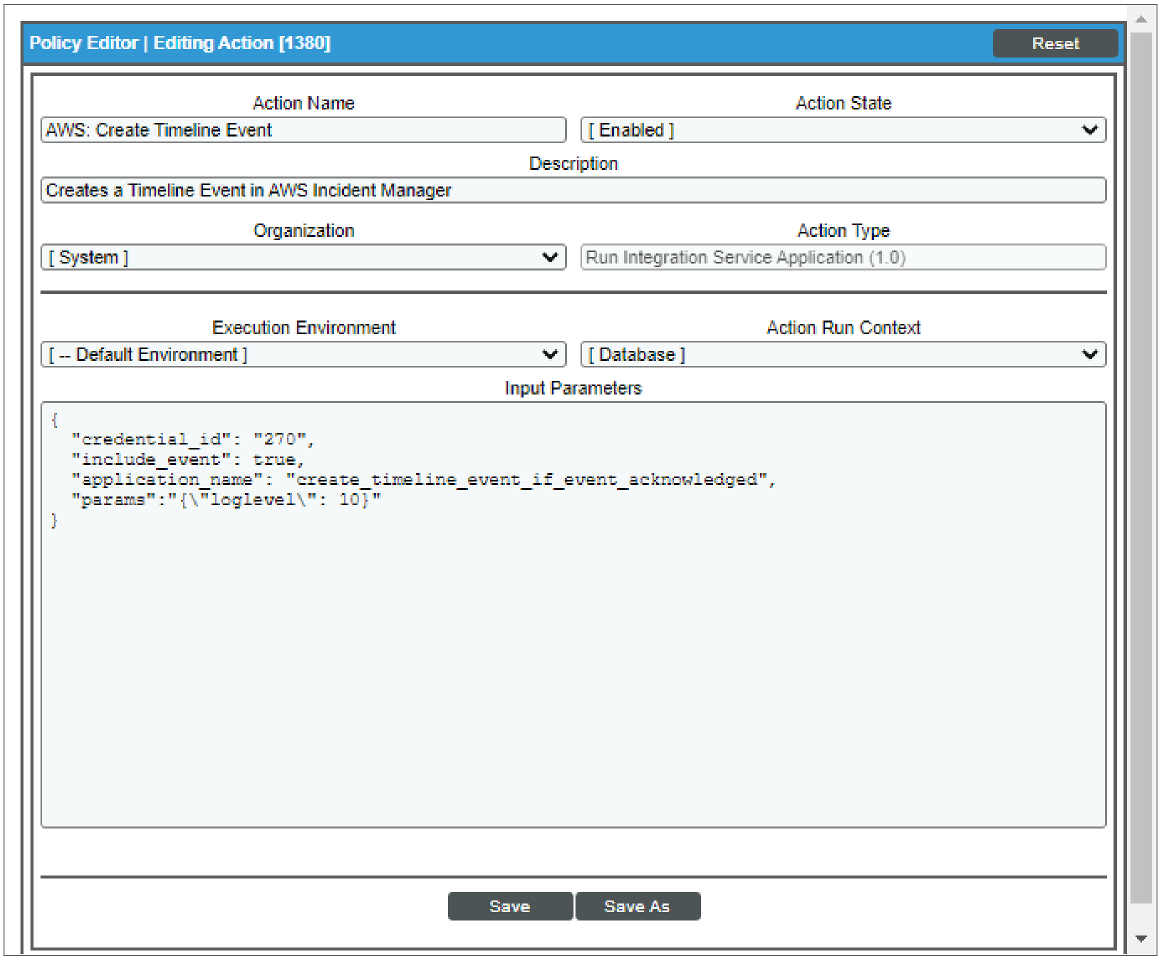
To utilize the automation included in the PowerPack, you must edit the following automation actions to communicate with your PowerFlow system:

- "AWS: Create Timeline Event"
- "AWS: Resolve Incident"
- "AWS: Trigger Incident"

To edit the automation actions included in the PowerPack:

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

2. Locate the automation action that you want to use, and then click its wrench icon (). The **Editing Action** page appears:



Action Name: AWS: Create Timeline Event

Action State: [Enabled]

Description: Creates a Timeline Event in AWS Incident Manager

Organization: [System]

Action Type: Run Integration Service Application (1.0)

Execution Environment: [-- Default Environment]

Action Run Context: [Database]

Input Parameters

```
{
  "credential_id": "270",
  "include_event": true,
  "application_name": "create_timeline_event_if_event_acknowledged",
  "params":"{\"loglevel\": 10}"
}
```

3. In the ***Input Parameters*** field, change the values of the following parameters:

   - ***credential_id***. Change the value to the credential ID that you noted earlier when creating a credential for your PowerFlow system. This field is required.
   - ***include_event***. Leave the value as "true".
   - ***application_name***. Leave the default application value.
   - ***params***. Leave the default parameter value.

4. Click **[Save]**.

Chapter

6

AWS Incident Manager Automation Policies

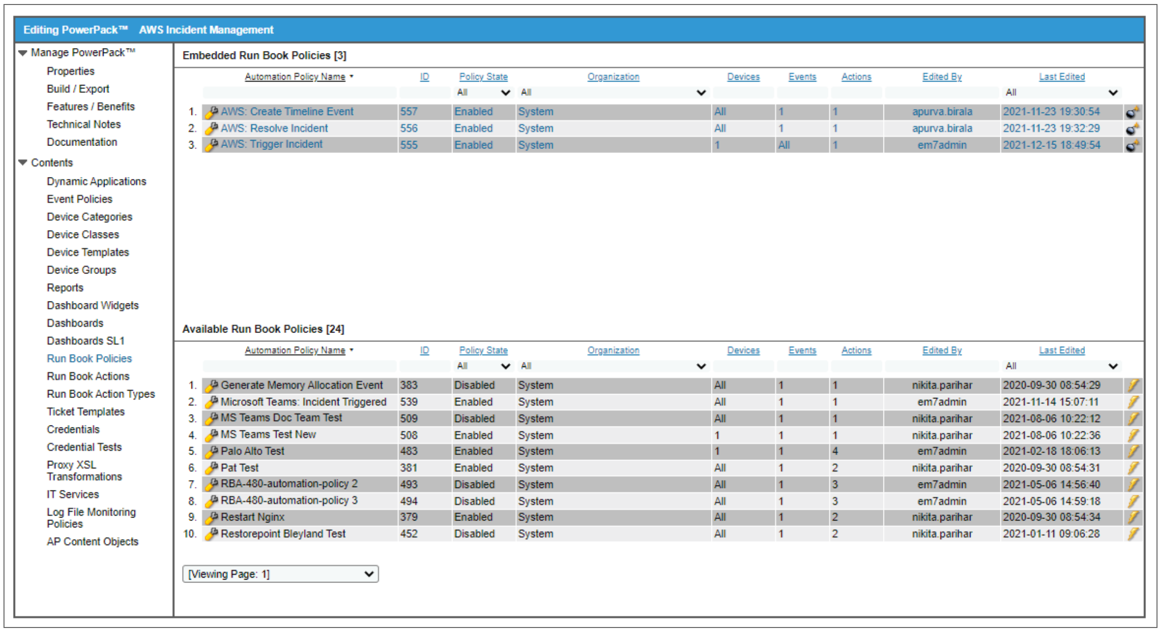
Overview

This chapter describes the automation policies found in the *AWS Incident Manager Automation* PowerPack.

This chapter covers the following topics:

Standard Automation Policies

The *AWS Incident Manager Automation* PowerPack includes three standard automation policies that you can enable, shown in the following figure. These policies update the AWS incident with the state of the event in SL1. When an event is detected in SL1, an incident is triggered in AWS. When an event is acknowledged in SL1, a timeline event is created in AWS. When an event is resolved in SL1, the incident is resolved in AWS.



Embedded Run Book Policies [3]

	Automation Policy Name	ID	Policy State	Organization	Devices	Events	Actions	Edited By	Last Edited
			All	All					All
1.	AWS: Create Timeline Event	557	Enabled	System	All	1	1	apurva.birala	2021-11-23 19:30:54
2.	AWS: Resolve Incident	556	Enabled	System	All	1	1	apurva.birala	2021-11-23 19:32:29
3.	AWS: Trigger Incident	555	Enabled	System	1	All	1	em7admin	2021-12-15 18:49:54

Available Run Book Policies [24]

	Automation Policy Name	ID	Policy State	Organization	Devices	Events	Actions	Edited By	Last Edited
			All	All					All
1.	Generate Memory Allocation Event	383	Disabled	System	All	1	1	nikita.parihar	2020-09-30 08:54:29
2.	Microsoft Teams: Incident Triggered	539	Enabled	System	All	1	1	em7admin	2021-11-14 15:07:11
3.	MS Teams Doc Team Test	509	Disabled	System	All	1	1	nikita.parihar	2021-08-06 10:22:12
4.	MS Teams Test New	508	Enabled	System	1	1	1	nikita.parihar	2021-08-06 10:22:36
5.	Palo Alto Test	483	Enabled	System	1	1	4	em7admin	2021-02-18 18:06:13
6.	Pat Test	381	Enabled	System	All	1	2	nikita.parihar	2020-09-30 08:54:31
7.	RBA-480-automation-policy 2	493	Disabled	System	All	1	3	em7admin	2021-05-06 14:56:40
8.	RBA-480-automation-policy 3	494	Disabled	System	All	1	3	em7admin	2021-05-06 14:59:18
9.	Restart Nginx	379	Enabled	System	All	1	2	nikita.parihar	2020-09-30 08:54:34
10.	Restorepoint Bleyland Test	452	Disabled	System	All	1	2	nikita.parihar	2021-01-11 09:06:28

[Viewing Page: 1]

The following table shows the automation policy, its default aligned events, and the automation action that runs in response to the events.

Automation Policy Name	Aligned Events	Automation Action
AWS: Create Timeline Event	All events	AWS: Create Timeline Event
AWS: Resolve Incident	All events	AWS: Resolve Incident
AWS: Trigger Incident	All events	AWS: Trigger Incident

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

ScienceLogic

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

International: +1-703-354-1010