



CrowdStrike Integrations

CrowdStrike Falcon Automation Synchronization PowerPack Version 1.0.0

CrowdStrike Falcon Automation PowerPack Version 100

Table of Contents

Introduction to the CrowdStrike Falcon Automation Synchronization PowerPack	3
What is the CrowdStrike Falcon Automation Synchronization PowerPack ?	4
Prerequisites for this Synchronization PowerPack	4
Contents of the Synchronization PowerPack	4
PowerFlow Applications	4
Configuration Object	5
Steps	5
Installing the Synchronization PowerPack	5
Downloading the Synchronization PowerPack	5
Importing the Synchronization PowerPack	6
Installing the Synchronization PowerPack	6
Configuring Applications for the CrowdStrike Falcon Automation Synchronization PowerPack	8
Creating and Aligning a Configuration Object in PowerFlow	9
Creating a Configuration Object	9
Aligning a Configuration Object and Configuring PowerFlow Applications	12
Scheduling PowerFlow Applications	13
Introduction to the CrowdStrike Falcon Automation PowerPack	18
What is the CrowdStrike Falcon Automation PowerPack?	19
Installing the CrowdStrike Falcon Automation PowerPack	19
Configuring Action Policy Credentials	21
Creating a SOAP/XML Credential to Access SL1 PowerFlow	22
Creating a SOAP/XML Credential to Access SL1 PowerFlow in the Classic User Interface	23
Configuring CrowdStrike Falcon Automation Event Policies	25
Standard Event Policies	26
Configuring the CrowdStrike Falcon Automation Action Policies	27
Editing the CrowdStrike Falcon Automation Action Policies	28
CrowdStrike Falcon Automation PowerPack Automation Policies	30
Standard Automation Policies	31

Chapter

1

Introduction to the CrowdStrike Falcon Automation Synchronization PowerPack

Overview

This chapter describes how you can configure and use the *CrowdStrike Falcon Automation Synchronization PowerPack* with the PowerFlow platform to integrate SL1 events and CrowdStrike detections.

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

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

This chapter covers the following topics:

What is the CrowdStrike Falcon Automation Synchronization PowerPack ?	4
Prerequisites for this Synchronization PowerPack	4
Contents of the Synchronization PowerPack	4
Installing the Synchronization PowerPack	5

What is the CrowdStrike Falcon Automation Synchronization PowerPack ?

The *CrowdStrike Falcon Automation* includes a configuration object, applications, and steps that bidirectionally sync jobs, pipeline jobs, and node status between CrowdStrike and SL1.

Prerequisites for this Synchronization PowerPack

This Synchronization PowerPack requires the following:

- **SL1 PowerFlow platform version:** 2.3.0 or later
- *CrowdStrike Synchronization PowerPack* version 100 or later
- **SL1 version:** 11.1.0 or later. For details on upgrading SL1, see the appropriate SL1 [Release Notes](#).
- The following dependencies are included in the Synchronization PowerPack:
 - SL1_Notifications >= 1.0.2
 - base_steps_syncpack >= 1.3.2
- Administrator access to both SL1 and CrowdStrike
 - CrowdStrike administrator access to the Administration Portal
 - CrowdStrike administrator access to the GUI Portal

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

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

NOTE: ScienceLogic highly recommends that you disable all firewall session-limiting policies as the firewalls will drop HTTPS requests resulting in data loss.

Contents of the Synchronization PowerPack

This section lists the contents of the *CrowdStrike Falcon Automation Synchronization PowerPack*.

PowerFlow Applications

- **Fetch Detections from CrowdStrike and Send Alert to SL1**. This application acquires tokens and New Detections from CrowdStrike and creates alerts for SL1.
- **Clear Detection from Cache**. This application acquires and saves event details to send to SL1.

For more information about how to configure these applications, see [Configuring Applications for the CrowdStrike Falcon Automation Synchronization PowerPack](#).

Configuration Object

- **CrowdStrike Sample Configuration**. This configuration object can be used as a template after the Synchronization PowerPack is installed on the PowerFlow system.

Steps

The following steps are included in this Synchronization PowerPack:

- Fetch Detections and Generate Payloads for SL1
- Fetch New Detections from CrowdStrike
- Get Alerted Detections from Cache
- Get Each Detection and Create SL1 Alerts
- Get Event Details and Clear Detections ID

Installing the Synchronization PowerPack

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

Downloading the Synchronization PowerPack

To locate and download the Synchronization PowerPack:

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

NOTE: After you download a Synchronization PowerPack, you can import it to your PowerFlow system using the PowerFlow user interface.

Importing the Synchronization PowerPack

To import a Synchronization PowerPack in the PowerFlow user interface:

1. On the **SyncPacks** page (☺) of the PowerFlow user interface, click **[Import SyncPack]**. The **Import SyncPack** page appears.
2. Click **[Browse]** and select the **.whl** file for the Synchronization PowerPack you want to install. You can also drag and drop a **.whl** file to the **Import SyncPack** page.
3. Click **[Import]**. PowerFlow registers and uploads the Synchronization PowerPack. The Synchronization PowerPack is added to the **SyncPacks** page.
4. You will need to activate and install the Synchronization PowerPack in PowerFlow. For more information, see [Activating and Installing a Synchronization PowerPack](#).

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

Installing the Synchronization PowerPack


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

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

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

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

2. Click **[Yes]** to confirm the activation and installation. When the Synchronization PowerPack is activated, the **SyncPacks** page displays a green check mark icon (✓) for that Synchronization PowerPack. If the activation or installation failed, then a red exclamation mark icon (⚠) appears.
3. For more information about the activation and installation process, click the check mark icon (✓) or the exclamation mark icon (⚠) in the **Activated** column for that Synchronization PowerPack. For a successful installation, the "Activate & Install SyncPack" application appears, and you can view the Step Log for the steps. For a failed installation, the **Error Logs** window appears.

4. If you have other versions of the same Synchronization PowerPack on your PowerFlow system, you can click the **[Actions]** button () for that Synchronization PowerPack and select *Change active version* to activate a different version other than the version that is currently running.

Chapter

2

Configuring Applications for the CrowdStrike Falcon Automation Synchronization PowerPack


Overview

This chapter describes how to set up the PowerFlow applications for the *CrowdStrike Falcon Automation Synchronization PowerPack*.

This chapter covers the following topics:

<i>Creating and Aligning a Configuration Object in PowerFlow</i>	9
<i>Scheduling PowerFlow Applications</i>	13

Creating and Aligning a Configuration Object in PowerFlow

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

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



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

Creating a Configuration Object

For this Synchronization PowerPack, you should make a copy of the "CrowdStrike Sample Configuration" configuration object, which is the sample configuration file that was installed with the *CrowdStrike Falcon Automation Synchronization PowerPack*.

TIP: The "CrowdStrike Sample Configuration" configuration object contains all of the required variables. Simply update the variables from that object to match your SL1 and CrowdStrike settings.

To create a configuration object based on the "CrowdStrike Sample Configuration" configuration object:

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

Crowdstrike Sample Configuration



Toggle JSON Editor

Description
Configuration values for integrating with Crowdstrike API's

Version
1.0.0

Configuration Data Values

Name	Value	Encrypted	
sl1_host	10.64.229.154	<input type="checkbox"/>	Encrypted
sl1_user	em7admin	<input type="checkbox"/>	Encrypted
sl1_password	Kza3Bx0xxCNI55AcIKIc	<input checked="" type="checkbox"/>	Encrypted
crowdstrike_client_id	CzbehX7RW/NdnTbUqE	<input checked="" type="checkbox"/>	Encrypted
crowdstrike_client_secret	2A+a64skmeYhGrqqxJL	<input checked="" type="checkbox"/>	Encrypted
crowdstrike_base_url	https://api.us-2.crowdstr	<input type="checkbox"/>	Encrypted

Add Value

Copy as

Save

3. Click **[Copy as]**. The **Create Configuration** pane appears.
4. Complete the following fields:
 - **Friendly Name**. Type a name for the configuration object that will display on the **Configurations** page.
 - **Description**. Type a brief description of the configuration object.
 - **Author**. Type the user or organization that created the configuration object.
 - **Version**. Type a version of the configuration object.
5. In the **Configuration Data** field, update the default variable definitions to match your PowerFlow configuration:
 - **sl1_host**. Type the hostname or IP address of the SL1 system the alerts will synchronize with.
 - **sl1_password**. Type the password for your SL1 system.
 - **sl1_user**. Type the username for your SL1 system.
 - **crowdstrike_url**. Enter the URL for your CrowdStrike system.
 - **crowdstrike_username**. Type the username for your CrowdStrike system.
 - **crowdstrike_password**. Type the password for your CrowdStrike system.
 - **job_name**. Type the name for your CrowdStrike job.
 - **receiver_mail**. Type the email address that you want to receive updates on SL1 events and your CrowdStrike jobs.
 - **sender_mail**. Type the email address that you want updates on SL1 events and your CrowdStrike jobs to send from.
 - **sender_mail_password**. Type the password for the sender email address that you entered.
 - **mailserver**. Type the server for your sender email.
 - **mailserverport**. Type the port for your sender email.

The following fields are required only if you choose to manually create a virtual device for your CrowdStrike instance:


 - **device_class_id**. Type the device class ID for your CrowdStrike instance.
 - **collector_group_id**. Type the collector group ID for your CrowdStrike instance.
 - **device_id**. Type the device ID for your CrowdStrike instance.
6. Click **[Save]**. You can now align this configuration object with one or more applications.

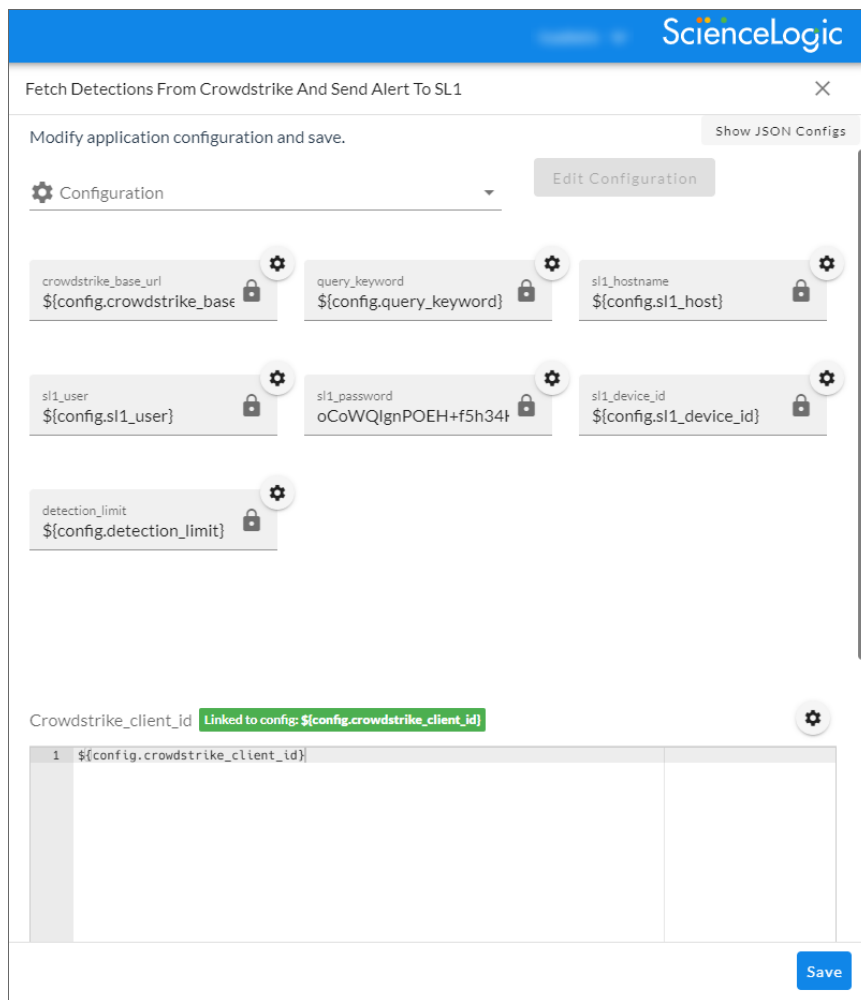
NOTE: For more information about the CrowdStrike terms and concepts in this section, see the CrowdStrike documentation.

Aligning a Configuration Object and Configuring PowerFlow Applications

With this Synchronization PowerPack, you can create SL1 events based on CrowdStrike jobs. You will need to align the *CrowdStrike Falcon Automation* applications with the relevant configuration object in PowerFlow, and, if needed, update any other fields on the **Configuration** pane for the applications.

To align the configuration object with the relevant PowerFlow applications:

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



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

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

- Click **[Save]** to align that configuration with the application.
- Repeat this process for the other PowerFlow applications.

Scheduling PowerFlow Applications

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

To create a schedule on PowerFlow version 2.5.0 and later:

- On the **Applications** page (📄), click the **[Schedule]** button for the application you want to schedule. The **Scheduler** window appears:

Name	Type	Last Run	Runs
Hourly*1	frequency	-	0
830 Daily	crontab	-	0

- In the **Schedule List** pane, click the down arrow icon (▼) next to an existing schedule to view the details for that schedule.
- In the **Schedule Creator** pane, complete the following fields for the default **Frequency** setting:
 - Schedule Name.** Type a name for the schedule.
 - Frequency in seconds.** Type the number of seconds per interval that you want to run the application.

- **Custom Parameters.** Type any JSON parameters you want to use for this schedule, such as information about a configuration file or mappings.
4. To use a cron expression, click the **Switch to Cron Expression** toggle to turn it blue. If you select this option, you can create complicated schedules based on minutes, hours, the day of the month, the month, and the day of the week:

Schedule Creator Switch to Frequency in Seconds

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

Schedule Name
Saturday Schedule

A unique name for the new schedule.

Cron Expression key operators

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

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

Runs app: "Every 0 and 30th minute past every hour on Sat" (UTC -4)
Derived from given values in fields above.

Custom Parameters (Optional)

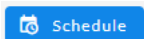
1	{}
---	----

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

Close Save Schedule

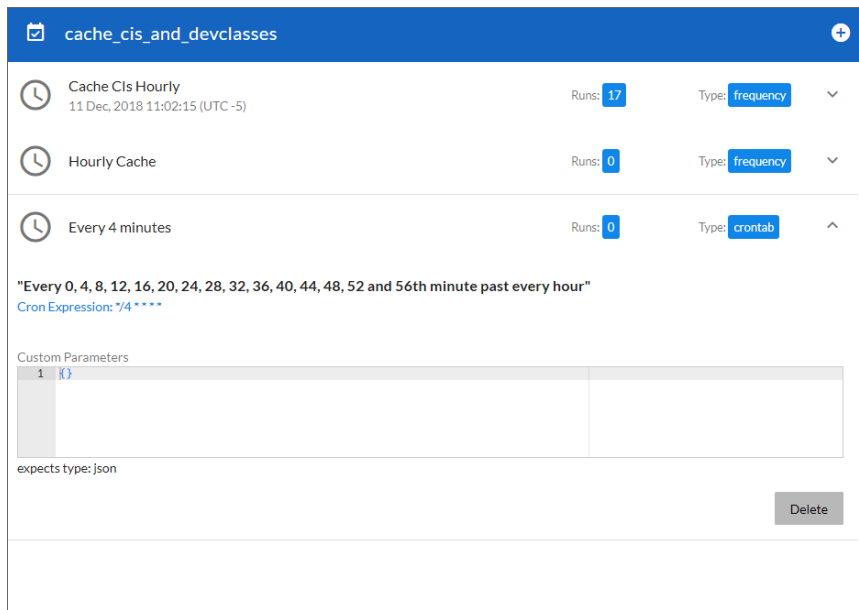
As you update the cron expression, the **Schedule** window displays the results of the expression in more readable language, such as *Runs app: "Every 0 and 30th minute past every hour on Sat"*, based on 0,30 in the **Minutes** field and 6 in the **Day of Week** field.

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



To create a schedule on PowerFlow version 2.4.1 or earlier:

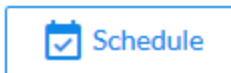
1. On the **Applications** page (📄), click the **[Schedule]** button for the application you want to schedule. The **Schedule** window appears, displaying any existing schedules for that application:



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



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

4. In the **Schedule** window, complete the following fields:
 - **Schedule Name**. Type a name for the schedule.
 - **Switch to**. Use this toggle to switch between a cron expression and setting the frequency in seconds.
 - **Cron expression**. Select this option to schedule the application using a cron expression. If you select this option, you can create complicated schedules based on minutes, hours, the day of the month, the month, and the day of the week. As you update the cron expression, the **Schedule** window displays the results of the expression in more readable language, such as *Expression: "Every 0 and 30th minute past every hour on the 1 and 31st of every month", based on */30 * */30 * **.
 - **Frequency in seconds**. Type the number of seconds per interval that you want to run the application.
 - **Custom Parameters**. Type any JSON parameters you want to use for this schedule, such as information about a configuration file or mappings.
5. Click **[Save Schedule]**. The schedule is added to the list of schedules on the initial **Schedule** window. Also, on the **Applications** page, the word "Scheduled" appears in the **Scheduled** column for this application, and the **[Schedule]** button contains a check mark:



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

To view or delete an existing schedule:

1. On the **Applications** page, click the **[Schedule]** button for the application that contains a schedule you want to delete. The **Scheduler** window appears.
2. Click the down arrow icon () to view the details of an existing schedule.
3. To delete the selected schedule, click the Actions icon () and select **[Delete]**.

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

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

Chapter

3

Introduction to the CrowdStrike Falcon Automation PowerPack

Overview

This chapter describes the how to integrate CrowdStrike with SL1 using the *CrowdStrike Falcon Automation* PowerPack. This PowerPack also contains the Run Book Automation policies and Run Book Action policies you can use with the *CrowdStrike Falcon Automation Synchronization* PowerPack in PowerFlow.

NOTE: This PowerPack is available with a ScienceLogic SL1 Standard solution. Contact your ScienceLogic Customer Success Manager or Customer Support to learn more.

This chapter covers the following topics:

<i>What is the CrowdStrike Falcon Automation PowerPack?</i>	19
<i>Installing the CrowdStrike Falcon Automation PowerPack</i>	19

What is the CrowdStrike Falcon Automation PowerPack?

The *CrowdStrike Falcon Automation PowerPack* includes automation policies and action policies that bidirectionally sync jobs, pipeline jobs, and node status between CrowdStrike and SL1.

The *CrowdStrike Falcon Automation PowerPack* includes:

- CrowdStrike: Clear Detection ID Run Book Automation policies
- CrowdStrike: Clear Detection ID Run Book Action policy
- CrowdStrike: Alert to Event event policy
- PowerFlow CrowdStrike SOAP/XML Credentials

Installing the CrowdStrike Falcon Automation PowerPack

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

IMPORTANT: You must install and configure the *CrowdStrike Falcon Automation Synchronization PowerPack* version 1.0.0 before using the *CrowdStrike Falcon Automation PowerPack*.

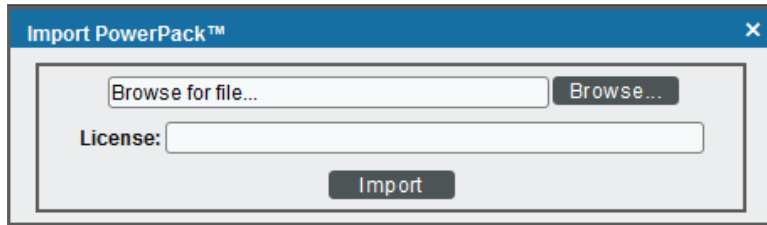
NOTE: The *CrowdStrike Falcon Automation PowerPack* requires SL1 version 11.1.0 or later. For details on upgrading SL1, see the appropriate SL1 [Release Notes](#).

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

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site at <https://support.sciencelogic.com/s/powerpacks>.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).

3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*. The **Import PowerPack** dialog box appears:



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

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

Chapter

4

Configuring Action Policy Credentials

Overview

This chapter describes how to configure CrowdStrike for monitoring by SL1 using the *CrowdStrike Falcon Automation PowerPack*.

This chapter covers the following topics:

Creating a SOAP/XML Credential to Access SL1 PowerFlow	22
Creating a SOAP/XML Credential to Access SL1 PowerFlow in the Classic User Interface	23

Creating a SOAP/XML Credential to Access SL1 PowerFlow

After you have integrated your CrowdStrike and PowerFlow systems, you must create a SOAP/XML credential so that the action policies included in the PowerPack can access your PowerFlow system. The *CrowdStrike Falcon Automation* PowerPack includes a template for a SOAP/XML credential that you can edit for use with your SL1 PowerFlow system.

NOTE: If you are on an SL1 system prior to version 11.1.0, you will not be able to duplicate the sample credential. It is recommended that you create your new credentials using [the SL1 classic user interface](#) so you do not overwrite the sample credential(s).

To create a SOAP/XML credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the **PowerFlow CrowdStrike** sample credential, then click its **[Actions]** icon (⋮) and select **Duplicate**. A copy of the credential, called **PowerFlow CrowdStrike copy** appears.

The screenshot shows the 'Edit Credential' form with the following details:

- Name:** PowerFlow Crowdstrike copy
- All Organizations:** (Toggle is blue)
- Select the organizations the credential belongs to:** (Dropdown menu)
- Timeout (ms):** 5000
- Content Encoding:** text/xml
- Method:** POST
- HTTP Version:** http/1.1
- URL:** https://10.2.11.157
- HTTP Auth User:** isadmin
- HTTP Auth Password:** *****
- Proxy Hostname/IP:** (Empty field)
- Proxy Port:** 0
- Proxy Password:** *****
- Proxy User:** (Empty field)
- Embedded Password [%P]:** *****
- Embed Value [%1]:** (Empty field)
- Embed Value [%2]:** (Empty field)

3. Supply values in the following fields:
 - **Profile Name.** Type a new name for the credential.
 - **All Organizations.** Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations.

- **URL.** Type the host name for your PowerFlow system.
 - **HTTP Auth User.** Type the administrator username for your PowerFlow
 - **HTTP Auth Password.** Type the administrator password for your PowerFlow system.
4. Click **[Save & Close]**.
 5. SL1 assigns the credential an ID number. Take note of the ID number for the new credential on the **Credentials** page, in the **ID** column. You will need the ID number when editing the input parameters of the automation actions included in the *CrowdStrike Falcon Automation* PowerPack.

Creating a SOAP/XML Credential to Access SL1 PowerFlow in the Classic User Interface

To create a SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **PowerFlow CrowdStrike** sample credential and click its wrench icon (🔧). The **Credential Editor** modal window appears.

The screenshot shows the 'Credential Editor [96]' window. The title bar indicates 'Edit SOAP/XML Credential #96'. The window is divided into several sections:

- Basic Settings:** Profile Name (PowerFlow CrowdStrike), Content Encoding ([text/xml]), Method ([POST]), HTTP Version ([HTTP/1.1]), URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name] (https://10.2.11.157), HTTP Auth User (isadmin), HTTP Auth Password (masked with dots), and Timeout (seconds) (5).
- Proxy Settings:** Hostname/IP, Port (0), and User.
- CURL Options:** A list of options including CAINFO, CAPATH, CLOSEPOLICY, CONNECTTIMEOUT, COOKIE, COOKIEFILE, COOKIEJAR, COOKIELIST, CRLF, CUSTOMREQUEST, and DNSCACHETIMEOUT.
- Soap Options:** Embedded Password [%P] and four Embed Value [%1] through [%4] fields.
- HTTP Headers:** A section with a '+ Add a header' button.

Buttons for 'New', 'Reset', 'Save', and 'Save As' are visible at the bottom of the window.

3. Supply values in the following fields:
 - **Profile Name.** Type a new name for the credential.
 - **Content Encoding.** Select *text/xml*.
 - **Method.** Select *POST*.

- **HTTP Version.** Select *HTTP/1.1*.
 - **URL.** Type the host name for your PowerFlow system.
 - **HTTP Auth Password.** Type the administrator password for your PowerFlow system.
 - **Timeout (seconds).** Type "5"
4. Click the **[Save As]** button to save the new SOAP/XML credential.
 5. SL1 assigns the credential an ID number. Take note of the ID number for the new credential on the **Credentials** page in the **ID** column or at the top of the **Credential Editor** modal. You will need the ID number when editing the input parameters of the automation actions included in the *CrowdStrike Falcon Automation PowerPack*.

Chapter

5

Configuring CrowdStrike Falcon Automation Event Policies

Overview

This chapter describes how to configure the event policies found in the *CrowdStrike Falcon Automation PowerPack*.


This chapter covers the following topics:

<i>Standard Event Policies</i>	26
--------------------------------------	----


Standard Event Policies

The *CrowdStrike Falcon Automation* PowerPack includes one standard API event policy, "CrowdStrike: Alert to Event", that you can enable to trigger the events detected by the applications included in the *CrowdStrike Falcon Automation* PowerPack and its associated automation action policy.

To enable the event policies:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Click the Actions menu () for the event policy and select *Edit*.
3. In the **Event Policy Editor** page, click on the **Enable Event Policy** toggle to enable the event policy.
4. Click **[Save]**.

To enable the event policies in the SL1 classic user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Click the wrench icon () for the event policy.
3. In the **Operational State** field, select *Enabled*.
4. Click **[Save]**.

Chapter

6

Configuring the CrowdStrike Falcon Automation Action Policies

Overview

This chapter describes how to edit the action policies included in the *CrowdStrike Falcon Automation* PowerPack so that the action policies can communicate with your SL1 PowerFlow system.

This chapter covers the following topics:

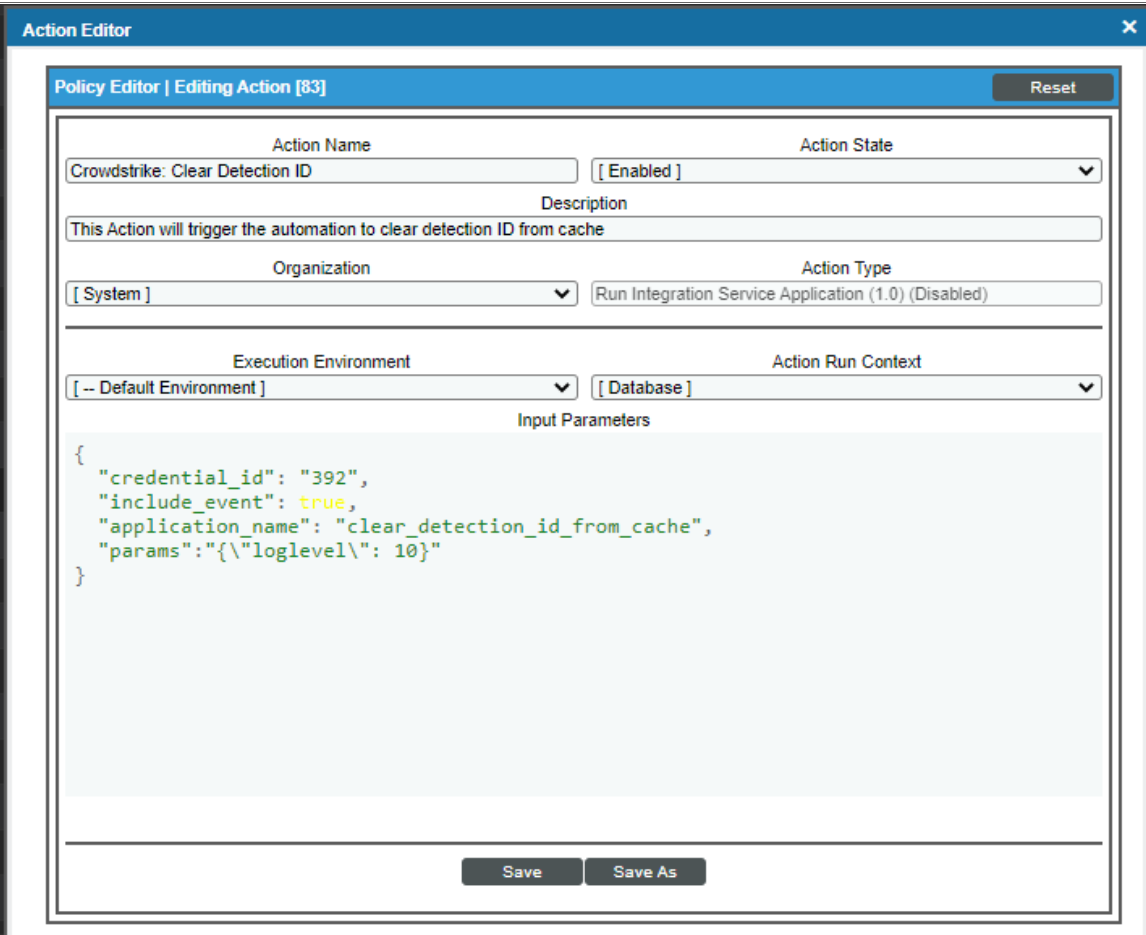
<i>Editing the CrowdStrike Falcon Automation Action Policies</i>	28
--	----

Editing the CrowdStrike Falcon Automation Action Policies

The *CrowdStrike Falcon Automation PowerPack* includes one action policy that uses the "Run Integration Service Application" action type to trigger the PowerFlow application that collects data from CrowdStrike. You can specify the credential ID in a JSON structure that you enter in the **Input Parameters** field in the **Action Policy Editor** modal.

To edit the action policies included in the PowerPack:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Locate the action policy that you want to use, and then click its wrench icon (🔧). The **Editing Action** page appears:



The screenshot shows the 'Action Editor' modal window. The title bar reads 'Action Editor' with a close button (X). The main content area is titled 'Policy Editor | Editing Action [83]' and includes a 'Reset' button. The form contains the following fields:

- Action Name:** Crowdstrike: Clear Detection ID
- Action State:** [Enabled]
- Description:** This Action will trigger the automation to clear detection ID from cache
- Organization:** [System]
- Action Type:** Run Integration Service Application (1.0) (Disabled)
- Execution Environment:** [-- Default Environment]
- Action Run Context:** [Database]
- Input Parameters:** A JSON object:

```
{
  "credential_id": "392",
  "include_event": true,
  "application_name": "clear_detection_id_from_cache",
  "params": {"loglevel": 10}
}
```

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

3. In the **Input Parameters** field, change the values of the following parameters:
 - **credential_id**. Change the value to the credential ID that you noted earlier when [creating a credential for your PowerFlow system](#). This parameter is required.
 - **include_event**. Leave the value as "true".

- ***application_name***. Leave the default application value.
- ***params***. Leave the default parameter value.

4. Click **[Save]**.

Chapter

7

CrowdStrike Falcon Automation PowerPack Automation Policies

Overview

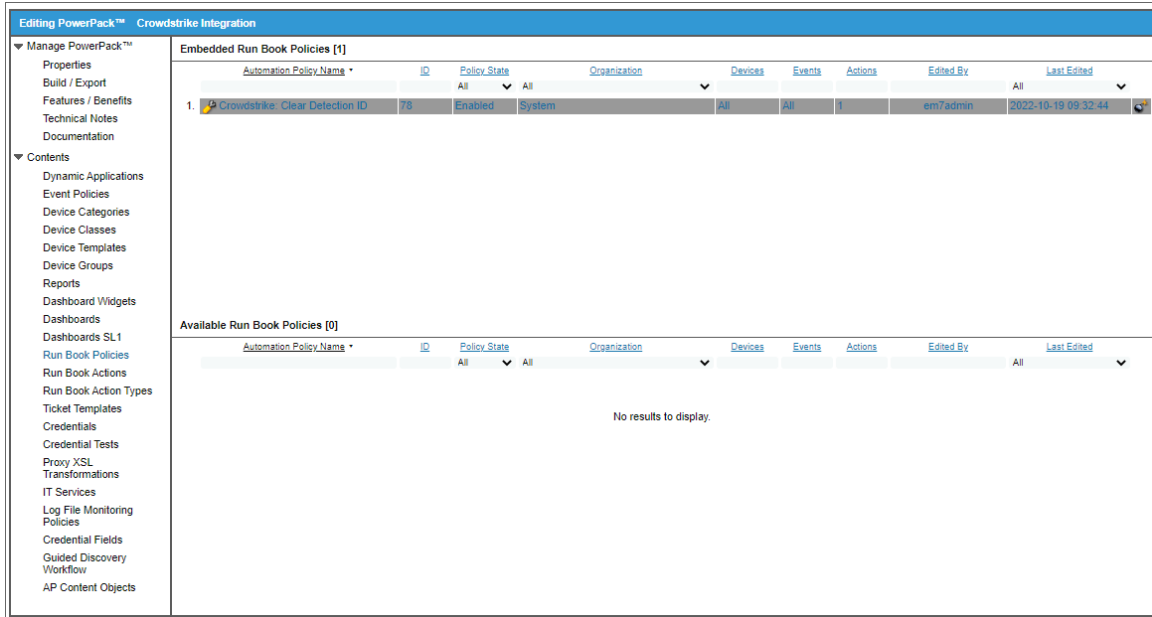
This chapter describes the automation policies found in the *CrowdStrike Falcon Automation PowerPack*.

This chapter covers the following topics:

<i>Standard Automation Policies</i>	31
---	----

Standard Automation Policies

The *CrowdStrike Falcon Automation* PowerPack includes one standard automation policy that you can enable, shown in the following figure:



This policy updates the SL1 event with the state of the associated CrowdStrike job. When a node is offline, a failure occurs, or a major event is detected in CrowdStrike, an SL1 event is created and the associated event is updated with any job details.

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

Automation Policy Name	Aligned Events	Automation Action
Crowdstrike: Clear Detection ID	All Events	Run Integration Service Application [100] CrowdStrike: Clear Detection ID

© 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/company/legal>.

ScienceLogic

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

International: +1-703-354-1010