



ELK Stack SyncPack

Version 1.0.0

Table of Contents

Introduction to the ELK Stack SyncPack	3
What Can I Do with this SyncPack?	4
Contents of the SyncPack	4
PowerFlow Applications	4
Configuration Object	4
Steps	4
Installing the ELK Stack SyncPack	5
Prerequisites for this SyncPack	6
Installing the ELK Stack SyncPack	6
Downloading the SyncPack	6
Importing the SyncPack	7
Installing the SyncPack	7
Installing the ELK Stack Automation PowerPack	8
Configuring PowerFlow Applications for the ELK Stack SyncPack	9
Workflow for Configuring the SyncPack	10
Configuring SL1	10
Configuring PowerFlow	10
Configuring SL1	10
Enabling the ELK Stack Event Policies	10
Creating a SOAP/XML Credential to Access PowerFlow	10
Editing the ELK Stack Run Book Actions	11
Enabling the ELK Stack Run Book Automations	12
Configuring PowerFlow	12
Creating and Aligning a Configuration Object in PowerFlow	12
Creating a Configuration Object	13
Aligning a Configuration Object and Configuring PowerFlow Applications	14
Scheduling PowerFlow Applications	14

Chapter

1

Introduction to the ELK Stack SyncPack

Overview

This chapter describes how you can configure and use the "ELK Stack" SyncPack with the PowerFlow platform to integrate SL1 events and ELK detections.

"ELK" stands for the grouping of the Elasticsearch, Logstash, and Kibana applications. Elasticsearch is a search and analytics engine. Logstash is a server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch. Kibana lets users visualize data with charts and graphs in Elasticsearch.

This SyncPack uses the "ELK Stack Automation" PowerPack.

This chapter covers the following topics:

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

What Can I Do with this SyncPack?

The "ELK Stack" SyncPack automatically triggers ELK based on SL1 events, which removes the need for manual search, logging and data visualization. Changes are synchronized between the two systems, so users making changes in ELK or SL1 can see each those changes without having make the changes manually in both systems.

"ELK" stands for the grouping of the Elasticsearch, Logstash, and Kibana applications. Elasticsearch is a search and analytics engine. Logstash is a server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch. Kibana lets users visualize data with charts and graphs in Elasticsearch.

The SyncPack automates the sharing and exchange of logs so that you can easily search log data, use logs to enrich incidents and tickets, and stash logs for later use.

You can also configure this SyncPack to generate an alert in SL1 if any log is inserted to Logstash at a specified time.

Contents of the SyncPack

This section lists the contents of the "ELK Stack" SyncPack.

PowerFlow Applications

- **Get Data from External Source.** This application acquires data from external sources to update ELK statuses in SL1.
- **Search Data in ELK.** This application searches data in ELK and posts updates to SL1.
- **Get Data from SL1.** This application acquires data from SL1 to send to ELK and back to SL1 for updates.

For more information about how to configure these applications, see [Configuring Applications for the ELK Stack SyncPack](#).

Configuration Object

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

Steps

The following steps are included in this SyncPack:

- Get Log Data from SL1
- Get Search Results from ELK
- Post Update To SL1
- Send Data to ELK
- Update ELK Status To SL1

Chapter

2

Installing the ELK Stack SyncPack

Overview

This chapter describes the how to install the "ELK Stack" SyncPack and the "ELK Stack Automation" PowerPack.

This chapter covers the following topics:

<i>Prerequisites for this SyncPack</i>	6
<i>Installing the ELK Stack SyncPack</i>	6
<i>Installing the ELK Stack Automation PowerPack</i>	8

Prerequisites for this SyncPack

This SyncPack requires the following:

- The latest "ELK Stack Automation" PowerPack
- An Elastic Cloud account
- Administrator access to both SL1 and ELK:
 - ELK administrator access to the Administration Portal
 - ELK administrator access to the GUI Portal

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

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

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

Installing the ELK Stack SyncPack

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

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 & SyncPacks*.

3. In the **Search** field, search for the SyncPack and select it from the search results. The **Release Version** page appears.
4. On the **[Files]** tab, click the down arrow next to the SyncPack version that you want to install, and select *Show File Details*. The **Release File Details** page appears.
5. Click the **[Download File]** button to download the SyncPack.

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

Importing the SyncPack

To import a SyncPack in the PowerFlow user interface:

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

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

Installing the SyncPack

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

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

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

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

2. Click **[Yes]** to confirm the activation and installation. When the SyncPack is activated, the **SyncPacks** page displays a green check mark icon (✓) for that SyncPack. If the activation or installation failed, then a red exclamation mark icon (❗) appears.

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

Installing the ELK Stack Automation PowerPack

The "ELK Stack Automation" PowerPack includes automation policies and event policies that bidirectionally sync jobs, pipeline jobs, and node status between ELK and SL1. This PowerPack also comes with one example credential.

NOTE: The "ELK Stack Automation" PowerPack requires SL1 version 11.1.0 or later. For details on upgrading SL1, see the [SL1 Platform 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 the PowerPack:

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

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

Configuring PowerFlow Applications for the ELK Stack SyncPack

Overview

This chapter describes how to set up the run book automations in SL1, and how to set up the PowerFlow applications for the "ELK Stack" SyncPack.

This chapter covers the following topics:

<i>Workflow for Configuring the SyncPack</i>	10
<i>Configuring SL1</i>	10
<i>Configuring PowerFlow</i>	12

Workflow for Configuring the SyncPack

Configuring SL1

1. [Enable the ELK Stack event policies](#)
2. [Create a SOAP/XML credential to access PowerFlow](#)
3. [Edit the ELK Stack run book actions](#)
4. [Enable the ELK Stack run book automations](#)

Configuring PowerFlow

1. [Create a PowerFlow configuration object](#)
2. [Align and configure the ELK Stack PowerFlow applications](#)
3. [Schedule the PowerFlow applications](#)

Configuring SL1

Enabling the ELK Stack Event Policies

The "ELK Stack Automation" PowerPack includes the following event policies that you can enable to trigger the events detected by the applications included in the "ELK Stack" SyncPack:

- "ELK ExternalLog"
- "ELK: Sync SL1 Log"
- "ELK: Search"


To enable the event policies:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Click the check boxes for all three event policies. A row of buttons appear at the top of the list.
3. Click **[Enable]**. The Status for all three policies is updated to "Enabled".

Creating a SOAP/XML Credential to Access PowerFlow

You will need to create a SOAP/XML credential so that the action policies included in the "ELK Stack Automation" PowerPack can access your PowerFlow system.

To create a SOAP/XML credential:

1. In SL1, go to the **Credentials** page (Manage > Credentials).
2. Locate the "ELK PowerFlow" sample credential, then click its **[Actions]** icon () and select **Duplicate**. A copy of the credential, called **ELK PowerFlow copy** appears.
3. Select the new credential and complete the following fields:
 - **Name**. Type a new name for the credential.
 - **All Organizations**. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations.
 - **URL**. Type the URL for your PowerFlow system.
 - **HTTP Auth User**. Type the username for your PowerFlow system.
 - **HTTP Auth Password**. Type the password for your PowerFlow system.
4. Click **[Save & Close]**.
5. Take note of the SL1-assigned ID number for the new credential on the **Credentials** page, in the **ID** column. You will need the ID number when editing the input parameters of the run book actions included in the "ELK Stack Automation" PowerPack, below.


Editing the ELK Stack Run Book Actions

The "ELK Stack Automation" PowerPack includes three action policies:

- "ELK: ExtLog"
- "ELK: Index Create"
- "ELK: Search"

These action policies use the corresponding "Run Integration Service Application" action type to trigger the PowerFlow application that collects data from the ELK Stack.

To edit the action policies included in the PowerPack:

1. In SL1, go to the **Actions** page (Registry > Run Book > Actions).
2. Locate the ELK action policy that you want to use and click its wrench icon () . The **Editing Action** page appears.
3. In the **Input Parameters** field, change the values of the following parameters:
 - **credential_id**. Change the value to the credential ID that you noted earlier when creating a credential for your PowerFlow system in the previous procedure. 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. Make sure the **Action State** is set to *Enabled*, and then click **[Save]**.


Enabling the ELK Stack Run Book Automations

The "ELK Stack Automation" PowerPack includes the following run book automation policies that you can enable:

- "ELK: ExtLog"
- "ELK: Index Create"
- "ELK: Search"

These run book automation policies update the SL1 event with the state of the associated ELK job. When a node is offline, a failure occurs, or a major event is detected in ELK, an SL1 event is created and the associated event is updated with any job details.

To enable the run book automations:


1. In SL1, go to the **Automation** page (Registry > Run Book > Automation).
2. Locate an ELK automation policy and click its wrench icon (). The **Automation Policy Editor** page appears.
3. Update the following fields:
 - **Policy State**. Select *Enabled*.
 - **Policy Priority**. Select *High* to ensure that this PowerFlow automation policy is added to the top of the queue.
 - **Available Actions**. If it is not already selected, select the "Run Integration Service Application: <name>" action that corresponds with the ELK automation policy you selected in step 2, and click the arrows to move it to **Aligned Actions**.

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

4. Click [**Save**].
5. Repeat steps 2-4 for the remaining ELK run book automation policies.

Configuring PowerFlow

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 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.

Creating a Configuration Object

For this SyncPack, you should make a copy of the "ElasticSearch Logstash Kibana Configuration" configuration object, which is the sample configuration file that was installed with the "ELK Stack" SyncPack.

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

To create a configuration object based on the "ElasticSearch Logstash Kibana Configuration" configuration object:

1. In the PowerFlow user interface, go to the **Configurations** page (⚙️).
2. Click the **[Actions]** button (⋮) for the "ElasticSearch Logstash Kibana Configuration" configuration object and select *Edit*. The **Configuration** pane appears.
3. Click **[Copy as]**. The **Create Configuration** pane appears.
4. Complete the following fields:
 - **Friendly Name**. Type a name for the configuration object that will display on the **Configurations** page.
 - **Description**. Type a brief description of the configuration object.
 - **Author**. Type the user or organization that created the configuration object.
 - **Version**. Type a version of the configuration object.
5. In the **Configuration Data** field, include the required block of code to ensure that the applications aligned to the ELK configuration object is successful:
 - **sl1_host**. Type the hostname or IP address of the SL1 system the alerts will synchronize with.
 - **sl1_user**. Type the username for your SL1 system.
 - **sl1_password**. Type the password for your SL1 system.
 - **elk_username**. Type the username for your ELK system.
 - **elk_password**. Type the password for your ELK system.
 - **elk_document_url**. Enter the URL for your ELK document.
 - **ELK_Cloud_id**. Type the ELK Cloud ID for login.
 - **create_index_name**. Type the name of the log data.
 - **URI_for_log_data**. Type the Log Data URL.
 - **from_date**. Type the start date in dd-mm-yyyy hh:mm:ss.
 - **to_date**. Type the end date in dd-mm-yyyy hh:mm:ss.

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

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

Aligning a Configuration Object and Configuring PowerFlow Applications

With this SyncPack, you can create SL1 events based on ELK jobs. You will need to align the PowerFlow applications from the "ELK Stack" SyncPack 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 an ELK Stack PowerFlow application and click **[Configure]**. The **Configurations** pane for that application appears.
2. From the **Configurations** drop-down, select the configuration object you want to use.

NOTE: The values for **sl1_hostname** and the other parameters that appear in the **Configuration** pane with a padlock icon (🔒) are populated 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.

3. Update the remaining fields on the **Configurations** pane as needed.
4. Click **[Save]** to align that configuration with the application.
5. 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:

1. On the **Applications** page (📄), click the **[Schedule]** button for the application you want to schedule. The **Scheduler** window appears.
2. In the **Schedule List** pane, click the down arrow icon (▼) next to an existing schedule to view the details for that schedule.
3. In the **Schedule Creator** pane, complete the following fields for the default **Frequency** setting:

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

Schedule Creator
Switch to Frequency in Seconds

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

Schedule Name
Saturday Schedule

A unique name for the new schedule.

Cron Expression key operators

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

Minutes
0,30

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)

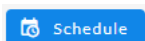
1	{}	
---	----	--

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:



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 ELK instances are involved with PowerFlow, you should create an individual configuration object for each SL1 or ELK 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 ELK instance. Creating copies of a PowerFlow application from a SyncPack for the purpose of distinguishing between domains is not supported, and will result in issues on upgrades.

© 2003 - 2024, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see <https://sciencelogic.com/company/legal>.

ScienceLogic

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

International: +1-703-354-1010