ScienceLogic

ServiceNow Incidents SyncPack

Version 4.1.2, rev 4

Table of Contents

Introduction to the ServiceNow Incidents SyncPack	. 4
What Can I Do with this SyncPack?	
Contents of the SyncPack	. 5
PowerFlow Applications	. 5
PowerFlow Application (Internal)	
Installing and Configuring the Incidents SyncPack	
Architecture Overview for ServiceNow SyncPacks	8
SL1 and ServiceNow Terminology	9
Dependency Map for ServiceNow SyncPacks	. 9
Prerequisites for ServiceNow SyncPacks	
Downloading, Importing, and Installing the ServiceNow Incident SyncPack	.10
Downloading the SyncPack	
Importing the SyncPack	
Installing the SyncPack	
Migrating from the "ScienceLogic SL1: CMDB & Incident Automation" Application to the "ScienceLogic	
SL1: Incident Automation" Application	.12
Installing the "ScienceLogic SL1: Incident Automation" Application in ServiceNow	.13
Installing the ServiceNow Base Pack PowerPack in SL1	
Validating Network Communications	
Checking DNS	
Checking HTTPS and JSON	
HTTP Codes	
Configuring Applications for the Incidents SyncPack	
Workflow for Configuring the SyncPack	
Configuring ServiceNow	
Configuring SL1	
Configuring PowerFlow	
Overview of the Run Book Automation for Incident Sync	
Configuring ServiceNow	
Configuring SL1	
Creating a ServiceNow Credential in SL1	
Enabling the Run Book Automation Policies	
Enabling and Customizing the Run Book Action Policy	
Customizing the Snippet Code in the Input Parameters Pane	
Customizing Logging in the Run Book Action	
Sending Custom Data to ServiceNow Using the Passthrough Option	
Passing Custom Data to ServiceNow	
Passthrough Example	
Snippet Code Example	
Configuring the "ServiceNow: Click to Create Incident" Automation Policy	
Enabling Run Book Automation Queue Retries	
Configuring PowerFlow	
Creating a Configuration Object	
Configuring the PowerFlow Applications	
Scheduling PowerFlow Applications	
Incident Topology Suppression	
Additional Options in ServiceNow	
Viewing Events with ServiceNow	
Hyperlinking Events	
Viewing the Incident Import Table in ServiceNow	. 46

SL1 Event to ServiceNow Incident Impact/Urgency Matrix	
Adding Additional Fields to the Transform Map	50
Troubleshooting the Incidents SyncPack	
Initial Troubleshooting Steps	
SL1 PowerFlow	
ServiceNow	57
Resources for Troubleshooting	
Useful PowerFlow Ports	
Helpful Docker Commands	58
Viewing Container Versions and Status	
Restarting a Service	
Stopping all PowerFlow Services	
Restarting Docker	
Diagnosis Tools	58
Retrieving Additional Debug Information (Debug Mode)	
Frequently Asked Questions	
Why are Incidents not getting created in ServiceNow?	62
What if my Incident does not have a CI?	
What if the PowerFlow user interface is unresponsive and Incidents are not being generated in	
ServiceNow?	63
Why are Incident numbers not populated in SL1 on Incident creation in ServiceNow?	
Why am I not getting any Incidents after disabling the firewall?	

Chapter

Introduction to the ServiceNow Incidents SyncPack

Overview

This chapter describes the "ServiceNow Incidents" SyncPack, which lets you sync ServiceNow incidents with SL1 events.

This SyncPack uses the "ScienceLogic SL1: Incident Automation" certified application in ServiceNow and the latest "ServiceNow Base Pack" PowerPack in SL1.

Do not use this SyncPack and the "ServiceNow Events" or the "ServiceNow Cases" SyncPacks on the same PowerFlow system. This SyncPack is compatible with the "ServiceNow Service Graph Connector" SyncPack, version 1.0.0 or later and the "ServiceNow CMDB" SyncPack version 3.0.0 or later.

This chapter covers the following topics:

What Can I Do with this SyncPack?	5
Contents of the SyncPack	. 5

What Can I Do with this SyncPack?

The "ServiceNow Incidents" SyncPack is the ScienceLogic integration with the ServiceNow Incident Management Module, and you can use this SyncPack to sync SL1 events with ServiceNow incidents.

This SyncPack automatically logs, de-duplicates, correlates, updates, and appends ServiceNow incidents, reducing the amount of time to resolve critical service issues. This SyncPack covers the entire incident life cycle, providing a bi-directional integration between SL1 events and ServiceNow incidents, while providing a granular view into both the event and the associated incident.

For this SyncPack, you can configure a run book action policy in SL1 to ensure that whenever SL1 detects a new, acknowledged, or cleared event, a corresponding incident is created or updated in ServiceNow. These automations are included in the latest "ServiceNow Base Pack" PowerPack. For more information, see Overview of the Run Book Automation for Incident Sync.

This SyncPack includes the following applications, which you can use to synchronize event and incident information between SL1 to ServiceNow:

- Sync Incident Details from ServiceNow to SL1 Events. Acknowledges or clears SL1 events from ServiceNow, updates the user note, and populates the incident number in the external ticket reference.
- Sync SL1 Event to ServiceNow Incident. The "ServiceNow: Add/Update/Clear Incident" Run Book Action policy triggers this application whenever an SL1 event is created, updated, or cleared. This application processes the SL1 event, caches it to PowerFlow to allow for bulk processing for ServiceNow by the "Sync Cached Events to ServiceNow" application, and then sends a status update to SL1.

For more information about how to configure these applications, see **Configuring the PowerFlow Applications**.

Contents of the SyncPack

This section lists the contents of the "ServiceNow Incidents" SyncPack.

PowerFlow Applications

The following PowerFlow applications are included with the "ServiceNow Incidents" SyncPack:

• Sync Cached Events to ServiceNow. Bulk processes all of the cached SL1 Events and posts them to ServiceNow. Sends a "Sync Success" or "Sync Failed" status update to PowerFlow based on the result of the post. ScienceLogic recommends that you schedule this application to run every 60 seconds or longer.

• Sync Incident Details from ServiceNow to SL1 Events. Acknowledges or clears SL1 Events from ServiceNow, updates the user note, and populates the incident number in the external ticket reference. This application also include the new user_note_template field that accepts a Jinja2 template to generate custom user notes. ScienceLogic recommends that you schedule this application to run every 60 seconds.

NOTE: In previous releases of this SyncPack, this application was named the "Sync Incident State from ServiceNow to SL1 Event" application.

• Sync SL1 Event to ServiceNow Incident. The "ServiceNow: Add/Update/Clear Incident" Run Book Action triggers this application whenever an SL1 Event is created, updated, or cleared.

NOTE: This application processes the SL1 event, caches it to PowerFlow to allow for bulk processing for ServiceNow by the "Sync Cached Events to ServiceNow" application, and then sends a status update to SL1.

For more information, see Configuring the PowerFlow Applications for the Incidents SyncPack.

The following PowerFlow applications from previous versions of this SyncPack have been deprecated:

- Create or Update ServiceNow Incident from SL1 Event
- Sync Incident State from ServiceNow to SL1 Event
- Update ServiceNow Incident when SL1 Event is Acknowledged
- Update ServiceNow Incident when SL1 Event is Cleared

You should uninstall previous versions of this SyncPack to make sure that these applications and any other configurations have been removed.

PowerFlow Application (Internal)

To view the internal PowerFlow application, click the Filter icon ($\overline{\overline{}}$) on the **Applications** page and select Show Hidden Applications. Internal applications are hidden by default. The following application is "internal" and should not be run directly. Instead, it is automatically run by applications from the previous list:

• Bulk Update SL1 Events. Bulk updates SL1 events with a given payload.

Chapter

2

Installing and Configuring the Incidents SyncPack

Overview

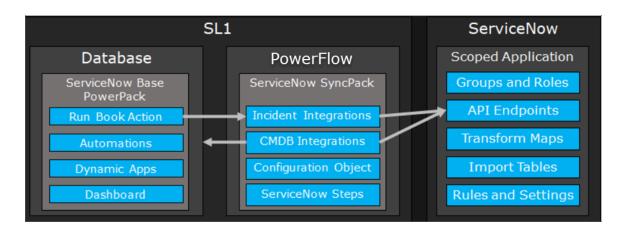
This chapter describes the how to install and configure the "ServiceNow Incidents" SyncPack and the other applications needed to use the SyncPack, including the "ScienceLogic SL1: Incident Automation" application and the "ServiceNow Base Pack" PowerPack.

This chapter covers the following topics:

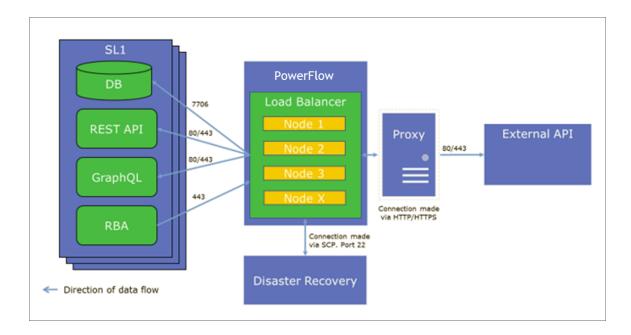
Architecture Overview for ServiceNow SyncPacks	. 8
SL1 and ServiceNow Terminology	. 9
Dependency Map for ServiceNow SyncPacks	. 9
Prerequisites for ServiceNow SyncPacks	. 9
Downloading, Importing, and Installing the ServiceNow Incident SyncPack	10
Installing the "ScienceLogic SL1: Incident Automation" Application in ServiceNow	13
Installing the ServiceNow Base Pack PowerPack in SL1	14
Validating Network Communications	10

Architecture Overview for ServiceNow SyncPacks

The following diagram details the various elements that are contained in SL1 and the PowerFlow system, and how PowerFlow sits between the core SL1 platform and an external data platform:



The following diagram provides an example of the high-level architecture of a PowerFlow system with High Availability, Disaster Recovery, and a proxy configured:



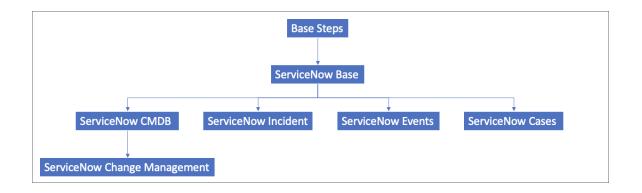
SL1 and ServiceNow Terminology

The following table lists the different names for the shared elements in SL1 and ServiceNow:

SL1	ServiceNow
Asset, Custom Attribute	Asset (ITAM)
Device	CI (Configuration Item)
Discovery Session	Service Request, Catalog Request
Event	Incident, Event, or Case (depending on the SyncPack you are using)
Alert	Event
Organization	Company, Domain
Schedule, Maintenance Schedule	Change Request, Change Schedule
Topology, Relationships, Dynamic Component Mapping and Relationships (DCM+R)	Dependency View, Affected Cls

Dependency Map for ServiceNow SyncPacks

The following graphic describes which SyncPacks depend on other SyncPacks:



TIP: For more information about the "Base Steps" SyncPack, see the SL1 PowerFlow Platform manual.

Prerequisites for ServiceNow SyncPacks

This section describes the prerequisites for the ServiceNow SyncPacks. For more information about the specific software versions required by a ServiceNow SyncPack, see the release notes for that SyncPack.

To install any of the ScienceLogic ServiceNow SyncPacks, you must have administrator access to both SL1 and ServiceNow. Specifically, you will need:

- ScienceLogic administrator access to the Administration Portal
- ServiceNow administrator access

If you want to upload and install multiple ServiceNow SyncPacks at the same time, you should upload *all* of the SyncPacks first, and then install them to address any dependencies between the SyncPacks.

WARNING: ScienceLogic does not support any deployment that attempts to sync one SL1 instance to multiple ServiceNow instances. A deployment of this type will be incredibly fragile and would require the customer to strictly control their environments. This is not something that can be controlled programmatically. Escalations related to this type of deployment are not supported.

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	ServiceNow API	Any	TCP 443	ServiceNow API Access
SL1 Run Book Action	PowerFlow	Any	TCP 443	Send SL1 data to PowerFlow

Downloading, Importing, and Installing the ServiceNow Incident SyncPack

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

NOTE: If you are using an older version of the ServiceNow Incident SyncPack, you should uninstall that version in the PowerFlow user interface before installing this release. Uninstalling ensures that all deprecated applications and configurations have been removed from your system.

NOTE: If you are upgrading from a previous version of this SyncPack and you want to keep your settings from the existing "ScienceLogic SL1: CMDB & Incident Automation" application, see Migrating from the "ScienceLogic SL1: CMDB & Incident Automation" Application to the "ScienceLogic SL1: Incident Automation" Application.

Downloading the SyncPack

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

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.
- 3. In the **Search PowerPacks** 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 SyncPack

NOTE: You must import and install the ServiceNow Base SyncPack before uploading and installing any of the other ServiceNow 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.

TIP: 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.

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.

- 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 (
- 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.

Migrating from the "ScienceLogic SL1: CMDB & Incident Automation" Application to the "ScienceLogic SL1: Incident Automation" Application

This section explains how to upgrade from the existing "ScienceLogic SL1: CMDB & Incident Automation" application to the new "ScienceLogic SL1: Incident Automation" application with version 4.0.0 and later of this SyncPack.

Both applications include the following functionality:

- 1. Create, update, or clear a ServiceNow Incident from an SL1 Event
- 2. Sync Incident State from a ServiceNow to an SL1 Event

These applications do not share any tables or fields within ServiceNow.

This section highlights some considerations when transferring to the Incident only application (version 4.0.0 or later of this SyncPack). Any customizations you made in another Certified Application do not carry over to other Certified Applications, even when both are provided by the same vendor. You will need to adapt customizations made previously so they can work within this new application.

Considerations:

- The Correlation ID (correlation _type in the Run Book Action Input Parameters) is no longer set in SL1 or PowerFlow. With the new application, the Correlation ID is set in the transformation map within ServiceNow. The preset Correlation IDs that were provided in past applications are also included and can be set by using the Properties page in the ServiceNow Application. You can address custom behavior within the transformation map.
- 2. The Incident "onBefore" script addresses *Impact* and *Urgency* states. You will most likely need to customize the default behavior for these states to meet your requirements.
- 3. The Incident "onBefore" script also addresses cleared event behavior, and you will need to evaluate and customize this behavior to fit your requirements.

Installing the "ScienceLogic SL1: Incident Automation" Application in ServiceNow

Version 4.0.0 or later of the "ServiceNow Incidents" SyncPack uses "ScienceLogic SL1: Incident Automation" application in ServiceNow to sync incident status update from ServiceNow back to SL1. You can access the application from the ServiceNow Store. This application is also known as the "Certified Application" or the "Scoped Application".

Versions of this SyncPack before 4.0.0 used the "ScienceLogic SL1: CMDB & Incident Automation" application, but that application is not supported with version 4.0.0 or later.

NOTE: You must have a ServiceNow HI Service Account to request this application and download it onto your ServiceNow instance.

You must first request the "ScienceLogic SL1: Incident Automation" application from the ServiceNow Store, and then you can install it.

To request and install the Certified Application:

- 1. Go to the ServiceNow Store at https://store.servicenow.com and search for "ScienceLogic SL1".
- 2. Select the "ScienceLogic SL1: Incident Automation" application. The detail page for the application appears.
- 3. Click the [Get] button and log in with your HI credentials.

- 4. After the request is approved, log in to ServiceNow as an administrator and navigate to **Application Manager** (System Applications > Applications or My Company Applications).
- 5. Click [Downloads] in the menu header or search for "ScienceLogic".
- 6. Click the version drop-down for the "ScienceLogic SL1: Incident Automation" application listing to make sure you are using the correct version of the application that is compatible with your version of this SyncPack.
- 7. Click the **[Install]** button for the application. The installation is complete when the button changes to **[Installed]**.
- 8. In the filter navigator, search for "ScienceLogic" and locate the application in the left-hand navigation menu to verify that the application was installed.

NOTE: You might need to log out of ServiceNow and log in again to see the updated left-hand navigation menu.

Installing the ServiceNow Base Pack PowerPack in SL1

The "ServiceNow Base Pack" PowerPack monitors the ServiceNow Incident and CMDB tables, and it returns information about Incident types, priorities, and states, displaying the information in an easy-to-consume dashboard. This PowerPack is a critical component of the Incident Sync Integration with ServiceNow, using Run Book Automations to integrate with ServiceNow.

TIP: By default, installing a new version of a PowerPack overwrites all content in 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 install the "ServiceNow Base Pack" PowerPack:

- 1. Search for and download the "ServiceNow Base Pack" PowerPack from the **PowerPacks** page at the ScienceLogic Support Site at https://support.sciencelogic.com/s/.
- 2. In SL1, go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 3. Click the Actions menu and choose Import PowerPack. The Import PowerPack modal appears.
- 4. Click [Browse] and navigate to the "ServiceNow Base Pack" PowerPack file from step 1.
- 5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal page displays a list of the PowerPack contents.
- 6. Click **[Install]**. After the installation is complete, the "ServiceNow Base Pack" PowerPack appears on the **PowerPack Manager** page.

Validating Network Communications

All communication between SL1 and ServiceNow is done through TCP port 443. To allow communication between SL1 and ServiceNow, the SL1 Database Server, Data Collector, or All-In-One Appliance must have external access to the ServiceNow instance. No inbound TCP ports are required to be open to the SL1 server. Outbound communication may use NAT or be direct.

NOTE: All firewall session-limiting policies must be disabled. If firewall session-limiting policies are enabled, HTTPS requests might be dropped by the firewall, resulting in data loss. Check with your security or firewall administrator to make sure there are no session limiting policies on TCP port 443 for your SL1 servers.

Checking DNS

Because ServiceNow is a cloud-based service, DNS must be configured on all SL1 servers that communicate with your ServiceNow instance.

NOTE: ServiceNow instances are generally named as: *your-instance.service-now.com*, where *your-instance* is the name of your ServiceNow server. The examples below use *mycompany.service-now.com*. Your instance name will be unique to your subscription.

To validate that your SL1 server has proper DNS name resolution configured, test network connectivity and name resolution using the nmap command, which is available from the command line of any SL1 server:

nmap -sT -p 443 mycompany.service-now.com

If the test was successful, you will see a message similar to the following:

```
Starting Nmap 5.51 ( http://nmap.org ) at 2013-11-12 20:22 UTC
```

Nmap scan report for mycompany.service-now.com (199.91.136.100)

Host is up (0.067s latency).

PORT STATE SERVICE

443/tcp open https

If domain name resolution fails, you will see a message similar to:

Failed to resolve given hostname/IP: mycompany.service-now.com.

Checking HTTPS and JSON

You can administer a simple test to determine if the ServiceNow JSON Plug-in web service is configured and operating using the Basic Authentication method on your ServiceNow instance. To do so, run the following command from the ScienceLogic Central Database or All-In-One Appliance:

NOTE: In the example below, replace the admin:admin username and password key/value pair with your ServiceNow administrator username and password and mycompany.service-now.com with your ServiceNow instance name.

```
curl --location -vu admin:admin -H "Accept: application/json" -H "Content-
Type: application/json"
```

'https://mycompany.service-now.com/api/now/table/incident'

If not successful, the following message appears:

HTTP/1.1 401 Unauthorized

If successful, a JSON encoded string starting with the "result" variable appears:

```
{"result":[{"upon_
approval":"","location":"1083361cc611227501b682158cabf646",....
```

HTTP Codes

HTTP codes are necessary for identifying specific problems. The following table lists typical HTTP codes that might occur when testing the ServiceNow JSON Web Service.

Code	Definition
401	Unauthorized. Check that the username and password are correct and properly formatted.
403	Forbidden. ServiceNow understood the request, but either the URL is incorrect, or the user account does not have permission to see the requested object.
404	The ServiceNow server has not found anything matching the requested URL. Check to make sure there is data in the target table.
200	Success.
201	Success. Data is posted.

TIP: For more information about the ServiceNow JSON Web Service and the Table API, see http://wiki.servicenow.com/index.php?title=Table_API. If you continue to have problems, please contact either ScienceLogic or ServiceNow customer support.

Chapter



Configuring Applications for the Incidents SyncPack

Overview

This chapter describes the how to configure and run the various PowerFlow applications and SL1 run book automations contained in the "ServiceNow Incidents" SyncPack.

After you align the PowerFlow applications in this SyncPack with the corresponding run book automation in SL1, whenever SL1 detects a new, acknowledged, or cleared event, PowerFlow creates or updates a corresponding incident in ServiceNow.

This chapter covers the following topics:

Workflow for Configuring the SyncPack	19
Configuring ServiceNow	21
Configuring SL1	22
Configuring PowerFlow	32
Additional Options in ServiceNow	. 45

Workflow for Configuring the SyncPack

The following workflows describe how to configure ServiceNow, SL1 and PowerFlow to work with Incident Sync.

Configuring ServiceNow

Use the Guided Setup process to configure an integration user account, configure an SL1 Incident Integration Application role, and connect to PowerFlow.

Configuring SL1

- 1. Create a ServiceNow credential in SL1
- 2. Enable the following run book automation policies in SL1:
 - "ServiceNow: [Incident] Add/Update"
 - "ServiceNow: [Incident] Event Acknowledged"
 - "ServiceNow: [Incident] Event Cleared
- 3. Enable and customize the "ServiceNow: Add/Update/Clear Incident" run book action policy
- 4. Optionally, send custom data to ServiceNow using the passthrough option
- 5. Optionally, enable and configure the "ServiceNow: Click to Create Incident" policy
- 6. Optionally, enable run book automation queue retries

Configuring PowerFlow

- 1. Create a configuration object in the PowerFlow user interface
- 2. Configure the following PowerFlow applications:
 - "Cache SL1 Users"
 - "Sync Cached Events to ServiceNow"
 - "Sync SL1 Event to ServiceNow Incident"
 - "Sync Incident Details from ServiceNow to SL1 Events"
- 3. Schedule the PowerFlow applications as needed

Overview of the Run Book Automation for Incident Sync

You can configure a run book automation to ensure that whenever SL1 detects a new, acknowledged, or cleared event, a corresponding incident is created or updated in ServiceNow.

The "ServiceNow: Add/Update/Clear Incident" run book action policy is responsible for sending the SL1 payload to PowerFlow. PowerFlow then sends that payload to ServiceNow and creates, updates, acknowledges, or clears an incident, as needed.

SL1 features three run book automation policies that facilitate this process:

- ServiceNow: [Incident] Add/Update
- ServiceNow: [Incident] Event Acknowledged
- ServiceNow: [Incident] Event Cleared

NOTE: A fourth run book automation policy, "ServiceNow: [Incident] Click to Create" lets you manually create an incident in ServiceNow by clicking the life-preserver icon (⁽²⁾) in SL1. For more information, see Configuring the "ServiceNow: [Incident] Click to Create" Automation Policy.

NOTE: The "Sync Incident State from ServiceNow to SL1 Event" application does not have an associated run book action that triggers Incident Sync. You must schedule this application to run every minute, or to a time suitable for your requirements. You can use a cron job to trigger this schedule, or you can use the PowerFlow user interface to schedule the application. For more information about scheduling, see the "Scheduling a PowerFlow Application" topic in the Managing PowerFlow Applications chapter of the **SL1 PowerFlow Platform** manual.

Each run book automation policy calls a single action in SL1. Ensure that the configuration object aligned with the PowerFlow application points to the relevant SL1 system and ServiceNow instance. The run book action then calls a PowerFlow application that determines the workflow to execute.

Events in SL1 frequently occur and resolve due to fluctuations in the network and other changing conditions. However, the run book automation policies above use a de-duplication algorithm to ensure that only a single open ServiceNow incident exists per device.

If a device already has an existing ServiceNow incident, the following updates are made:

- The "Work Notes" is updated when there is an Acknowledge action.
- Impact and Urgency are updated, if they are different.
- The State is updated, and the **Assigned to** field is cleared when an incident state moves from Resolved to In Progress.
- If an event is cleared in SL1 and then later reoccurs before the incident has been "Closed" in ServiceNow, then the subsequent events appear in the original ServiceNow incident record for that device. If an incident record has been "Closed," then ServiceNow will create a new incident record when a cleared event reoccurs in SL1.

• By default, if an event is acknowledged in SL1, the ServiceNow incident record will be updated with the work notes and the acknowledging user. Clearing an SL1 event will move the ServiceNow incident record state to "Resolved". If all SL1 events associated with a ServiceNow incident record are clear, the ServiceNow incident record will, by default, move to a "Resolved" state.

NOTE: You can edit the snippet code in the run book action to adjust the behavior for changing states when an SL1 event is acknowledged or cleared. For more information, see *Customizing the Snippet Code in the Input Parameters Pane*.

Configuring ServiceNow

In ServiceNow, you can use the Guided Setup process to configure an integration user account, configure an SL1 Incident Integration Application role, and connect to PowerFlow.

To use the Guided Setup process in ServiceNow

1. In ServiceNow, go to ScienceLogic SL1: Incident Automation > Guided Setup. The ScienceLogic Integration with Incident page appears:

Servicence. Service Management			D Defau	alt (Glob 🗸 🔚 Global 🗸 🥘 System Administrator - 🔍 🕮 🕐 🗔
♥ incident automation ● ▶ ● ▶ ● Sciencet right SL1: Incident Automation Guided Samp Support incident Properties Settings ♥ Levet	0% Complete	ScienceLogic Integration	with Incident Setup Integration Account Setup the inbound integration user account. For the most current <u>SeturceLogic Documentations</u> .	Filter Stow all
¥ import Imports Transform Mags	¥ Import Imports:	Status: Not Started	Powerflow Setup Step For the most current <u>ScienceLogic Documentations</u> . WARNING: This setup requires a setup PowerFlow system.	O / 5 Tasks completed Install SyncFisck and Dependencies Crastie & Configuration Object Align configuration to Application Rin Cache Unext App Scheduling PowerFlow Application
		0% Sature Not Stanted Get Stanted	SL1 Run Book Automation Policies Setup Salp For the most current <u>ScienceLopic Documentation</u>	O / 3 Tasks completed Crusting a ServiceNow Credential in SL1 Enabling the Run Book Automation Policies Customizing the Run Book Action Policy
O		0%	Scheduled Script, System property and Related Lists Setup in ServiceNow. (Optional) Skip Scheduled Script Decotors to clear Events associated to cleared incidents in ServiceNow.	0 / J Tasks completed Navigate to Schedule Job Navigate to System property

- 2. In the Setup Integration Account section, click [Get Started] and complete the tasks in order.
- 3. Click [Configure] button to configure each task.
- 4. After you complete each task, click [Mark as Complete].

5. After you finish all the tasks in the **Setup Integration Account** section, complete the steps in the **PowerFlow Setup** section and **SL1 Run Book Automation Policies Setup** section.

NOTE: These tasks are explained in the Guided Setup sections in ServiceNow , and they are also explained in this manual.

6. Optionally, you can run the steps in the Scheduled Script, System property and Related Lists Setup in ServiceNow section.

Configuring SL1

The following topics cover how to set up your SL1 instance to work with Incident Sync.

Creating a ServiceNow Credential in SL1

To configure SL1 to communicate with ServiceNow, you must first create a SOAP/XML credential. This credential allows the run book automations in the "ServiceNow Base Pack" PowerPack to connect with your ServiceNow instance. These run book automations are responsible for sending the SL1 event data to PowerFlow, which ultimately sends the data to ServiceNow.

The **ServiceNow RBA - Example** credential from the "ServiceNow Base Pack" PowerPack is an example SOAP/XML credential that you can configure for your own use.

To configure the ServiceNow RBA - Example credential:

- 1. In SL1, go to the Credential Management page (System > Manage > Credentials).
- 2. Locate the ServiceNow RBA Example credential and click its wrench icon (*P*). The Edit SOAP/XML Credential page appears.
- 3. Complete the following fields:
 - Profile Name. Type a new name for the ServiceNow credential.
 - Timeout. Leave as the default of "5000" ms.
 - Content Encoding. Make sure text/xml is selected.
 - Method. Make sure POST is selected.
 - HTTP Version. Select http/1.1.
 - URL. Type the URL for your PowerFlow instance.
 - HTTP Auth User. Type the username of your PowerFlow instance.
 - HTTP Auth Password. Type the password of your PowerFlow instance.
- 4. Click [Save & Close]. The credential is added to the Credentials page
- 5. On the Credentials page, make a note of the value in the ID column for the credential you just created. You will use this value with the sl1_credential_id parameter when you enable the snippet code of the "ServiceNow: Add/Update/Clear (Case/Event/Incident)" run book action policy.

Enabling the Run Book Automation Policies

NOTE: Versions 104 and later of the "ServiceNow Base Pack" PowerPack separated these run book action policies by Cases, Events, and Incident, such as "ServiceNow: **[Incidents]** - Add/Update".

Before you can run the "ServiceNow: Add/Update/Clear" run book action, you must enable the incident specific run book automation policies in SL1:

- ServiceNow: [Incident] Add/Update
- ServiceNow: [Incident] Event Acknowledged
- ServiceNow: [Incident] Event Cleared

CAUTION: Version 106 and later of the "ServiceNow Base Pack" PowerPack aligned all default Incident Automation policies with the new "ServiceNow: Send to PowerFlow" action type. If you have upgraded to the "ServiceNow Base Pack" PowerPack version 106 or later, but not the "ServiceNow Incident" SyncPack version 4.0.0 or later, you will need to update those default automation policies to align with the older action type. If you made copies of the automation policies, you will not need to update them.

To enable the three ServiceNow run book automation policies:

- 1. In SL1, go to the Automation Policy Manager page (Registry > Run Book > Automation).
- 2. Locate the "ServiceNow: [Incident] Add/Update" automation policy and click its wrench icon (*P*). 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 the corresponding ServiceNow run book action policy. Filter the Available Actions section by typing "ServiceNow" in the search field.

TIP: By default, the "ServiceNow: [Incidents] Add/Update" automation policy will create ServiceNow Incidents for all devices. You can limit the devices affected by making changes to the Organization, Severity, Match Logic, Aligned Devices, and/or Aligned Events fields.

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 "ServiceNow: [Incident] Event Acknowledged" and "ServiceNow: [Incident] Event Cleared" run book automation policies.

Enabling and Customizing the Run Book Action Policy

The "ServiceNow: Add/Update/Clear Incident" run book action policy contains snippet code that you can customize to use with the "ServiceNow Incident" SyncPack.

You can edit these values in the Input Parameters pane of the Actions page for this policy.

NOTE: Make sure you are using the most recent version of the run book action policy. If there are two policies with the same name, always use the policy with the higher number in the **ID** column of the **Actions** page.

To enable and customize the Incident run book action policy:

- 1. In SL1, go to the **Actions** page (Registry > Run Book > Actions).
- 2. Locate the "ServiceNow: Add/Update/Clear Incident" policy and click its wrench icon (*P*). The Action Policy Editor page appears:

Policy Editor Editing Action [38]	Reset
Action Name ServiceNow: Add/Update/Clear Incident	Action State
Desc	ription
Adds and Updates Incidents in ServiceNow. SyncPack 4.0.0+	
Organization ([System]	Action Type ServiceNow: Send to PowerFlow (1.1)
Execution Environment [Default: ServiceNow Base Pack (python2)]	Action Run Context
<pre>{ "sl1_credential_id": "107"; debug": Talse; "configuration": "<configuration "";="" "cmdb_integration":"<cmdb="" "queue":="" from="" id="" or="" po="" sgc="">" } </configuration></pre>	werFlow>",
Save	Save As

- 3. For the Action State filed select Enabled.
- 4. For the sl1_credential_id field in the Input Parameters pane, specify the credential ID form the ID column on the Credential Management page (System > Manage > Credentials). For example: "sl1_credential id": "107"
- 5. Edit the snippet code as necessary, using the information in the **Customizing the Snippet Code in the** *Input Parameters Pane* section, below.
- 6. When you are finished, click **[Save]**.

Customizing the Snippet Code in the Input Parameters Pane

SL1 Run Book Action snippets are written in Python. In the event of a syntax error, the policies will no longer run. As a result, you must ensure that all edits adhere to Python standards. True and False options are case-sensitive and must not contain quotes.

NOTE: The Correlation ID (*correlation _type* in the run book action **Input Parameters**) is no longer set in SL1 or PowerFlow starting with version 4.0.0 of the "ServiceNow Incidents" SyncPack. The Correlation ID is now set in the transformation map within ServiceNow. The preset Correlation IDs that were provided in past applications are also included and can be set by using the **Properties** page in the ServiceNow Application. You can address custom behavior within the transformation map.

You can customize the following values in the "ServiceNow: Add/Update/Clear Incident" run book action snippet code:

- sl1_credential_id. Specifies the ID of the credential object. You can find this value in the ID column of the Credentials page (System > Manage > Credentials of SL1. For example: "sl1_credential_id": "107"
- **debug**. A true/false value that determines if the action is logged in SL1 and if the application is run in Debug Mode on PowerFlow. Troubleshooting logs are written to **/data/tmp/servicenow_rba.log**.
- configuration. Specifies the ID of the configuration object used on PowerFlow. The configuration ID is all lower-case, with spaces in the configuration object "friendly" name replaced by underscores. For example: "configuration": "servicenow_syncpack_configs"

NOTE: To find the configuration ID with the API, make a GET request on this endpoint: https://<powerflow hostname>/api/v1/configurations.

- queue. Specifies the worker queue on which the application runs. Leave this as default.
- **cmdb_integration**. Specifies which CMDB SyncPack you are using to ensure that PowerFlow sends the correct identifiers to ServiceNow.
 - If you are using the "ServiceNow CMDB" SyncPack version 3.5.0 or later, use "SGC" to allow Cls to attach to incidents. For example: "cmdb integration": "SGC"
 - If you are using versions of the "ServiceNow CMDB" SyncPack before version 3.5.0, use "CMDB".
 - If you are using the "ServiceNow Service Graph Connector" SyncPack, use "SGC".

Starting with version 4.1.0 of this SyncPack, the following fields have been deprecated. If you still want to sync these fields, see Sending Custom Data to ServiceNow Using the Passthrough Option.

- *pf_app_override*. If you are using a custom PowerFlow application to consume SL1 Events, add the system name of that application to this parameter. Optional. If this parameter is not present and populated, PowerFlow will use the default application for consuming events.
- **discard_if_no_ci**. Deprecated. Previous versions let you specify whether PowerFlow should create cases, events, or incidents in ServiceNow for devices that do not have a matching CI record.
- servicenow_state_new:
 - ° 1. Incident state is "New". This is the default value.
 - 2. Incident state is "In Progress".
 - 3. Incident state is "On Hold".
 - ° 6. Incident state is "Resolved".
 - ° 7. Incident state is "Closed".
 - ° 8. Incident state is "Canceled".
- servicenow_state_ack:
 - ° 1. Incident state is "New". There is no default value.
 - ° 2. Incident state is "In Progress".
 - ° 3. Incident state is "On Hold".
 - ° 6. Incident state is "Resolved".
 - 7. Incident state is "Closed".
 - ° 8. Incident state is "Canceled".
- servicenow_state_clear:
 - ° 1. Incident state is "New".
 - ° 2. Incident state is "In Progress".

- ° 3. Incident state is "On Hold".
- ° 6. Incident state is "Resolved". This is the default value.
- 7. Incident state is "Closed".
- ° 8. Incident state is "Canceled".
- To assign an assignment group, set the variable value to the **sys_id** of the ServiceNow Assignment Group. In the following example, the assignment group is assigned to incidents that are *cleared*:

```
"assignment group new": "",
```

```
"assignment_group_ack": "",
```

```
"assignment_group_clear": "sys_id"
```

Customizing Logging in the Run Book Action

You can customize the following logging-related items in the "ServiceNow: Add/Update/Clear" Run Book Action snippet code:

- logfile = /data/tmp/ServiceNow_add_update_clear_incident.log
 - ° Location for logging output.
 - Will be created if it does not exist.
 - Will be appended with each Run Book job.
 - Is case-sensitive.
- do debug logging = True
 - True is on, False is off.
 - Is case-sensitive.
 - ° For troubleshooting, these can be enabled or changed.
 - Writes logs to /data/tmp/servicenow_rba.log.

Sending Custom Data to ServiceNow Using the Passthrough Option

You can use the "ServiceNow: [(Cases/Events/Incidents)] Add/Update" run book automation and the "ServiceNow: Add/Update/Clear (Case/Event/Incident)" run book action to "pass through" custom data about SL1 cases, events, or incidents to ServiceNow (depending on the SyncPack you are using with PowerFlow).

For example, you might want to use the passthrough functionality to overwrite the impact and urgency of a ServiceNow incident, which is the only way to change the priority of the incident.

To pass custom data to ServiceNow:

- Create a new run book action that pulls the relevant data and adds it to a dictionary called EM7 RESULT.
- Add the new run book action to the "ServiceNow: [(Cases, Events, or Incident)] Add/Update " run book automation Policy, ahead of the "ServiceNow: Add/Update/Clear (Case/Event/Incident)" run book action so that the new action runs first, and then is consumed by the ServiceNow action.

Passing Custom Data to ServiceNow

The following procedure describes how to configure the passthrough functionality, using the "ServiceNow: [*Incident*] Add/Update" run book automation and the "ServiceNow: Add/Update/Clear *Incident*" run book action as examples.

To pass custom data to ServiceNow:

- 1. In SL1, go to the **Actions** page (Registry > Run Book > Actions) and click [**Create**] to create a new run book action policy.
- 2. Complete the following fields:
 - Action Name. Type a unique name for the action.
 - Action State. Select Enabled.
 - Action Type. Select Run a Snippet.
 - Execution Environment. Select ServiceNow Base Pack.
 - Complete the other fields as needed, or leave them at their default settings.
- 3. In the **Snippet Code** pane, add the snippet code you want to include for the EM7_RESULT dictionary. For example, the following snippet code lets you override the ServiceNow Incident work notes with a hardcoded note:

```
EM7 RESULT = {"work notes": "This is a new note"}
```

Additional notes about the structure of the EM7_RESULT dictionary:

- EM7_RESULT = is required for the dictionary, and the formatting of the keys should match the example above.
- All keys defined in the EM7_RESULT dictionary need to map to field IDs on the **ScienceLogic Events** table in ServiceNow.
- You can hard-code the values in the EM7_RESULT dictionary, or you can use variables and functions, like the "Snippet Code Example", below.
- As a best practice, avoid sending null passthrough values to ServiceNow. If you must send 'null' or 'NULL' values to ServiceNow, pass through that value as an empty string, such as "location":"". Also, only pass through values that you need. For example, instead of sending {"location": "", "work notes": "stuff"}, simply send {"work notes": "stuff"}.
- A long snippet might delay the ticket being created
- 4. Click [Save].
- 5. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation) and open the "ServiceNow: Add/Update Incident" run book automation Policy.

6. In the **Available Actions** section, add the new run book action before the "ServiceNow: Create, Update, Clear Incident" run book action:

Policy Name		Policy Type	Policy Stat	te	Policy Prin	ority	Organizat	ion
ServiceNow: Add/Update Incident	[Active Events] *	[Enabled]		[High] V		[System] V		
Criteria Logic		Match Logic			Match Sy	ntax		
[Severity >=] [Major.]	۲	[Text search] *	5			- THE C		-
[and no time has elapsed]	٠	Dece	at Time	t Time Align With				
[since the first occurrence,]		[Only once]	as inne		[Devices]	1 VINEN		
[and event is NOT cleared]	٠	-						
[and all times are valid]		Include events for	entities other that	in devi	ces (organizatio	005, 355	ets, etc.)	
	٣							
Trigger on Child Rollup								
Available Devices			Aligned Devis	ces				_
			(All devices	0.52				_
System ServiceNow: Instance: ven01056		Ĵ	8					
Available Events			Aligned Even	ts				
			(All events)	1				
[3569] Critical: AKCP: AC Voltage ser [3578] Critical: AKCP: DC Voltage ser [3579] Critical: AKCP: DC Voltage ser [3558] Critical: AKCP: Dry Contact Se [3574] Critical: AKCP: Smoke Detecto [3572] Critical: AKCP: Water Sensor I	nsor H nsor Lo ensor L or Alert	igh Critical ow Critical ow Critical	8					
Available Actions			Aligned Actio	ns				٦.
Snippet [5]: Cisco: VOS Component I Snippet [5]: Cisco: VOS Node Classit Snippet [5]: Dell EMC: Unity Classit Snippet [5]: Dell EMC: VMAX Unisph Snippet [5]: EM7 Ping Snippet Snippet [5]: Example Pastthrough EM	Root D ere Cla	and Cluster Crea evice Class issify Root Device			nple Passificou ate, Update, C			

- **NOTE**: The output of this new run book action will be consumed by the "ServiceNow: Create, Update, Clear Incident" run book action, ensuring that the EM7_RESULT dictionary is passed through to ServiceNow. The "ServiceNow: Create, Update, Clear Incident" run book action automatically populates the passthrough values with any values from EM7_LAST_RESULT. The passthrough overwrites any other previously defined fields, such as assignment group.
- 7. You can add additional run book actions to the run book automation Policy for any additional workflows that you might want to run. The Automation Policy execute these Actions in a sequential, top-down order. However, the "ServiceNow: Create, Update, Clear Incident" run book action only consumes the EM7_ RESULT dictionary from the run book action directly above it.

Passthrough Example

For the Dictionary Entry of the ServiceNow field on the import table, you can reference the XML of the record. You will need to copy the *<sys name>* value so you can use that as the key for the passthrough.

In this example, you want to bring in an additional field called *sl1 category*.

1. Create the new *sl1 category* field on the import table in ServiceNow. You can right-click on the header of the form to view the XML:

C = Dictionary Entry sl1 category			0
			ctionary entries, select a Table and the field Type of the new column. Also enter a column label, which becomes the field la leid a <u>Disalay Value</u> for reference fields so it appears on records that reference this table. <u>More info</u>
* Table	ScienceLogic Incident import [x_sclo_incide	•	O https://ven01056.service-now.com/sys_dictionary.do?sys_jd =4fcfd8741bbee9102e420fs4cc4bcb528 − □ ×
* Type	String	م١	wen01056.service-now.com/sys_dictionary.do?sys_id=4fcfd8741bbee9102e420fa4cc4bcb528sys_target creference_qual/>
* Column label	sl1 category	Ť	<pre><reterence_qual> </reterence_qual></pre>
* Column name	u_sl1_category		<sizeclass></sizeclass> <spell_check>false</spell_check>
* Max length		24	<tsgcd>false <sys_class_name:sys_dictionary< sys_class_name=""> <sys by="" by:admin="" created="" sys=""></sys></sys_class_name:sys_dictionary<></tsgcd>
			<pre><sys_inetad_on>2023-05-11 15:13:11</sys_inetad_on></pre> <pre>created_on> <sys_id>4fcf8f74bbee9102e420fa4cc4bcb52c/sys_id> <sys_id> <sys_id> </sys_id></sys_id></sys_id></pre>
Choice List Specification Default Value			<pre>ctype_package display_value="ScienceLogic SL1: Incident Automation" source="x,scienceLogic SL1: Incident ScienceLogic SL1: Incident Automation" source="x,scienceLogic SL1: Incident ScienceLogic SL1: Incident Automation" source="x,scienceLogic SL1: Incident ScienceLogic SL1: Incident Automation" source="x,scienceLogic SL1: Incident SL1: Incident SL1: Incident Automation" source="x,scienceLogic SL1: Incident SL1: Incident SL1: Incident Automation" source="x,scienceLogic SL1: Incident SL1: In</pre>
Displays a list of suggested values in a Choi	ce list. In the Advanced view you can select the Cl	hoice t	
Choice	None	_	<pre><sys_update_name>sys_dictionary_x_sclo_incident_import_u_sll_category</sys_update_name> <sys_updated_by>admin <sys_updated_on>2023-05:</sys_updated_on></sys_updated_by></pre>
	(<table_reference>false</table_reference> <text_index>false</text_index> <unsure_false< unsure_index=""></unsure_false<>
Delete Column Update			<pre><unique>raise</unique> <use_dependent_field>false</use_dependent_field> <use_dynamic_default>false</use_dynamic_default></pre>
Related Links			<pre><use_reference_qualifier>simple</use_reference_qualifier> <virtual>false</virtual></pre>
Show Table Run Point Scan			<pre><virtual_type>script</virtual_type> <widget></widget></pre>
Advanced view			<pre><write_roles></write_roles> <xml_view>false</xml_view></pre>
Access Controls Choices Attributes	Labels (1)		

- 2. Look for the *<sys name>* value.
- 3. Copy that value directly out and use that in your EM7_RESULT for the passthrough value (in the Snippet Code pane):

```
EM7_RESULT = { 'sl1 Category': 'test' }
```

Snippet Code Example

The following snippet code example shows how to pull additional information and make it available for passthrough. All of the additional information that is going to be sent is contained in a dictionary variable called EM7_RESULT. You can pass through multiple items through in a single run book action by adding additional keys to the EM7_RESULT dictionary.

This example lets you assign assignment groups to an Incident based on certain criteria, such as event policy IDs:

```
from future.utils import iteritems

def invert_mappings(mappings):
    """
    Invert received one-to-many mappings and converts it into a one-to-one
    mapping.
    Args:
        mappings (dict): Dictionary of mapped values
    Returns:
        dict: inverted dictionary.
    """
    inverted mappings = dict()
```

```
for key, values in iteritems(mappings):
        for sub value in values:
            invert mappings[sub value] = key
    return inverted mappings
# Example of assignment group to list of event policy ids mapping.
assignment groups to event policies = {
    "sys id 1": [1, 2, 3, 4, 5],
    "sys id 2": [6, 7, 8, 9, 10],
# which sys id to use if the current event policy id isn't mapped
default sys id = "sys id 3"
# invert the mappings
event policy to assignment group = invert mappings(assignment groups to
event policies)
# Send assignment group sys id to IS RBA
EM7 RESULT = \{
    "assignment group": event policy to assignment group.get(
        EM7 VALUES["%3"], default sys id
    )
```

Configuring the "ServiceNow: Click to Create Incident" Automation Policy

The "ServiceNow: [(Cases/Events/Incident)] - Click to Create" automation policy lets you manually create a case, event, or incident in ServiceNow by clicking the **Actions** button (--) in SL1 for an event and selecting "Create External Ticket" (or by clicking the life-preserver icon (2)) for an event in the classic user interface).

This run book action policy is available in the "ServiceNow Base Pack" PowerPack.

To configure the "ServiceNow: Click to Create" run book action policy:

- In SL1, go to the Behavior Settings page (System > Settings > Behavior) and set the Event Console Ticket Life Ring Button Behavior option to Create/View External Ticket.
- 2. Click **[Save]** to save your changes. You might need to log out of SL1 and log back into SL1 for the changes to update.
- 3. Go to the Automation page (Registry > Run Book > Automation).

- 4. Locate the "ServiceNow: (Cases/Events/Incident) Click to Create" policy and click its wrench icon ("). The Automation Policy Editor page appears:
- 5. Update the following fields:
 - Policy State. Select Enabled.
 - In the **Criteria Logic** section, select and external ticket IS requested in the fifth drop-down. Leave the other values in this section at their default settings.
 - **Repeat Time**. Specify 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". By default, the policy only runs once.
 - Available Actions. If it is not already selected, select ServiceNow: Send to PowerFlow: ServiceNow: Add/Update/Clear Incident and add it to the Aligned Actions field.
- 6. Click [Save]. The "Click to Create" feature is now available on the Events and Event Investigator pages.

Enabling Run Book Automation Queue Retries

You can enable run book action (RBA) queue retries to keep from losing any data if PowerFlow is unavailable. Those pending PowerFlow applications are added to an RBA queue that you can access to retry the applications that failed.

For more information, see Enabling Run Book Automation Queue Retries.

Configuring PowerFlow

The following topics cover how to set up your PowerFlow instance to work with Incident Sync.

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 that are triggered by the Run Book Actions in SL1.

TIP: Depending on your SL1 environment and the third-party environment with which you are syncing data, you might be able to use the same configuration object with more than one SyncPack.

For this SyncPack, you can make a copy of the "ServiceNow SyncPack" configuration object, which is the sample configuration file that was installed with the "ServiceNow Base" SyncPack.

TIP: The "ServiceNow SyncPack" configuration object contains all of the required variables. Make a copy of the configuration object and update the variables from that object to match your SL1 and ServiceNow settings.

To create a configuration object based on the "ServiceNow SyncPack" configuration object:

- 1. In the PowerFlow user interface, go to the **Configurations** page (‡).
- For the "ServiceNow SyncPack" configuration object, click the [Actions] button (
) and select Edit. The Configuration pane appears.

TIP: Click [Toggle JSON Editor] to show the JSON code. Click the button again to see the fields.

3. Click [Copy as]. The Create Configuration pane appears.

IMPORTANT: This step is required. Do *not* use the original configuration object to run PowerFlow applications.

- 4. Complete the following fields:
 - Friendly Name. Name of the configuration object that will display on the Configurations page.
 - **Description**. A brief description of the configuration object.
 - Author. User or organization that created the configuration object.
 - Version. Version of the configuration object.

5. In the **Configuration Data** field, include the required block of code to ensure that the applications aligned to this configuration object do not fail:

```
{
   "encrypted": false,
   "name": "sl1_db_host",
   "value": "${config.sl1_host}"
},
```

For example:

```
{
    "encrypted": false,
    "name": "sl1_db_host",
    "value": "10.2.11.42"
},
```

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

NOTE: The *region* value is a user-defined variable that identifies your SL1 instance within ServiceNow.

- 7. To create a configuration variable in the JSON Editor, define the following keys:
 - **encrypted**. Specifies whether the value will appear in plain text or encrypted in this JSON file. If you set this to "true", when the value is uploaded, PowerFlow encrypts the value of the variable. The plain text value cannot be retrieved again by an end user. The encryption key is unique to each PowerFlow system. The value is followed by a comma.
 - **name**. Specifies the name of the configuration file, without the JSON suffix. This value appears in the user interface. The value is surrounded by double-quotes and followed by a comma.
 - **value**. Specifies the value to assign to the variable. The value is surrounded by double-quotes and followed by a comma.
- 8. Click [Save]. You can now align this configuration object with one or more applications.

Configuring the PowerFlow Applications

To run Incident Sync, you must "align" the configuration object to run with the following PowerFlow applications:

• Cache SL1 Users. Performs a query for all existing users and writes them to a cache. To maintain the user cache for this SyncPack, ScienceLogic recommends that you schedule this application to run at least once a week.

- Sync Cached Events to ServiceNow. Bulk processes all of the cached SL1 Events and posts them to ServiceNow. Sends a "Sync Success" or "Sync Failed" status update to PowerFlow based on the result of the post. ScienceLogic recommends that you schedule this application to run every 60 seconds or longer.
- Sync Incident Details from ServiceNow to SL1 Events. Acknowledges or clears SL1 Events from ServiceNow, updates the user note, and populates the incident number in the external ticket reference. This application also include the new user_note_template field that accepts a Jinja2 template to generate custom user notes. ScienceLogic recommends that you schedule this application to run every 60 seconds.

NOTE: In previous releases of this SyncPack, this application was named the "Sync Incident State from ServiceNow to SL1 Event" application.

• Sync SL1 Event to ServiceNow Incident. The "ServiceNow: Add/Update/Clear Incident" Run Book Action triggers this application whenever an SL1 Event is created, updated, or cleared.

NOTE: This application processes the SL1 event, caches it to PowerFlow to allow for bulk processing for ServiceNow by the "Sync Cached Events to ServiceNow" application, and then sends a status update to SL1.

In addition, you can configure additional fields from the **Configuration** pane for the "Sync Incident Details from ServiceNow to SL1 Events" and the "Sync Cached Events to ServiceNow" PowerFlow applications.

NOTE: If you are using the "ServiceNow CMDB" SyncPack and you want to link incidents with ServiceNow Configuration Items (CIs), you will need to run the "Sync Devices from SL1 to ServiceNow" application. If this is the first time you are running the Incident Sync, you will need to run the "Sync Devices from SL1 to ServiceNow" application twice to build the internal cache. For more information, see the **ServiceNow CMDB SyncPack** manual.

To configure the PowerFlow applications:

- 1. On the **Applications** page of the PowerFlow user interface, open the "Sync SL1 Event to ServiceNow Incident" application and click **[Configure]**. The **Configuration** pane for that application appears.
- 2. From the **Configurations** drop-down, select the configuration object you want to use.
- 3. Click **[Save]** to align that configuration object with the "Sync SL1 Event to ServiceNow Incident" application. You do not need to edit any other fields for that application.
- 4. Repeat steps 1-3 for the "Cache SL1 Users" application. This application is in the "System Utils" SyncPack. ScienceLogic recommends that you schedule this application to run at least once a week.
- 5. Go to the **Applications** page, open the "Sync Cached Events to ServiceNow" application, and click **[Configure]**. The **Configuration** pane for that application appears.
- 6. From the **Configurations** drop-down, select the configuration object you want to use.
- 7. Update the following fields, as needed:

- *retry_max*. The maximum number of times PowerFlow will retry to execute the step before it stops retrying and logs a step failure. For example, if retry_max is 3, PowerFlow will retry after 1 second, then 2 seconds, then 4 seconds, and stop if the last retry fails. The default is 0.
- *retry_jitter*. Instead of using a defined interval between retries, the PowerFlow system will retry the step execution at random intervals. The default is unselected.
- *retry_backoff*. Instead of using a defined interval between retries, PowerFlow will incrementally increase the interval between retries. The default is unselected.
- retry_backoff_max. The maximum time interval for the retry_backoff option, in seconds. For example, This means, if you have retry_max set to 15, the delays will be 1, 2, 4, 8, 16, 32, 64, 120, 240, 480, 600, 600, 600, and 600. The default is 600.
- *limit*. Specify the number of events to send per batch. The default is 2000.

- 8. Click [Save].
- 9. Go to the **Applications** page, open the "Sync Incident Details from ServiceNow to SL1 Events" application, and click **[Configure]**. The **Configuration** pane for that application appears:

Sync Incident Details fro	m ServiceNow to SL1 Events	×
Modify configuration and save.		Show JSON Configs
Configuration ven01056	•	· · · · · · · · · · · · · · · · · · ·
snow_hostname ven01767.service-now.com 🔒	snow_user Inc Integration user	snow_password
\${config.snow_host}	\${config.snow_user}	
sl1_hostname 10.2.11.154	sl1_user em7admin	sl1_password
\${config.sl1_host}	\${config.sl1_user}	
region unique_id	read_timeout 200	resolve_states Resolved
\${config.region}		Enter comma-separated strings.
✓ enable_sl1_ack	update_user_note	user_note_template {{ 'Event State: {} Aligned events:
chunk,size		
		Save
		Jure

NOTE: This application populates the incident numbers in SL1 as well as updating other incident behaviors.

- 10. From the **Configurations** drop-down, select the configuration object you want to use.
- 11. Update the following fields, as needed:
 - **resolve_states**. Specify one or more state labels that PowerFlow will consider as "Resolved", separated by commas. SL1 Events associated with a ServiceNow Incident in these states will be cleared.
 - **enable_sl1_ack**. Select this option to allow this integration to acknowledge events. The application attempts to acknowledge with the user assigned to the incident.

- **update_user_note**. De-select this option if you do not want this application to update the User Note in SL1.
- **user_note_template**. Lets you add a Jinja2 template to define a customer format for populating the User Notes in SL1. If you leave this field blank, PowerFlow uses the state label that displays in gray text. For more information about Jinja2 filters, see the <u>List of Built-in Filters in the Jinja2</u> <u>documentation</u>.

```
TIP: The following is an example of a Jinja2 template that you can use in this field:
    {{ 'Incident {} is assigned to {} has {} events aligned to it
    and is currently in state {}'.format(incident.incident_
    number, incident.user.user|default(None),
    incident.events|length, incident.state)}}
```

12. Click [Save].

Scheduling PowerFlow Applications

ScienceLogic recommends that you schedule the following PowerFlow applications:

- "Cache SL1 Users": at least once a week
- "Sync Incident Details from ServiceNow to SL1 Events": every 60 seconds
- "Sync Cached Events to ServiceNow": every 60 seconds; less than 60 seconds might cause adverse performance issues within ServiceNow

You do *not* need to schedule or run the "Sync SL1 Event to ServiceNow Incident" application, as the "ServiceNow: Add/Update/Clear Incident" Run Book Action triggers this application whenever an SL1 Event is created, updated, or cleared

For more information about scheduling applications, see Scheduling a PowerFlow Application.

Incident Topology Suppression

Incident topology suppression is used when ServiceNow incidents that have been synced with SL1 devices occur on devices that have a parent/child relationship. If you choose to enable incident topology suppression in SL1, child events synced with ServiceNow incidents do not appear in the SL1 **Event Console** as separate events. Instead, the child events are nested under the parent event.

NOTE: The steps in this process use the Classic user interface for SL1.

To enable incident topology suppression:

1. In SL1, navigate to the **Event Policy Manager** page (Registry > Events > Event Manager) and click the **[Create]** button. The **Event Policy Editor** modal appears:

	Event Policy E	litor Edit	ting Eve	ent Pol	icy [489	5]											New		Reset	Guide
ſ	Policy	Adva	anced	Sup	pression	IS														
l		Event	Source										Po	licy Name						
Ш	API	Onumbia			\sim) Top	ology Si	ppress							-					
	[Enabled]	Operatio	onal State	9		Chi	ild ev	ents w	ere su	ppress	ed for	this		nt Messag :e .	le		 			 •
		Event S	Severity																	-
Ш	Critical	\sim) 🗆 U	lse Moo	difier 🧯						_									.::
ľ										Policy	Descriptio	n								
	🖹 - 🖍	B <i>I</i>	<u>U</u>	S	A٠	T!-	ð -	¶ -	% -	≣·		∎ i≡	≣	•	-	%	/	>		
	Start typi																			
	Start typ	ig																		
Ш																				
ľ										Save	Sav	e As								

- 2. On the **[Policy]** tab, update the following fields:
 - Event Source: Select API.
 - **Operational State**: Select Enabled.
 - Event Severity: Select Critical as the severity of the event.
 - **Policy Name**. Type the name of the event. Can be any combination of alphanumeric characters, up to 48 characters in length
 - Event Message. Type the message that will appear when this event occurs.
- 3. Click the **[Advanced]** tab.

Event Policy Editor Policy Successfully Saved [48	95] Editing Event Policy [4895]	New	Reset	Guide
Policy Advanced Suppressions				
Occurrence Count	First Regular Expression			
[Disabled]	CRITICAL			0
Occurrence Time	Second Regular Expression	ı		
[Disabled]				?
Expiry Delay	Identifier Pattern		Override Ytype	
[Disabled]		😧 [None]		√ ?
Detection Weight	Identifier Format			
20 - Last 🗸 🗸 😪				0
Component Type				
[N/A]	Auto-Clear		Topology Suppression	n
External Event Id		😧 🛛 Both		✓ ?
	[None Selected] Healthy: AKCP: AC Voltage sensor now reporting Normal Status [3192]		Category	
External Category	Healthy: AKCP: DC Voltage sensor returned to Normal Status [3199]			😧
0	Healthy: AKCP: Dry contact sensor now Normal [3190] Healthy: AKCP: Smoke detector now Normal Status [3187]	[None Se	lected]	^
Match Logic	Healthy: AKCP: Water sensor now Normal [3188]			
Regex Match	Healthy: Alteon: Primary Power Supply Healthy [3013] Healthy: Alteon: Redundant Power Supply Healthy [3015]			
Use Multi-match 🚱	Healthy: AMQP: RabbitMQ Device Running [4889]			
Use Message-match	Healthy: APC: Batteries Do Not Need Replacement [1516] Healthy: APC: Battery Charge Normal [1524]			
Use message-match 😈	Healthy: APC: Battery Run Time Remaining No Longer Critical [1518] Healthy: APC: Calibration Test Completed [1537]			
	Healthy: APC: Calibration Test Completed [1537] Healthy: APC: Communication Status Okay [1528]			
	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 N			
	Healthy: AWS: API 4xx Error Has Returned To Normal [4658] Healthy: AWS: API 5xx Error Has Returned To Normal [4660]			
	Healthy: AWS: API Count Has Returned To Normal [4664]			\sim
	Save Save As			

- 4. On the [Advanced] tab, update the following fields:
 - **Detection Weight**. Select 20 Last. If two event definitions are very similar, the weight field specifies the order in which SL1 should match messages against the similar event definitions. The event definition with the lowest weight will be matched first. This field is most useful for events that use expression matching. Options range from 0 (first) 20 (last).
 - Match Logic. Select Regex Match. Specifies whether SL1 should process the First Match String field and Second Match String as regular expressions or as simple text matches. Because you selected Regex Match, you cannot define a "match all" expression by leaving the First Match String and Second Match String fields empty.
 - Use Message-match. Select this option. If SL1 has generated an event and then a second log message or alert matches the same event policy for the same entity, SL1 will not generate a second event, but will increase the count value for the original event. This behavior will occur only if the log messages or alerts contain the same message.
 - *First Regular Expression*. Type "CRITICAL" as the string used to correlate the event with a log message.
 - **Topology Suppression**. Select Both. If this event occurs on a parent device, it behaves as a suppressing event. If this event occurs on a child device, it behaves as a suppressible event.
- 5. Click [Save] and close the Event Policy Editor modal.
- 6. Next, go to the **Device Groups** page (Registry > Device Groups) and click the **[Create]** button. A **Device Group Editor** page appears:

Device Group Editor Creating new group Click S	Save to commit changes	Guide Reset
Device Group Name	Force Child Visibility?	Sharing Permissions
All Devices	[No]	[Private (visible to you only)]
Icon	Visibility	Permission Keys
	Mags/Vevs Coning Potievies/Buik Edit Notification/Automation Discovery Device Schedules Event Soupression RSS Feeds	EM7 System Administration Grant All Basic User Privleges PowerFack Administration Proverfack Administration Proverfack Administration Proverfack Administration To Services - View IT Services - View IT Services - Administration V
Static Devices and Groups Devices [0] Groups	[0]	Del Add
Device Name Class Sub-class	D Organization Device Gr	oup Name • ID Devices Groups Rules I
No devices in current device group		No sub-groups in current device group.
Dynamic Rules Rules Found [1] Adding rules [Selector Type 1.1. Provide Name *] Selector Targets	Devices matched for rule 1: 9 Devices matched for rule 1: 9
	Save	matuleu
	Save	

- 7. Complete the following fields, and leave the default settings for the remaining fields:
 - Template Name. Specify the name of the new device group.
 - Force Child Visibility. Select "No".
 - Visibility. Select Config Policies/Bulk Edit to let you configure all the devices in the new device group using a device template.
- 8. Click the **[Save]** button and then click the **[Add]** button in the **Dynamic Rules** pane to add dynamic rules to the new device group. The Device Group Rule Editor modal page appears:

Add Rule						×
Device Group Rule Editor Active S	election				Res	set
Active Selectors Organization Device Class Device Category Device Name Device Name Device State Collector Group Open TCP Ports Running Process Windows Service Subscribed Product Active Event	9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Begins with "term" Ends with "term" Is "term", "team", "teem" Is not "term"				
Matched Devices [9]	0.1	Olare 10th class		Querra institut	Collection	^
<u>Device Name</u> • 1. 10.2.11.66	Category Unknown	Class Sub-class Ping Generic Linux	<u>D</u> 9	Organization System	Active	
2. 10.2.11.68	Unknown	Ping Generic Linux	10	System	Active	
3. <mark>M</mark> airlocks	Unknown	Ping Generic Linux	11	System	Active	
4. MAzure Device	Service	Microsoft Azure Services	3	System	Active	
5. 📶 em7ao	EM7	ScienceLogic, Inc. EM7 All-In-0	1	System	Active	
6. 📶 em7ao	EM7	ScienceLogic, Inc. EM7 All-In-(2	System	Active	
7. Integration Service Docs	EM7	ScienceLogic Integration Serv	5	System	Active	
				Select rela	ted devices OK	

- 9. In the Active Selectors pane, select Device Name.
- 10. Optionally, in the **Selector Definitions** pane, type an asterisk (*) in the **Device Name** field. Using the * includes all devices by Device Name. In the **Matched Devices** pane, a list of all devices appears.
- 11. Click **[OK]** to close the modal page.
- 12. On the Device Group Editor modal page, click [Save] and close the page.

13. Next, create a Device Group Template that will disable Event Masking for all devices in the new Device Group. Click the building blocks icon (🂫) for the new device group. A **Device Template Editor** page appears:

Template New / One-off	Template	Save W	hen Aj	pplied & Confirr	ned Template N	lame 🦳		
C on fig	Inter fa ce	CV Policies	F	Port Policies	Svc Policies	Proc Poli	cies Dyn Apps	Logs
Access & Monitoring							Device Preferences	
Device Organization	Acme Inc		\sim				Auto-Clear Events	Scan All IPs
SNMP Read	Cisco SNMPv2 - Ex	ample	\sim	SNMP Write	None	\sim		
Availability Protocol	ТСР		\sim	Avail Port	ICMP	\sim	Accept All Logs	Dynamic Discovery
Latency Protocol	TCP			Latency Port	ICMP	\sim		
Avail+Latency Alert	Disabled		\sim				Daily Port Scans	Preserve Hostname
Collection	Enabled		\sim	Collector Grp	CUG	\sim		
Coll. Type	Standard		\sim				Auto-Update	Disable Asset Update
Critical Ping	Disabled		\sim					
Event Mask	Disabled		\sim]			Bypass Interface Inventory	
evice Retention & Bas								
System Latenc	^y			100 ms	Daily Rollup Bandwidth Data		<u> </u>	730 days
					Hourly Rollup Bandwidth Data	÷	1 1	120 days
Availability Packet Siz	-10	1		56 bytes	Raw Performance		1	7 days
Availability Ping Cou	nt 🔟	I		1 pings	Daily Rollup Performance Data			730 days
nterface Inventory Set	-							
Interface Invent	ory Lat	1	60	00000 ms	Maximum Allowed		I I (10000 interfaces

- 14. Because all of the fields are disabled (grayed-out) by default, click the **Event Mask** field name to enable the field. Use the default setting of *Disabled*.
- 15. Click [Apply] and click [Confirm] on the Device Template Editor page.
- 16. Next, turn off the Trigger on Child Rollup option on the "ServiceNow: Add/Update Incident" Run Book Automation. Go to the Automation Policy Manager page (Registry > Run Book > Automation) and click the wrench icon (²) for the "ServiceNow: Add/Update Incident" Run Book Automation. The Automation Policy Editor page appears:

Automation Policy Editor Editin	ng Automation P	Policy [49] Reset	
Policy Name ServiceNow: [Incident] - Add/Update Criteria Logic [Severity >=] ∨ [Notice,] ∨ [and no time has elapsed] ∨ [since the first occurrence,] ∨ [and event is NOT cleared] ∨ [and all times are valid] ∨ V Trigger on Child Rollup	Policy Type [Active Events] Match Logic [Text search] V Repea [Only once]	e Policy State Policy Priority Organization v [Disabled v) [High] v) [System] v Match Syntax eat Time Align With	×
Available Devices Internal Servers ScienceLogic: PowerFlow: 10.2.11.149 ScienceLogic: PowerFlow: 10.2.11.65 System		Aligned Devices (All devices) %	
Available Events [2838] Critical: AKCP: AC Voltage sensor de [2847] Critical: AKCP: DC Voltage sensor Lo [2848] Critical: AKCP: DC Voltage sensor Lo [2837] Critical: AKCP: Dry Contact Sensor L [2843] Critical: AKCP: Smoke Detector Alert	igh Critical working worki	Aligned Events (All events) «	
Available Actions SNMP Trap [1]: SL1 Event Trap Snippet [5]: Automation Utilities: Calculate M Snippet [5]: AWS: Disable Instance By Tag Snippet [5]: AWS: Discover from EC2 IP Snippet [5]: AWS: Get EC2 Instance Config	emory Size for Each	Aligned Actions 1. ServiceNow: Send to PowerFlow [101]: ServiceNow: A	
	Save	Save As	_

17. Make sure the Trigger on Child Rollup option is not selected and click **[Save]**. Close the **Automation Policy Editor** page.

Additional Options in ServiceNow

Viewing Events with ServiceNow

Within ServiceNow, the Incident Sync sends as much data as possible, but limits what is sent or updated directly to the incident table. All SL1 Event-specific data is mapped to a separate record and custom application-specific table. A related list option is available to provide event record data that you can view from the incident.

NOTE: The related list **[SL1] Events** is not configured when you install the Certified application. You need to add that related list to the incident form.

You can also view the actual Event records at ScienceLogic SL1: Incident Automation > Event > ScienceLogic Events.

Hyperlinking Events

Both ServiceNow and SL1 provide mechanisms for hyperlinking to multiple active events and incidents.

Each Incident in ServiceNow will have one or more events aligned with it through a related list: [SL1] Event.

By default the *Hyperlink* field "Event URL" only appears on the Event (x_sclo_incident_event) custom table provided by the Certified application. If a URL link is required, you would need to customize it to be applied to different location.

The following image shows the Event record for an event aligned with an Incident:

Event ID 100179 Event message Device Failed Availability Chick: KMP Ping	
Event message Device Failed Availability Check: ICMP Ping	
Event severity label MAJOR	
Event severity 3	
Event active timestamp 2021-09-27 05:00:39	
Event first timestamp 2021-09-27 05:00:39	
Event last timestamp 2021-09-29 03:20:51	
Event clear timestamp 2021-09-29 03:25:31	
Event counter 546	
Event Policy ID 1581	
Event policy name Polier: Availability Check Failed	
Event source label Internal	
Event policy stateful 1	
Event source 2	
Event policy external ID	
Event policy cause 4 p class="fr-agr">strong=Event Definition.ahosp: fragr">strong=Probable Cause.ahosp; strong=The device may be down, or the network connection to the device may be malfunctioning.	
Event policy category	
Event user note In Progress	
Event clear user auto-clear	
Event external licket reference INC0022320	
Event URL http://em7.mydomain.com/em7/index.em7?evec-events&q_type=aid&q_arg=100179&q_sev=1&q_sort=0&q_ope=0	

Viewing the Incident Import Table in ServiceNow

Each time SL1 creates or changes an incident in ServiceNow, data is inserted into a temporary import table on the ServiceNow system. This table displays all inbound data from SL1 and is a useful tool to determine what data is being sent and imported. The incident import table is created automatically when you install the ScienceLogic Certified (Scoped) Application.

To view the data and the status of the import process, go to the **Import Incidents** page (ScienceLogic > Event > Events) in ServiceNow:

Sciencelogic		8		import inc	idents New	Search	Updated	¥ S	earch							≪≪ ≪ []1	o 100 of 1,310 🕨 🕨
	*		7	All													
Favorites		^	0	Q	Event ID	_	■ Created	_	Correlation ID	■ Incident	E CMDB CI	Updated ▼	Target record	≡ State	Incident state	■ Created by	Import set run
E ScienceLogic	- Dependents				Search	_	Search		Search	Search	Search	Search	Search	Search	Search	Search	Search
ScienceLogic				()		1176595	2019-09-19 09:	33:21	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:33:21	Event: 1176595	Updated	Resolved	fsun	(empty)
Support				0		1176595	2019-09-19 09:	33:21	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:33:21	Incident: INC0013376	Updated	Resolved	fsun	(empty)
▼ Event				0		1176595	2019-09-19 09:	28:27	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:28:27	Event: 1176595	Inserted	In Progress	fsun	(empty)
Event Propertie				0		1176595	2019-09-19 09:	28:27	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:28:27	Incident: INC0013376	Updated	In Progress	fsun	(empty)
Severity Looku	p Rules			0		1176592	2019-09-19 09:	28:26	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:28:26	Incident: INC0013377	Updated	Resolved	fsun	(empty)
				()		1176592	2019-09-19 09:	28:26	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:28:26	Event: 1176592	Updated	Resolved	fsun	(empty)
Device				()		1176592	2019-09-19 09:	23:22	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:23:22	Event: 1176592	Inserted	In Progress	fsun	(empty)
Device Properti	ks			()		1176592	2019-09-19 09:	23:22	fsundemo89+DEV+2197+EVENT+1705	INC0013377	(empty)	2019-09-19 09:23:22	Incident: INC0013377	Updated	In Progress	fsun	(empty)
Automations				()		1176577	2019-09-19 09:	03:34	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:03:34	Event: 1176577	Updated	Resolved	fsun	(empty)
Automation Pro	operties			()		1176577	2019-09-19 09:	03:34	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 09:03:34	Incident: INC0013376	Updated	Resolved	fsun	(empty)
Sessions Prope	rties			0		1176577	2019-09-19 08:	58:30	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:58:30	Incident: INC0013376	Updated	In Progress	fsun	(empty)
Dependents Tasks		*		()		1176577	2019-09-19 08:	58:30	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:58:30	Event: 1176577	Inserted	In Progress	fsun	(empty)
Tasks Catalog Templa	tes			()		1176570	2019-09-19 08:	53:35	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:53:35	Incident: INC0013376	Updated	Resolved	fsun	(empty)
▼ Maintenance				(j)		1176570	2019-09-19 08:	53:35	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:53:35	Event: 1176570	Updated	Resolved	fsun	(empty)
Maintenance Pr	roperties			()		1176570	2019-09-19 08:	48:31	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:48:31	Incident: INC0013376	Updated	In Progress	fsun	(empty)
V Supporting Imp	ports			()		1176570	2019-09-19 08:	48:31	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:48:31	Event: 1176570	Inserted	In Progress	fsun	(empty)
Organization				()		1176556	2019-09-19 08:	38:32	fsundemo89+DEV+2196+EVENT+1705	INC0013376	(empty)	2019-09-19 08:38:32	Incident: INC0013376	Updated	Resolved	fsun	(empty)

You can view a complete audit of all import data and transforms by going to the **Transform Histories** page (System Import Sets > Advanced > Transform History):

E	ransforn	n Histories G	io to Started	▼ Sea	arch							44 4	l 1 to	100 of 20440 🕨 🕨
₽ ⊗	All Q	≡ Started	≡ State	■ Completed	≡ Run time	≡ Set	≡ Import set table	≡ Total	≡ Inserts	≡ Updates	≡ Ignored	≡ Skipped	≡ Errors	≡ Transform Map
	(i)	2016-09-04 04:00:50	Complete	2016-09-04 04:00:50	0 Seconds	ISET0013291	ScienceLogic File System [u_sciencelogic_file_system]		⊥ msens	0 Optimies	0 gnored	<u>= экірреч</u> 1		0 ScienceLogic File System T-Map
	(j)	<u>2016-09-01</u> <u>12:00:27</u>	 Complete 	2016-09-01 12:00:27	0 Seconds	ISET0013275	ScienceLogic Network Interfaces [u_sciencelogic_adapters]		1	0	0	1	0	0 <u>ScienceLogic Adapter</u> <u>T-Map</u>
	(j)	<u>2016-09-02</u> <u>14:00:12</u>	 Complete 	2016-09-02 14:00:12	0 Seconds	ISET0013278	ScienceLogic Hardware Models [u_sciencelogic_hardware_models]		1	0	0	1	0	ScienceLogic 0 Hardware Model T- Map
	(j)	2016-09-01 16:00:44	 Complete 	2016-09-01 16:00:44	0 Seconds	ISET0013276	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	0 ScienceLogic File System T-Map
	(j)	<u>2016-08-31</u> <u>18:01:16</u>	 Complete 	2016-08-31 18:01:16	0 Seconds	ISET0013271	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	0 ScienceLogic File System T-Map
	(j)	2016-09-02 03:00:28	 Complete 	2016-09-02 03:00:28	0 Seconds	ISET0013280	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	0 ScienceLogic File System T-Map
	i	2016-09-01 20:01:03	 Complete 	2016-09-01 20:01:03	0 Seconds	ISET0013276	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	0 ScienceLogic File System T-Map
	i	2016-09-03 02:01:22	 Complete 	2016-09-03 02:01:22	0 Seconds	ISET0013286	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	0 ScienceLogic File System T-Map
	i	2016-09-01 12:00:59	 Complete 	2016-09-01 12:00:59	0 Seconds	ISET0013275	ScienceLogic Network Interfaces [u_sciencelogic_adapters]		1	0	0	1	0	0 ScienceLogic Adapter T-Map
	(j)	<u>2016-09-03</u> <u>12:00:12</u>	 Complete 	2016-09-03 12:00:12	0 Seconds	ISET0013283	ScienceLogic Hardware Models [u_sciencelogic_hardware_models]		1	0	0	1	0	ScienceLogic 0 Hardware Model T- Map
	(j)	2016-09-04 22:00:33	 Complete 	2016-09-04 22:00:33	0 Seconds	ISET0013290	ScienceLogic Network Interfaces [u_sciencelogic_adapters]		1	0	0	1	0	0 ScienceLogic Adapter T-Map
	í	<u>2016-09-01</u> <u>16:01:17</u>	 Complete 	2016-09-01 16:01:17	0 Seconds	ISET0013276	ScienceLogic File System [u_sciencelogic_file_system]		1	0	0	1	0	0 ScienceLogic File System T-Map

SL1 Event to ServiceNow Incident Impact/Urgency Matrix

By default, when SL1 triggers an Event, the Event is sent to ServiceNow through PowerFlow. The following mappings are currently in place for mapping the Severity of an SL1 Event to the Impact and Urgency of a ServiceNow Incident:

SL1 Event Severity	ServiceNow Incident Impact	ServiceNow Incident Urgency
Critical	1-High	1-High
Major	2-Medium	2-Medium
Minor	2-Medium	3-Low
Notice	3-Low	3-Low
Healthy	3-Low	3-Low

The Severity conversions are handled in an "onBefore" transform script under the "ScienceLogic (SL1) Incident" transform map that automatically deploys with the ScienceLogic Certified (Scoped) Application.

The "onBefore" transform script calls a script include called "taskMappingHelper" that handles the conversion from Severity to Impact or Urgency.

To customize a Severity to Impact or Urgency conversion rule:

1. In ServiceNow, create a new script include with new conversion rules. You can change the return values for SL1 Severity labels to the desired Impact and Urgency values. The following is an example:

```
1
      var taskMappingHelper = Class.create();
2 🔻
      taskMappingHelper.prototype = {
3
          initialize: function() {},
4
5
          //Impact and Urgency fields validation based on event's severity label
6 .
          determineImpactUrgency: function(severity) {
7
              severity = severity.toLowerCase();
8 -
              if (severity.includes("critical")) { //Critical
9
                  return "1+1";
              } else if (severity.includes("major")) { //Major
10 -
11
                  return "2+2";
12 •
              } else if (severity.includes("minor")) { //Minor
13
                  return "2+3";
14 -
              } else if (severity.includes("notice")) { //Notice
15
                  return "3+3";
              } else if (severity.includes("healthy")) { //Healthy
16 •
17
                  return "3+3";
18 •
              } else { //No Severity
                  return "";
19
20
              }
21
          },
```

NOTE: In the above example, if the SL1 Severity label is Minor, return the corresponding ServiceNow Incident Impact of 2 and Urgency of 3.

2. In the "onBefore" transform script under the "ScienceLogic (SL1) Incident" transform map:

- Modify line 60 to call the newly created script include.
- Modify line 61 to call the newly created function under script include with the same parameter source.u_event_severity_label.
 For example:

	ScienceLogic SL1: Incident Automation
Active order Inction of this script and the globals available to it vary depending on when the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script S	, i i i i i i i i i i i i i i i i i i i
Active order Inction of this script and the globals available to it vary depending on when the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script S	, i i i i i i i i i i i i i i i i i i i
Order Inction of this script and the globals available to it vary depending on when the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script Image: Comparison of the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script Image: Comparison of the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script Image: Comparison of the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script Image: Comparison of the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script Image: Comparison of the script is set to run. For more information will be script is set to run. For more information will detion with source field event_policy_cause is ''' (Sit Image: Comparison of the script is set to run. For more information will detion with source field event_policy_cause is ''' (
nction of this script and the globals available to it vary depending on when the script is set to run. For more information, see the Wiki. See also the article about the recommended form of the script. Script Script Scri	\checkmark
Script Scr	
Script Scr	
<pre>45 45 46 5 46 47 48 49 //Description field transformation validation with source field event_policy_cause 50 4 51 51 </pre>	
<pre>53 target.description = helper.formatHTNLtoTXT(source.u_event_policy_cause); 54 } 55 56 //Impact and Urgency fields transformation validation with source field event_severity_label 57 * if (source.u_event_severity_label != '') { 58 59 var impactUrgency = ''; 60 var impactUrgency = ''; 60 var impactUrgency = helper4.determineImpactUrgency(source.u_event_severity_label); 61 dispactUrgency = helper4.determineImpactUrgency(source.u_event_severity_label); 62 var splitinpactUrgency(source.u_event_severity_label); 63 target.impact = splitinpactUrgency(l); 64 target.impact = splitinpactUrgency[1]; 65 target.impact = splitinpactUrgency[1]; 66 target.impact = splitinpactUrgency[1]; 67 target.impact = splitinpactUrgency[1]; 68 target.impact = splitinpactUrgency[1]; 69 target.impact = splitinpactUrgency[1]; 60 target.impact = splitinpactUrgency[1]; 60 target.impact = splitinpactUrgency[1]; 61 target.impact = splitinpactUrgency[1]; 62 target.impact = splitinpactUrgency[1]; 63 target.impact = splitinpactUrgency[1]; 64 target.impact = splitinpactUrgency[1]; 65 target.impact = splitinpactUrgency[1]; 66 target.impact = splitinpactUrgency[1]; 67 target.impact = splitinpactUrgency[1]; 68 target.impact = splitinpactUrgency[1]; 69 target.impact = splitinpactUrgency[1]; 60 target.impact = splitinpactUrgency[1]; 61 target.impact = splitinpactUrgency[1]; 61 target.impact = splitinpactUrgency[1]; 61 target.impact = splitinpactUrgency[1]; 61 target.impact = splitinpactUrgency[1]; 62 target.impact = splitinpactUrgency[1]; 63 target.impact = splitinpactUrgency[1]; 64 target.impact = splitinpactUrgency[1]; 65 target.impact</pre>	

NOTE: By default, the Incident **Priority** field is read-only and must be set by selecting the Impact and Urgency values.

Adding Additional Fields to the Transform Map

If you require additional mandatory fields to be filled out to resolve an incident, you can add those fields to the **transform map** in ServiceNow.

For example, if you require four mandatory fields in the ServiceNow Incident—Assignment Group, IT Service, Service Component, and Description—to be filled out before that incident can be resolved in SL1, you would perform the following steps.

Main De	tails* Notes F	Related Records	s Resolution Information	Admin					
	*	Caller S	cience Logic	Q	H ^a (j)		Contact type	web	\$
	Behalf	of user		Q			Impact	Some Users	\$
UIP	* Cor	mpany M	lotorpoint Limited		0		Urgency	3 - Low	\$
	Lo	cation		Q	_		Priority (?)	4 - Low	
	* 1⊺s	service		Q			Major incident state		
	★ Service comp	oonent		Q			Owning group	0	K.
	Syn	nptom		Q	_		Assignment group	0	R.
	Configuratio	n item		Q			Assigned to	0	L.
	* Short descr	ription m	np-sql-2014-01: Host Resource	Storage l	tilization (E:\ Labe	el:Data Serial Number d	01ef7f2) has exceeded th	reshold 90%, currently 90.02%	Q
					Rela	ted Search Results >]		
	\star Descr	ription							

To add an assignment group:

- 1. Navigate to **User Administration > Groups** and select the assignment group you want to add. The Group record appears.
- 2. Right-click the gray task bar at the top and select Copy sys_id.

< Group Access Requests					
	Insert				
Access Requ	Insert and Stay				
-	Configure	> Q			
	Export	>			
support@n	View				
	Create Favorite				
	Copy URL	· ·			
04-05-2018	Copy sys_id				
Д	Show XML				
	History	>			
Access Requ	Reload form				
	support@n 04-05-2018	Access Req Insert and Stay Configure Export support@n View Create Favorite Copy URL 04-05-2018 Copy sys_id Show XML History Bload form			

- 3. In SL1, open to the "ServiceNow: Add/Update/Clear Incident" Run Book Action (Registry > Run Book > Actions).
- 4. Edit the Input Parameters of the Run Book Action to add the sys_id to the relevant parameter or parameters to assign the assignment group to one of the new, acknowledged, or cleared incidents that are mapped. After an incident is created, the assignment group value will not be changed by the Run Book Action.

In the following example, the assignment group is assigned to incidents that are cleared:

```
"assignment_group_ack": "",
"assignment_group_clear": "sys_id"
```

"assignment group new": "",

The *IT Service*, *Service Component*, and *Description* fields in our example must be filled in before an Incident can be closed. To do this, changes must be made in the transform maps that are provided in the form of update sets from ScienceLogic.

TIP: For more information about mapping new fields and other mappings options, see <u>https://docs.servicenow.com/bundle/newyork-platform-administration/page/script/server-scripting/concept/c MappingOptions.html</u>.

To add the **Description** field:

- 1. In ServiceNow, search for "transform map" in the filter navigator. Click **Transform Maps**.
- 2. In the list of transform maps, search for "ScienceLogic" in the field above the Name column.

3. Open the "ScienceLogic Incident" map:

Servicenuw servi	Service Management ScienceLogic + S System Administrator + Q D () ()									
(י 🔳 ו	able Tran	sform Maps New	Go to Order 💌	Şearch		44 4	1 to 8	of 8 🕨 🕨	
	- ·	All								
System Import Sets	\$\$ 	Q	■ Name	Search	Target table	Run business rules	Order		≡ Updated	
Create Transform Map			Search	Search	Search	Search	Search	Search	Search	
▼ Administration		i	<u>ScienceLogic</u> Incident	ScienceLogic Incident Import [u_imp_silo_incidents]	Incident [incident]	true	100	true	2018-05-18 20:44:15	
Transform Maps 🥒 ピ		i	Notification	Notification [imp_notification]	Incident [incident]	true	100	true	2008-12-28 22:08:39	
System LDAP		i	User	User [imp_user]	User [sys_user]	true	100	true	2015-07-07 07:32:42	
Transform Maps		i	Location	Location [imp_location]	Location [cmn_location]	true	100	true	2015-07-07 07:30:52	
		i	Computer	Computer [imp_computer]	Computer [cmdb_ci_computer]	true	100	true	2015-07-07 07:29:19	
		i	LDAP User Import	label [ldap_import]	User [sys_user]	true	100	true	2011-04-11 16:17:55	
		i	LDAP Group Import	label [ldap_group_import]	Group [sys_user_group]	true	100	true	2009-11-12 09:33:59	
		i	<u>ScienceLogic</u> <u>Event</u>	ScienceLogic Incident Import [u_imp_silo_incidents]	ScienceLogic Events [u_silo_events]	true	200	true	2018-05-18 21:27:35	

- The Field Maps table at the bottom of the page allows you to edit or create mappings from the ScienceLogic Incident Import table to the ServiceNow Incident table. Click [New] to create a new field mapping.
- 5. The **Source table** field should contain the ScienceLogic Incident Import and the **Target table** should include the ServiceNow Incident table:

Field Map New record			R *
Мар	ScienceLogic Incident Q	(i) Application	Global
Source table	ScienceLogic Incident Import [u_imp_s ▼	Target table	Incident [incident]
Source field	Action Policy	Target field	Active \$
Use source script		Coalesce	

- 6. To create a new mapping to copy the contents of the **Short description** field to the **Description** field, select Short description from the **Source field** drop-down menu.
- 7. In the Target field drop-down menu, select Description.
- 8. Click **Update** to save your changes.

The *IT Service* and *Service Component* fields in our example are set in the Transform Script in the "ScienceLogic Event" transform map. To set the fields:

- In ServiceNow, make sure you have the sys_id value for the target fields. If a field contains a magnifying glass, it will require a sys_id. If a field has a drop-down, type in the field you wish to apply from the drop-down. In the case of our example, the sys_id values of the two fields are required.
- 2. In your ServiceNow instance, navigate to the Transform Maps table and select "ScienceLogic Event".

3. In the ScienceLogic Event transform map page, click the **[Transform Script]** tab and open the "onAfter" script.

Table Transfor ScienceLogic F	rm Map Event		🖉 🗮 👓 Update	e Copy Delete 🛧
Current View: Default view (c	lick me for other views)	Application	ScienceLogic	(i)
* Source table	ScienceLogic Incident Import [u_imp_s V	Created	2018-05-18 21:27:35	
Active	\checkmark	* Target table	ScienceLogic Events [u_silo_events]	•
Run business rules	\checkmark	Order		200
Enforce mandatory fields	No	Run script		
Copy empty fields				
Update Copy De	elete			
Related Links				
Auto Map Matching Fields Transform Index Coalesce Fields				
Field Maps (16) Transfo	orm Scripts (2)			
Transform Scripts	Search		44 4	1 to 2 of 2 🕨 🍽 🖻
Map = ScienceLo	gic Event			
©w	hen 🗮 Script		≡ Order 🔺	≡ Active
i onAft	er (function runTransformSc	ript(source, map	10	00 true
i <u>onBe</u>	fore (function runTransformSc	ript(source, map	10	00 true

4. Add the following under the "//Update target record when the Event was cleared from Sciencelogic" text:

sl_INT.(target field) = '[sys_id of the source field]'; //(IT service
field)

sl_INT.(target field) = '[sys_id of the source field]'; //(Service component)

When ⑦	onAfter	Application ScienceLogic ①	1
		Active	
		Order 100	
of this script a	nd the global	Is available to it vary depending on when the script is set to run. For more information, see the Wiki. See also the article about the recommended	for
Script ?	§ 📮		
		<pre>(function runTransformScript(source, map, log, target /*undefined onStart*/) {</pre>	
	2	avent state management().	
	4	<pre>event_state_management();</pre>	
	5 *	<pre>function event_state_management(){</pre>	
	6	//Check ScienceLogic Events to see, if the Incident can be closed.	
	7	<pre>var sl_events = new GlideRecord('u_silo_events');</pre>	
	8	<pre>sl_events.addEncodedQuery('u_active=true^u_silo_task=' + source.u_task);</pre>	
	9	<pre>sl_events.query();</pre>	
	10 *	<pre>if(sl_events.getRowCount() == 0){</pre>	
	11 12	<pre>var sl_INT = new GlideRecord('incident'); sl_INT.get(target.u_silo_task);</pre>	
	13 •	if(source.u incident state == 6 && sl INT.close code.nil()){	
	14	//Update target record when the Event was cleared from Sciencelogic.	
	15	sl INT.close_code='Closed/Resolved by Caller';	
	16	sl_INT.close_notes=source.u_work_notes;	
	17	sl_INT.state= 6;	
	18 🔻	<pre>}else if(source.u_incident_state ==6 && !sl_INT.close_code.nil()){</pre>	
	19	//Update target record when Event was cleared From ServiceNow.	
	20	<pre>sl_INT.close_notes= sl_INT.close_notes + " (" + source.u_work_notes + ")";</pre>	
	21	}	
]	22	<pre>sl_INT.update();</pre>	
]	23	3	
]	24 25	return;	
]	25		
		<pre>})(source, map, log, target);</pre>	
		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	

5. To find the target field, make a temporary mapping to see what the target field is. This mapping can be deleted once you know the target field.

Field Maps (14) Transform Scripts (3) Versions (1)									
E Field Maps New									
ŝ	\equiv Source field	Target field							
	(j) <u>u short description</u>	short_description							
	i <u>u contact type</u>	contact_type							
	i <u>u active</u>	active							
	i <u>u short description</u>	description							
	i <u>u_assignment_group</u>	ass <mark>i</mark> gnment_group							
	i <u>u correlation id</u>	correlation_id							
	i sys_updated_by	caller_id							
	i <u>u urgency</u>	urgency							
	i <u>u cmdb ci</u>	cmdb_ci							
	i <u>u work notes</u>	work_notes							
	i <u>u impact</u>	u_service_component							
	i <u>u impact</u>	impact							
	(j) [Script]	company							
	() [Script]	location							
	Actions on selected rows 2								

6. Click **[Update]** to save your changes. The selected fields will be added into an Incident on closure.

Chapter

4

Troubleshooting the Incidents SyncPack

Overview

This chapter contains troubleshooting resources, procedures, and the answers to frequently asked questions to use with the "ServiceNow Incidents" SyncPack.

This chapter covers the following topics:

Initial Troubleshooting Steps	57
Resources for Troubleshooting	.57
Frequently Asked Questions	.61

Initial Troubleshooting Steps

PowerFlow acts as a middle server between data platforms. For this reason, the first steps should always be to ensure that there are no issues with the data platforms with which PowerFlow is talking. There might be additional configurations or actions enabled on ServiceNow or SL1 that result in unexpected behavior. For detailed information about how to perform the steps below, see *Resources for Troubleshooting*.

SL1 PowerFlow

- 1. Run docker service 1s on the PowerFlow server.
- 2. Note the Docker container version, and verify that the Docker services are running.
- 3. If a certain service is failing, make a note the service name and version.
- If a certain service is failing, run docker service ps <service_name> to see the historical state of the service and make a note of this information. For example: docker service ps iservices_ contentapi.
- 5. Make a note of any logs impacting the service by running docker service logs *<service_name>*. For example: docker service logs iservices_couchbase.

ServiceNow

- 1. Make a note of the ServiceNow version and SyncPack version, if applicable.
- 2. Make a note of the SyncPack application that is failing on PowerFlow.
- 3. Make a note of what step is failing in the application, try running the application in debug mode, and capture any traceback or error messages that occur in the step log.

Resources for Troubleshooting

This section contains port information for PowerFlow and troubleshooting commands for Docker, Couchbase, and the PowerFlow API.

Useful PowerFlow Ports

- https://<IP of PowerFlow>:8091. Provides access to Couchbase, a NoSQL database for storage and data retrieval.
- https://<IP of PowerFlow>:15672. Provides access to the RabbitMQ Dashboard, which you can use to monitor the service that distributes tasks to be executed by PowerFlow workers.
- https://<IP of PowerFlow>/flower/dashboard. Provides access to Flower, a tool for monitoring and administrating Celery clusters.

IMPORTANT: Port 5556 must be open for both PowerFlow and the client.

Helpful Docker Commands

PowerFlow is a set of services that are containerized using Docker. For more information about Docker, see the Docker tutorial.

Use the following Docker commands for troubleshooting and diagnosing issues with PowerFlow:

Viewing Container Versions and Status

To view the PowerFlow version, SSH to your PowerFlow instance and run the following command:

docker service ls

In the results, you can see the container ID, name, mode, status (see the *replicas* column), and version (see the *image* column) for all the services that make up PowerFlow:

D	NAME	MODE	REPLICAS	IMAGE	PORTS
mmihuj5v30i	iservices_gui	replicated		repository.auto.sciencelogic.local:5000/is-gui:1.7.0	*:80->80/tcp,*:443->443/tcp
0vs9ltlwnh3	iservices redis	replicated		redis:4.0.2	
lm6hljtumlf	iservices_flower	replicated		repository.auto.sciencelogic.local:5000/is-worker:1.7.0	*:5555->5555/tcp
h3pt2181rsf	iservices_scheduler	replicated		repository.auto.sciencelogic.local:5000/is-worker:1.7.0	
timltvg6xhx	iservices_contentapi	replicated		repository.auto.sciencelogic.local:5000/is-api:1.7.0	*:5000->5000/tcp
yln9qgsudmi	iservices rabbitmg	replicated		rabbitmg:3	
lul9h8jsfs6	iservices visual	replicated		dockersamples/visualizer:latest	*:8081->8080/tcp
cy38w8buauw	iservices_couchbase	replicated		repository.auto.sciencelogic.local:5000/is-couchbase:1.7.0	*:8091->8091/tcp,*:8092->809
->8093/tcp,*:80	94->8094/tcp,*:11210->112	10/tcp			
lbxstxoz7uf	iservices steprunner	replicated	5/5	repository.auto.sciencelogic.local:5000/is-worker:1.7.0	

Restarting a Service

Run the following command to restart a single service:

docker service update --force <service name>

Stopping all PowerFlow Services

Run the following command to stop all PowerFlow services:

docker stack rm iservices

Restarting Docker

Run the following command to restart Docker:

systemctl restart docker

NOTE: Restarting Docker does not clear the queue.

Diagnosis Tools

Multiple diagnosis tools exist to assist in troubleshooting issues with the PowerFlow platform:

- **Docker PowerPack**. This PowerPack monitors your Linux-based PowerFlow server with SSH (the PowerFlow ISO is built on top of an Oracle Linux Operating System). This PowerPack provides key performance indicators about how your PowerFlow server is performing. For more information on the Docker PowerPack and other PowerPacks that you can use to monitor PowerFlow, see the "Using SL1 to Monitor SL1 PowerFlow" chapter in the **SL1 PowerFlow Platform** manual.
- *Flower*. This web interface tool can be found at the /flower endpoint. It provides a dashboard displaying the number of tasks in various states as well as an overview of the state of each worker. This tool shows the current number of active, processed, failed, succeeded, and retried tasks on the PowerFlow platform. This tool also shows detailed information about each of the tasks that have been executed on the platform. This data includes the UUID, the state, the arguments that were passed to it, as well as the worker and the time of execution. Flower also provides a performance chart that shows the number of tasks running on each individual worker.
- **Debug Mode**. All applications can be run in "debug" mode via the PowerFlow API. Running applications in debug mode may slow down the platform, but they will result in much more detailed logging information that is helpful for troubleshooting issues. For more information on running applications in Debug Mode, see *Retrieving Additional Debug Information*.
- Application Logs. All applications generate a log file specific to that application. These log files can be found at /var/log/iservices and each log file will match the ID of the application. These log files combine all the log messages of all previous runs of an application up to a certain point. These log files roll over and will get auto-cleared after a certain point.
- Step Logs. Step logs display the log output for a specific step in the application. These step logs can be accessed via the PowerFlow user interface by clicking on a step in an application and bringing up the Step Log tab. These step logs display just the log output for the latest run of that step.
- **Service Logs**. Each Docker service has its own log. These can be accessed via SSH by running the following command:

docker service logs -f <service name>

Retrieving Additional Debug Information (Debug Mode)

The logs in PowerFlow use the following **loglevel** settings, from most verbose to least verbose:

- 10. Debug Mode.
- 20. Informational.
- 30. Warning. This is the default settings if you do not specify a loglevel.
- 40. Error.

WARNING: If you run applications in Debug Mode ("loglevel": 10), those applications will take longer to run because of increased I/O requirements. Enabling debug logging using the following process is the only recommended method. ScienceLogic does not recommend setting "loglevel": 10 for the whole stack with the **docker-compose** file.

To run an application in Debug Mode using the PowerFlow user interface:

- 1. Select the PowerFlow application from the Applications page.
- 2. Hover over the **[Run]** button and select *Custom Run* from the pop-up menu. The **Custom Run** window appears.
- 3. Select the Logging Level. Debug is the most verbose and will take longer to run.
- 4. Specify the configuration object for the custom run in the **Configuration** field, and add any JSON parameters in the **Custom Parameters** field, if needed.
- 5. Click [Run].

To run an application in Debug Mode using the API:

1. POST the following to the API endpoint:

```
https://<PowerFlow IP>/api/v1/applications/run
```

2. Include the following in the request body:

```
{
  "name": "<application_name>",
  "params": {
  "loglevel": 10
  }
}
```

After running the application in Debug Mode, review the step logs in the PowerFlow user interface to see detailed debug output for each step in the application. This information is especially helpful when trying to understand why an application or step failed:

=	Application			🕐 Help	Notifications 105 isa	admin ~ Scie	nceLogic
	Delete Devices From SL1	/ 0	Open Editor	≡ Reports	🛩 Timeline 🛛 🛱 Ro	eplay 🕨 Run	🌣 Configure
٢							ଷ
							٩
\$		Pull Affected Device Ir	nfo				\bigcirc
	Pull Disabled Devices from VCUG in SL1	from SL1 (GQL)	Verify Device Dele Requests	te 🔶 Delete De	vices		G
07		Pull Affected Device Ir from SL1 (MySQL)	nfo				
	STEP LOG STEP DATA				Cop	py ③ Download	C Full screen
	Module \uparrow	Date (UTC-4) \uparrow	Log Level ↑ Mess Filter ▼	age			
	∨ BaseStep	Aug 29, 2023 10:48:21, 347	INFO Exec	uting: Pull Disabled Devices from VCUG in SL1 -	steps/PullAndProcessDisabledDev	vices.py	D
	∨ ipaas_logger	Aug 29, 2023 10:48:21, 348	FLOW Start	Pull Disabled Devices from VCUG in SL1			ľ
	∨ ipaas_logger	Aug 29, 2023 10:48:21, 355	FLOW Step	Pull Disabled Devices from VCUG in SL1 still fail	ed after 0 retries		Ō
	∧ BaseStep	Aug 29, 2023 10:48:21, 357	ERROR Trace	back (most recent call last): File "/usr/local/lib/p	ython3.8/site-packages/ipaascore/	/BaseStep	٦
	retry_step task.retry(File "/usr/local/lib/ "/usr/local/lib/python3.8/site-packages/	′python3.8/site-packages/celery/app ipaascore/BaseStep.py'', line 51, in ir	p/task.py", line 706, in retry raise_with_context(nner_execute execute = method(self) File "/var/s	tep self.retry_step(task=task, exc=err, File "/usr/ exc) File "/usr/local/lib/python3.8/site-packages/ yncpacks_virtualenvs/servicenow_cmdb_syncpa ons.MissingRequiredStepParameter: taræt_vcu	ipaascore/BaseStep.py", line 579, i ck/lib/python3.8/site-packages/se	in execute_step self.execut ervicenow_cmdb_syncpack	e() File s/steps

You can also run an application in debug using curl via SSH:

- 1. SSH to the PowerFlow instance.
- 2. Run the following command:

```
curl -v -k -u isadmin:<password> -X POST "https://<your_
hostname>/api/v1/applications/run"
  -H 'Content-Type: application/json' -H 'cache-control: no-cache' -d
'{"name":
"interface_sync_sciencelogic_to_servicenow","params": {"loglevel":
10}}'
```

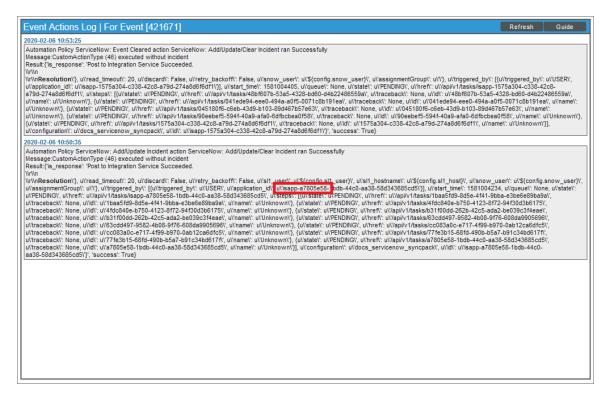
Frequently Asked Questions

This section contains a set of frequently asked questions (FAQs) and the answers to address those situations.

Why are Incidents not getting created in ServiceNow?

- 1. In SL1, go to the **[Events Console]** (Classic user interface) or the **Events** page (SL1 user interface) and locate the event that was created.
 - In the SL1 user interface, click the [Actions] button (••••) for that event and select View Automation Actions.
 - In the Classic user interface, click the **View Notification Log** mailbox icon () for that event.

The Event Actions Log window appears:



- 2. On the **Event Actions Log** window, verify that the Run Book Action was triggered, and that the Run Book Action successfully posted to PowerFlow.
- In the "Add/Update Incident action" pane, locate the PowerFlow run ID, which is the first six or seven characters of the "isapp" integration ID associated with that run of the integration. For example: isappa7805e58.
- 4. In the PowerFlow user interface, go to the **Applications** page and open the "Create or Update ServiceNow Incident from SL1 Event" application.
- 5. Click the **[Timeline]** button () to locate the run that contains the PowerFlow run ID associated with that run of the integration (from step 3, above).
- 6. Click **[View Run]** for that run on the **Timeline** and review the logs in the **Step Log** panel to see where the application failed.

What if my Incident does not have a CI?

For an incident with an active event:

- 1. In SL1, go to the **[Events Console]** (classic user interface) or the **Events** page (new user interface) and locate the event that was created.
 - In the SL1 user interface, click the **[Actions]** button (***) for that event and select View Automation Actions.
 - In the Classic user interface, click the **View Notification Log** mailbox icon (^(D)) for that event.

The Event Actions Log window appears

- 2. On the **Event Actions Log** window, locate the PowerFlow run ID, which is the first six or seven characters of the "isapp" integration ID associated with that run of the integration. For example: *isapp*-a7805e58.
- 3. In the PowerFlow user interface, go to the **Applications** page and open the application that used that run.
- 4. Review the Step Log and confirm that the device class was mapped in the "Sync Devices from SL1 to ServiceNow" application.
- 5. Confirm that the "Sync Devices from SL1 to ServiceNow" application is running at least every 24 hours, and that the "Sync Devices from SL1 to ServiceNow" application has run within 24 hours of that event sync run.

What if the PowerFlow user interface is unresponsive and Incidents are not being generated in ServiceNow?

If the PowerFlow user interface is unresponsive, and Incidents are not being generated in ServiceNow, this might mean that during the deployment process, a change to the firewall rules for monitoring broke the ingress network for Docker.

To address this issue, run the following command to restart Docker every time you make a firewall or network configuration change:

systemctl restart docker

Why are Incident numbers not populated in SL1 on Incident creation in ServiceNow?

If an incident exists in ServiceNow, but incident data is not getting back to SL1, first make sure that the "Sync Incident Details from ServiceNow to SL1 Events" PowerFlow application was set up on a schedule. Next, run the application in Debug mode and view the step logs as needed to further troubleshoot the issue.

Why am I not getting any Incidents after disabling the firewall?

If you disabled the firewall to enable SNMP monitoring on PowerFlow, but were not able to connect, you should add the additional rule you need.

© 2003 - 2023, 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.



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

International: +1-703-354-1010