



AWS Incident Manager SyncPack

Version 1.0.0

Table of Contents

Introduction to the AWS Incident Manager SyncPack	3
What Can I Do with this SyncPack?	4
Contents of the SyncPack	4
PowerFlow Applications	4
Configuration Object	5
Steps	5
Installing the AWS Incident Manager SyncPack	6
Prerequisites for this SyncPack	7
Installing the SyncPacks	7
Downloading the SyncPacks	7
Importing the SyncPacks	8
Installing the SyncPack	8
Installing the AWS Incident Manager Automation PowerPack	9
Configuring Applications for the AWS Incident Manager SyncPack	10
Workflow for Configuring the SyncPack	11
Configuring SL1	11
Configuring PowerFlow	11
Configuring SL1	11
Creating a SOAP/XML Credential to Access PowerFlow	11
Editing the AWS Incident Manager Run Book Actions	12
Enabling the AWS Incident Manager Run Book Automations	12
Configuring PowerFlow	13
Creating a Configuration Object	13
Aligning a Configuration Object and Configuring PowerFlow Applications	15
Scheduling PowerFlow Applications	16

Chapter

1

Introduction to the AWS Incident Manager SyncPack

Overview

This chapter describes how you can use the "AWS Incident Manger" SyncPack to automatically synchronize SL1 events and Amazon Web Services (AWS) incidents between your AWS and SL1 systems.

This SyncPack uses the "AWS Incident Manager Automation" PowerPack and the "AWS Base" SyncPack.

This chapter covers the following topics:

<i>What Can I Do with this SyncPack?</i>	4
<i>Contents of the SyncPack</i>	4

What Can I Do with this SyncPack?

The "AWS Incident Manager" SyncPack lets you configure PowerFlow to automatically synchronize SL1 events and incidents generated with AWS Incident Manager. The integration is bidirectional between AWS Incident Manager and SL1 systems.

This SyncPack includes the following PowerFlow applications:

- **Send SL1 Event to AWS Incident Manager.** Sends SL1 event information to the AWS console. The application takes SL1 event data as input and makes a request to the AWS Incident Manager. Based on the input parameters, the request to the AWS API does one of the following:
 - Sends event details to AWS incident manager
 - Incident Manager contact channels will be created and send email/message
 - All the target actions in AWS services to be validated for each use case
- **Bulk Resolve SL1 Events From AWS.** Receives input from a user action in the AWS Console, such as "resolving" an incident, and shares the action being performed, the SL1 instance information and the Event ID. This application clears the SL1 event in the specified SL1 instance based on the resolution on AWS incident manager.

Contents of the SyncPack

This section lists the contents of the "AWS Incident Manager" SyncPack.

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 SyncPack 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 SyncPack:

- 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

Chapter

2

Installing the AWS Incident Manager SyncPack

Overview

This chapter describes how to install the "AWS Incident Manager" SyncPack, as well as the "AWS Incident Manager Automation" PowerPack and the "AWS Base" SyncPack.

This chapter covers the following topics:

<i>Prerequisites for this SyncPack</i>	7
<i>Installing the SyncPacks</i>	7
<i>Installing the AWS Incident Manager Automation PowerPack</i>	9

Prerequisites for this SyncPack

This SyncPack requires the following:

- The latest "AWS Base" SyncPack
- The latest "SL1 Base Notifications" SyncPack
- The latest "AWS Incident Manager" Automation PowerPack

For the latest System Requirements, see the [SL1 PowerFlow SyncPack Release Notes](#).

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

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

Installing the SyncPacks

A SyncPack file has the `.whl` file extension type. You can download the SyncPack file from the ScienceLogic Support site.

NOTE: You must download and install the "AWS Base" SyncPack before downloading and installing the "AWS Incident Manager" SyncPack. You can download and install the "SL1 Base Notifications" SyncPack before or after the other two SyncPacks.

Downloading the SyncPacks

NOTE: If you are installing or upgrading to the latest version of this SyncPack in an offline deployment, see [Installing or Upgrading in an Offline Environment](#) to ensure you install any external dependencies.

To locate and download the SyncPack:

1. Go to the ScienceLogic Support Site at <https://support.sciencelogic.com/s/>.
2. Click the **[Product Downloads]** tab and select *PowerPacks & SyncPacks*.
3. In the **Search** field, search for the SyncPack and select it from the search results. The **Release Version** page appears.

4. On the **[Files]** tab, click the down arrow next to the SyncPack version that you want to install, and select *Show File Details*. The **Release File Details** page appears.
5. Click the **[Download File]** button to download the SyncPack.

After you download the SyncPack, you can import it to your PowerFlow system using the PowerFlow user interface.

Importing the SyncPacks

To import a SyncPack 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 SyncPack you want to install. You can also drag and drop a **.whl** file to the **Import SyncPack** page.
3. Click **[Import]**. PowerFlow registers and uploads the SyncPack. The SyncPack is added to the **SyncPacks** page.
4. You will need to activate and install the SyncPack in PowerFlow. For more information, see the following topic.

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

Installing the SyncPack

To activate and install a SyncPack in the PowerFlow user interface:

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

NOTE: If you try to activate and install a SyncPack 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 SyncPack is activated, the **SyncPacks** page displays a green check mark icon (✓) for that SyncPack. 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 SyncPack. 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 SyncPack on your PowerFlow system, you can click the **[Actions]** button (⋮) for that SyncPack and select *Change active version* to activate a different version other than the version that is currently running.

Installing the AWS Incident Manager Automation PowerPack

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

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 the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the [ScienceLogic Support Site](#).
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** 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

3

Configuring Applications for the AWS Incident Manager SyncPack

Overview

This chapter describes how to set up the PowerFlow applications for the "AWS Incident Manager" SyncPack. This chapter also covers how to configure the "AWS Incident Manager Automation" PowerPack and the "AWS Base" SyncPack.

This chapter covers the following topics:

<i>Workflow for Configuring the SyncPack</i>	11
<i>Configuring SL1</i>	11
<i>Configuring PowerFlow</i>	13

Workflow for Configuring the SyncPack

The following workflows describe how to configure SL1 and PowerFlow to work with the "AWS Incident Manager" SyncPack.

Configuring SL1

1. [Create a SOAP/XML credential to access PowerFlow](#)
2. [Edit the AWS Incident Manager run book actions](#)
3. [Enable the AWS Incident Manager run book automations](#)

Configuring PowerFlow

1. [Create and align a PowerFlow configuration object](#)
2. [Configure the PowerFlow applications](#)
3. [Schedule the PowerFlow applications](#)

Configuring SL1

The following topics cover how to set up your SL1 instance to work with the "AWS Incident Manager" SyncPack.

Creating a SOAP/XML Credential to Access PowerFlow

You will need to create a SOAP/XML credential in SL1 so that the automation actions included in the PowerPack can access your PowerFlow system.

To create a SOAP/XML credential:

1. In SL1, go to the **Credentials** page (Manage > Credentials).
2. Click **[Create New]** and select *Create SOAP/XML Credential*. The **Create Credential** window appears.
3. Complete the following fields:
 - **Name**. Type a new name for the credential.
 - **All Organizations**. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations.
 - **URL**. Type the URL for your PowerFlow system.
 - **HTTP Auth User**. Type the username for your PowerFlow system.
 - **HTTP Auth Password**. Type the password for your PowerFlow system.

4. Click **[Save & Close]**.
5. Take note of the SL1-assigned ID number for the new credential on the **Credentials** page, in the **ID** column. You will need the ID number when editing the input parameters of the run book actions included in the PowerPack, below.


Editing the AWS Incident Manager Run Book Actions

The "AWS Incident Manager Automation" PowerPack includes run book 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.

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

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

To edit the run book actions included in the PowerPack:


1. Go to the **Actions** page (Registry > Run Book > Actions).
2. Locate the AWS run book action that you want to use, and then click its wrench icon (). The **Editing Action** page appears.
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 in the previous procedure 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. Make sure the **Action State** is set to *Enabled*, and then click **[Save]**.

Enabling the AWS Incident Manager Run Book Automations

The "AWS Incident Manager" PowerPack includes three run book automation policies that you will need to enable:

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

To enable the run book automations:

1. In SL1, go to the **Automations** page (Registry > Run Book > Automation).
2. Locate the "AWS: Create Timeline Event" automation policy and click its wrench icon (). The **Automation Policy Editor** page appears.
3. Update the following fields:
 - **Policy State**. Select *Enabled*.
 - **Policy Priority**. Select *High* to ensure that this PowerFlow automation policy is added to the top of the queue.
 - **Available Actions**. If it is not already selected, select "Run Integration Service Application: Ansible:Command" (or "Ansible: Tower" for the "Ansible: Tower" automation policy) and click the arrows to move it to **Aligned Actions**.


WARNING: ScienceLogic highly recommends that you do not make changes to the **Policy Type, Repeat Time, or Align With** fields or the *And event is NOT acknowledged* setting.

4. Click **[Save]**.
5. Repeat steps 2-4 for the "AWS: Resolve Incident" and "AWS: Trigger Incident" run book automation policy.

Configuring PowerFlow

The following topics cover how to set up your PowerFlow instance to work with the "AWS Incident Manager" SyncPack.

Creating a Configuration Object

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 SyncPack, 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.

For this SyncPack, 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" SyncPack.

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.
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::XXXXXXXXX: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 SyncPack, 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 SyncPack, 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.
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. 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 so it runs on a regular basis.

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 create a schedule:

1. On the **Applications** page (📄), click the **[Schedule]** button for the application you want to schedule. The **Scheduler** window appears.
2. In the **Schedule List** pane, click the down arrow icon (▼) next to an existing schedule to view the details for that schedule.
3. In the **Schedule Creator** pane, complete the following fields for the default **Frequency** setting:
 - **Schedule Name.** Type a name for the schedule.
 - **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.
4. To use a cron expression, click the **Switch to Cron Expression** toggle to turn it blue. 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:

Schedule Creator
Switch to Frequency in Seconds

For more information about schedules, see [schedules documentation](#).

Schedule Name
Saturday Schedule

A unique name for the new schedule.

Cron Expression key operators

* any value , list separator - range of values / step values

Minutes 0,30	Hours *	Day of Month *	Month *	Day of Week 6
Allowed values: 0-59	Allowed values: 0-23	Allowed values: 1-31	Allowed values: 1-12 Alt. values JAN-DEC	Allowed values: 0-6 Alt. values SUN-SAT

Runs app: "Every 0 and 30th minute past every hour on Sat" (UTC -4)

Derived from given values in fields above.

Custom Parameters (Optional)

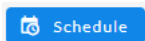
1	{ }
---	-----

Overrides default application variables for ad-hoc execution settings. Any application variable may be specified, and overridden per run here. Special properties like "queue" may also be set here.

Close Save Schedule

As you update the cron expression, the **Schedule** window displays the results of the expression in more readable language, such as *Runs app: "Every 0 and 30th minute past every hour on Sat"*, based on 0,30 in the **Minutes** field and 6 in the **Day of Week** field.



- Click **[Save Schedule]**. The schedule is added to the **Schedule List** pane. Also, on the **Applications** page, the **[Schedule]** button now displays with a dark blue background:



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:

- On the **Applications** page, click the **[Schedule]** button for the application that contains a schedule you want to delete. The **Scheduler** window appears.

2. Click the down arrow icon () to view the details of an existing schedule.
3. To delete the selected schedule, click the Actions icon () and select **[Delete]**.

TIP: On the **Scheduler** window for a PowerFlow application, you can click the **[Copy as]** button from the **Schedule List** pane to make a copy of an existing schedule.

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 SyncPack for the purpose of distinguishing between domains is not supported, and will result in issues on upgrades.

© 2003 - 2024, 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. For more information, see <https://sciencelogic.com/company/legal>.

ScienceLogic

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

International: +1-703-354-1010