CrowdStrike Falcon SyncPack

Release Notes Version 1.0.0

Overview

Version 1.0.0 of the "CrowdStrike Falcon" SyncPack describes how to use CrowdStrike with the PowerFlow platform and provides integration between SL1 events and CrowdStrike detections.

This SyncPack uses the "CrowdStrike Falcon Automation" PowerPack.

This document covers the following topics:

Features Included in this Release

The following applications are included in this SyncPack:

- ***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.

The following configuration object is included in the SyncPack:

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

The following steps are included in this SyncPack:

- 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 Detection ID

TIP: To view the latest manuals for the SL1 PowerFlow Platform, see the ***SL1 PowerFlow*** page. To view the latest release notes for PowerFlow, see ***SL1 PowerFlow Release Notes***.

System Requirements

"CrowdStrike Falcon" SyncPack version 1.0.0 requires:

- SL1 PowerFlow platform version 2.4.0 or later
- SL1 version 11.2.0 or later. For details on upgrading SL1, see the relevant *SL1 Platform Release Notes*.
- "Base Steps" SyncPack version 1.3.2 or later
- "CrowdStrike Falcon Automation" PowerPack version 100 or later
- Administrator access to CrowdStrike

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

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

Installing the SyncPack

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

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 this 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 .zip file containing the SyncPack.

After you download a SyncPack, you can import it to the PowerFlow platform using the PowerFlow user interface.

To import a SyncPack in the PowerFlow user interface:

1. On the **SyncPacks** page, click **[Import SyncPack]**. The **Import SyncPack** page appears.
2. Click **[Browse]** and select the **.whl** file for the SyncPack you want to install. You can also drag and drop a **.whl** file to the **Import SyncPack** page.
3. Click **[Import]**. PowerFlow registers and uploads the SyncPack. The SyncPack is added to the **SyncPacks** page.

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.

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

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

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

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

2. Click **[Yes]** to confirm the activation and installation. When the SyncPack is activated, the **SyncPacks** page displays a green check mark icon for that SyncPack. If the activation or installation failed, then a red exclamation mark icon appears.
3. For more information about the activation and installation process, click the check mark icon or the exclamation mark icon in the **Activated** column for that SyncPack. For a successful installation, the "Activate & Install SyncPack" PowerFlow 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.

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.

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

International: +1-703-354-1010