GUIDE

STORMSHIELD LOG SUPERVISOR

SOAR SETTINGS GUIDE

Version 2

Document last updated: July 4, 2024

Reference: sls-en_soar_settings_gde

Table of contents

Change log

Date	Description
July 4, 2024	New document

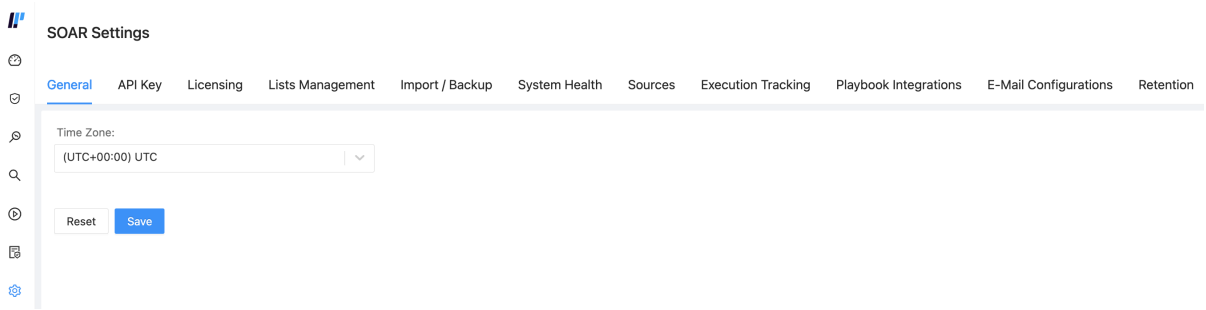
Getting started

Welcome to the SLS version 2 SOAR Settings Guide.

You can manage how your SOAR works, including:

- General
- API Key
- Licensing
- Lists Management
- Import/Backup
- System Health
- Sources
- Execution Tracking
- Playbook Integrations
- E-Mail Configurations
- Retention

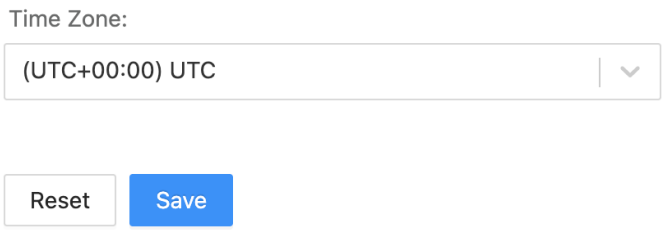
Go to `Settings >> SOAR Settings` from the navigation bar.



In this document, Stormshield Log Supervisor is referred to in its short form SLS. Images used in this document are from the partner vendor's (Logpoint) software program. In your SLS, the graphics may vary but user experience is exactly the same.

General

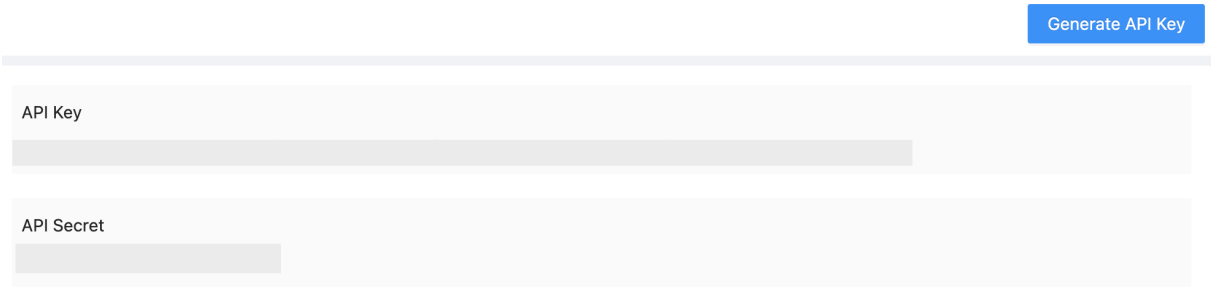
Use **General** to select the timezone.



1. Go to `Settings >> SOAR Settings` from the navigation bar and click **General**.
2. Select the Time Zone from the drop-down.
3. Click **Save**.

API Key

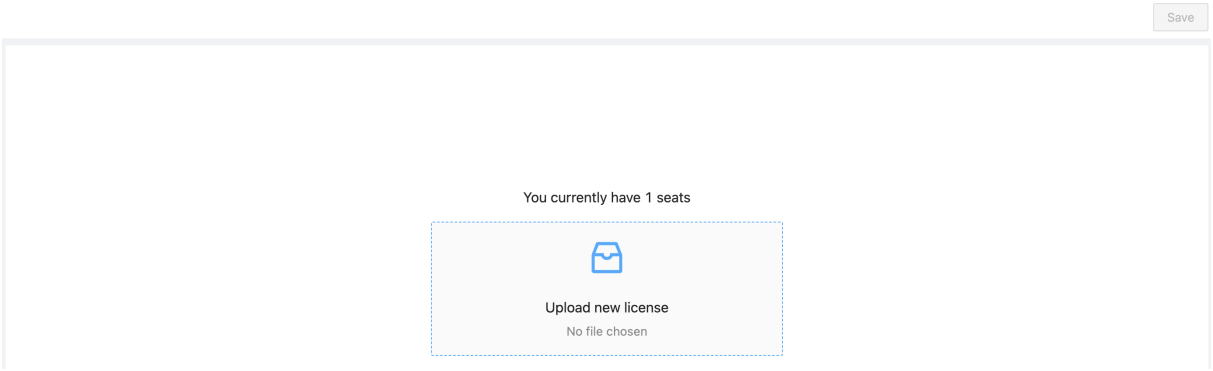
You can use the API Key of SLS SOAR to access features and data of SLS SOAR externally.



1. Go to `Settings >> SOAR Settings` from the navigation bar and click **API Key**.
2. Click **Generate API Key**.

Licensing

After the fresh installation, one seat is available to access SOAR in a single active session by default. However, you need to add the SLS SOAR license for multiple concurrent access.



Adding a SLS SOAR License

Before adding a license, contact SLS Sales team and provide them your Hardware Key. Go to `Settings >> System Settings` from the navigation bar and click **SLS License** to access the Hardware Key. The Stormshield Sales team then sends you the license key based on your requirements.

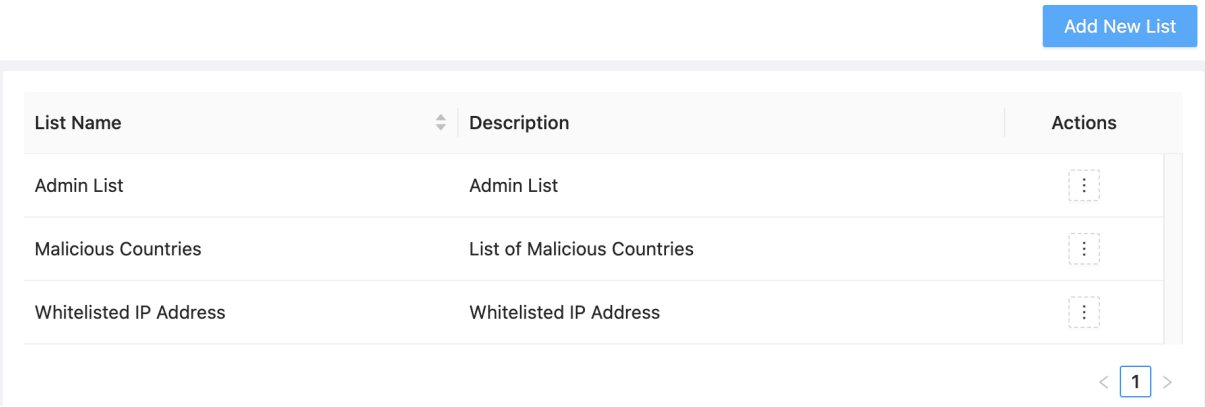
1. Download the **License Key**.
2. Go to `Settings >> SOAR Settings` from the navigation bar and click **Licensing**.
3. Click **Upload new license** and select the downloaded **License Key** file.
4. Click **Save**.

Lists Management

You can maintain a collection of values as a List. You can use the list to search for the incidents associated with its values. For example, if you create a list named **Admin Users** having the usernames as the list members, you can use the list to query incidents associated with all the usernames that are members of the **Admin Users** list. You can also use the list to define a trigger condition or perform bulk actions.

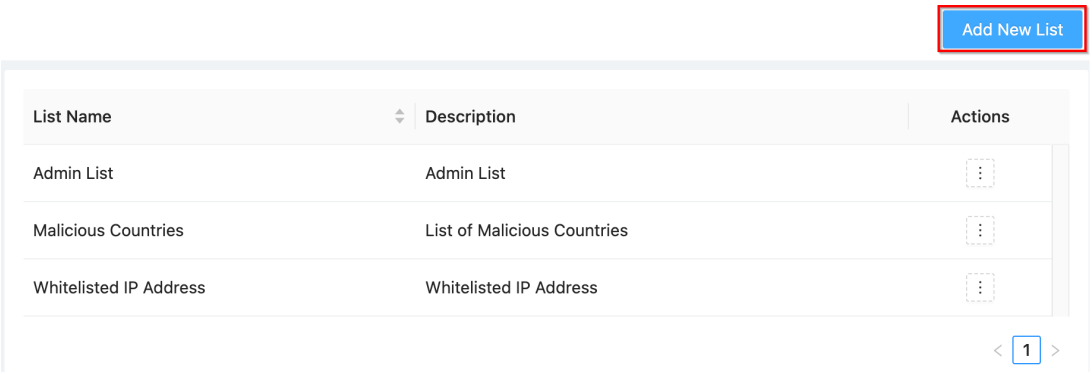
The list remains unchanged until you add or remove the list members.

Go to `Settings >> SOAR Settings` from the navigation bar and click **Lists Management** to view, add, edit, and delete the list configured in SLS SOAR.



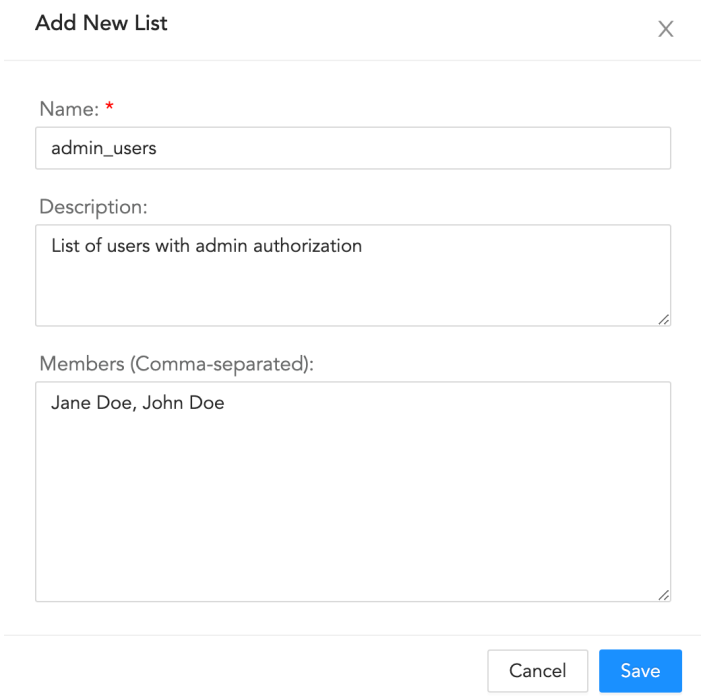
Adding a List

1. Go to `Settings >> SOAR Settings` from the navigation bar and click **Lists Management**.
2. Click **Add New List**.



3. Enter the List's **Name** and **Description**.

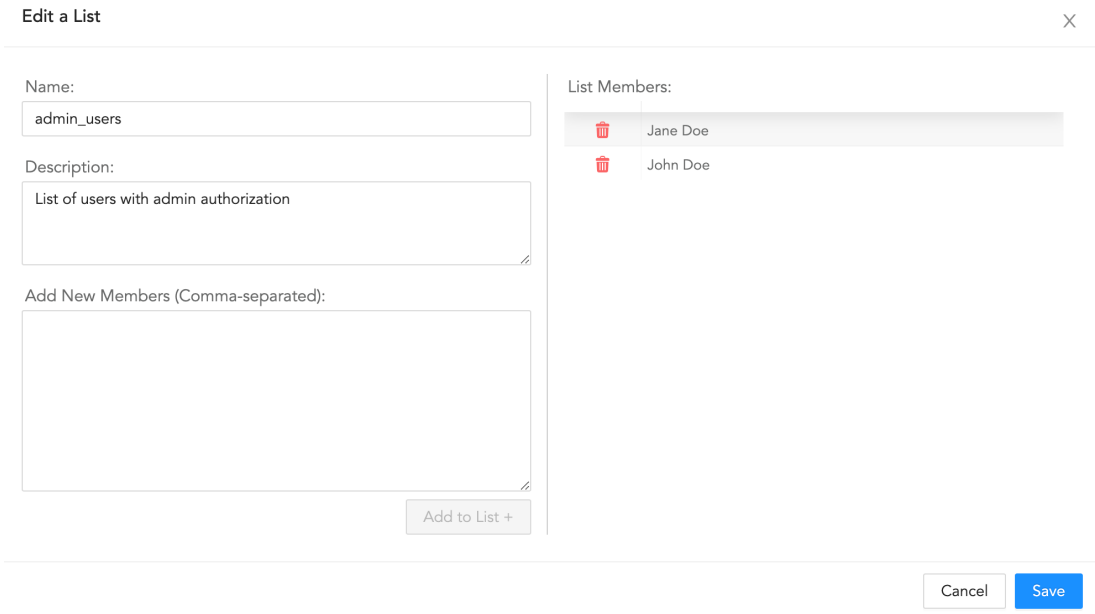
4. Enter the **Members** of the List seperated by commas.



5. Click **Save**.

Editing a List

1. Go to `Settings >> SOAR Settings` from the navigation bar and click **Lists Management**.
2. Hover over the (⋮) icon and Click the **Edit** option.
3. Edit the information.



4. Click **Save**.

Deleting a List

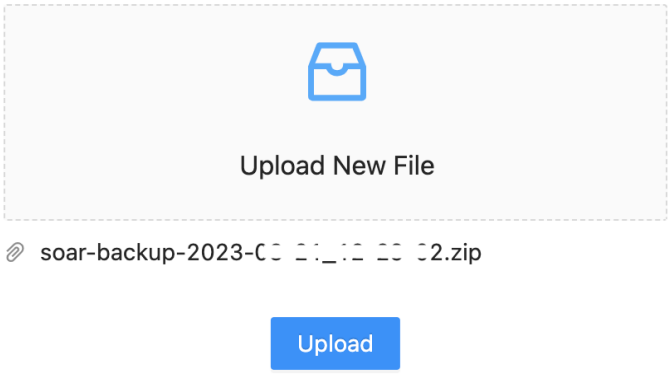
1. Go to `Settings >> SOAR Settings` from the navigation bar and click **Lists Management**.
2. Hover over the (⋮) icon and Click the **Delete** option.
3. Click **Delete**.

Import/Backup

Import

You can import configuration from other devices into SLS SOAR.

1. Go to `Settings >> SOAR Settings` from the navigation bar and click **Import/Backup**.
2. Click **Upload New File** to upload the file.



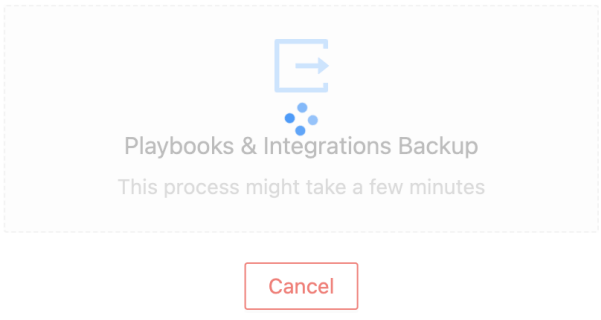
3. Click **Upload**.

Backup

You can backup and restore SOAR, how it is configured, and its data. After backup, you can restore SOAR on the same system or a different one. Backup helps you protect your system from any errors during a software upgrade or due to hardware failure.

After creating the backup file, you can import it to SOAR using Import.

1. Go to `Settings >> SOAR Settings` from the navigation bar and click **Import / Backup**.
2. Click **Playbooks & Integrations Backup** to download the file.



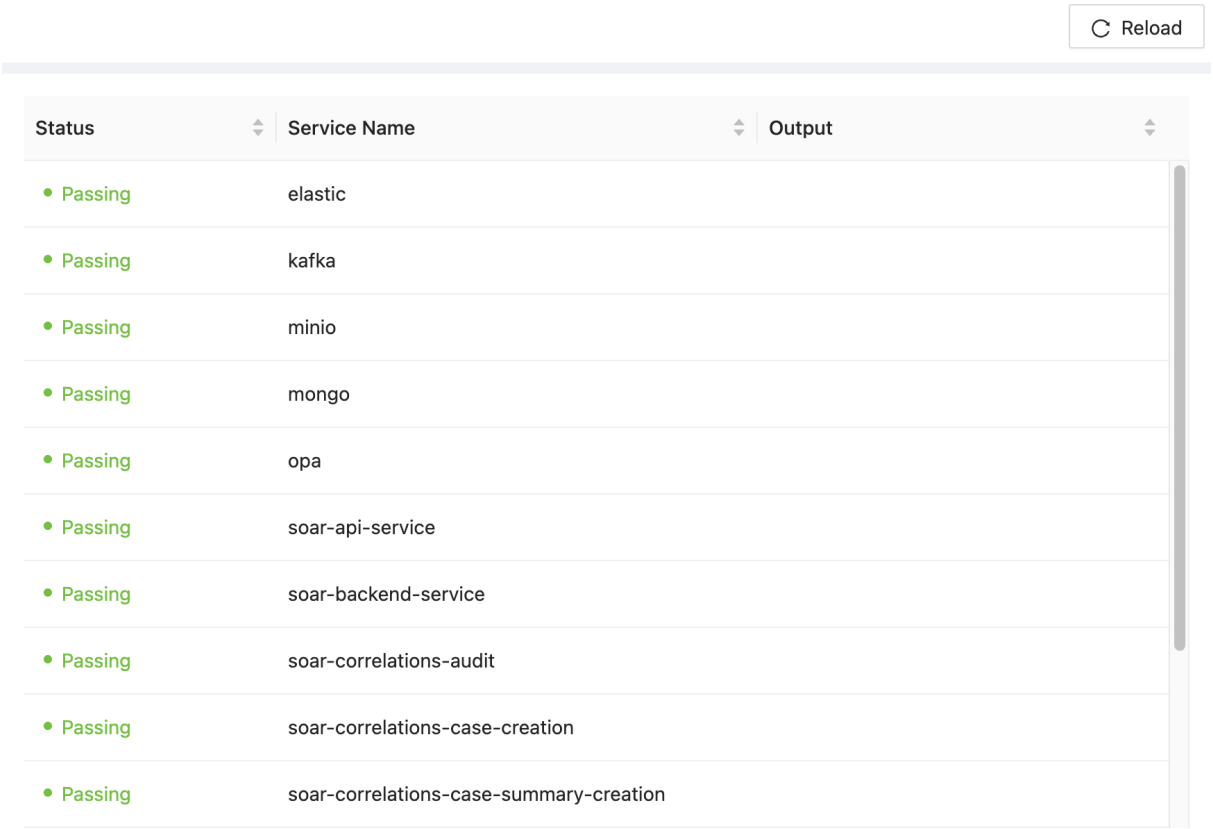
> **NOTE**
> Backup takes a few minutes. Do not navigate away until backup is generated or backup will stop.

3. A .zip file is created. Go to your downloads folder to access it.

System Health

You can monitor the health status of services used by SOAR from System Health. The status are passing or critical. When a service is critical, we recommend you contact SLS Support and share the reason of the status from the **Output** column to debug the problem.

Go to `Settings >> SOAR Settings` from the navigation bar and click **System Health** to view all the services for SLS SOAR. From the **System Health** page, you can refresh the list of services and their information by clicking on the **Reload** icon.



Sources

Sources are where incidents originate.

NOTE
Sources are for SLS use only.

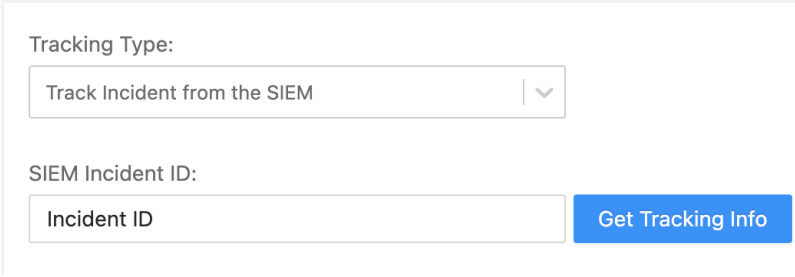
Execution Tracking

You can track all the internal stages of a playbook's execution from Execution Tracking, from activation to completion.

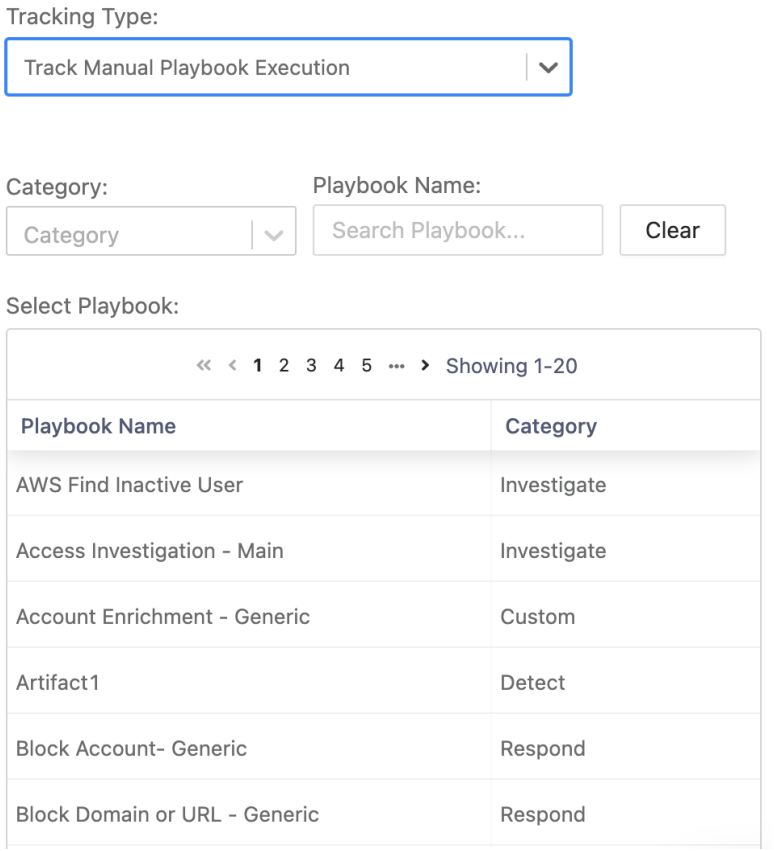
NOTE
Execution Tracking is disabled by default. Contact SLS Support to enable it.

There are two ways to track playbook execution:

1. **Track Incidents from the SIEM**: Track the execution of playbooks SLS-based incidents automatically generate. To do this, enter the incident ID and click **Get Tracking Info**.



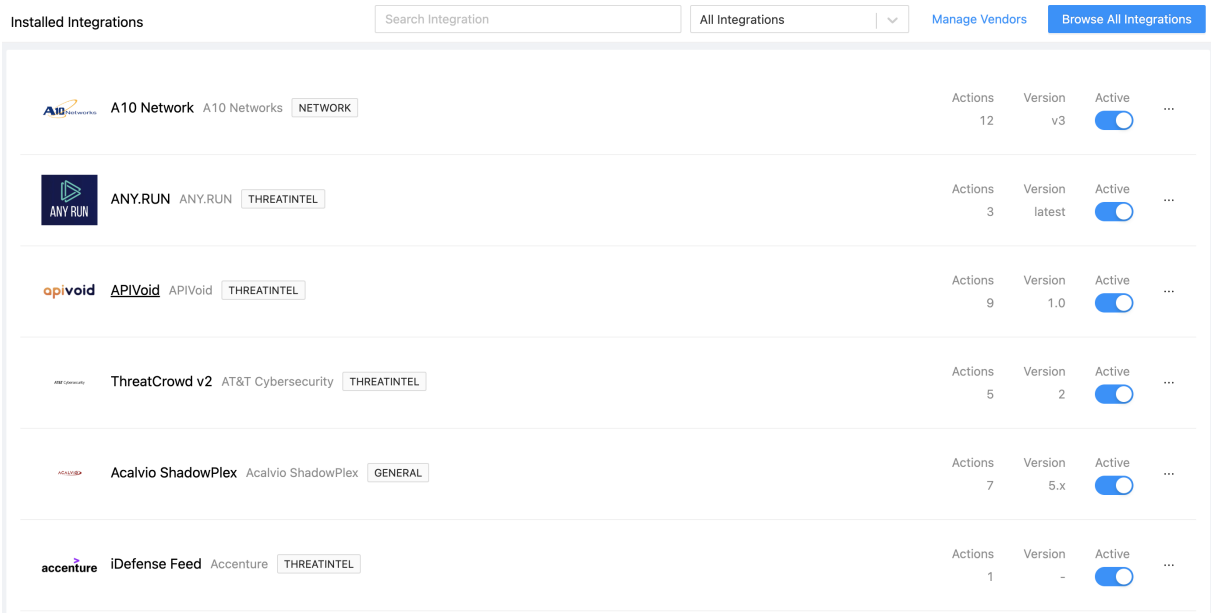
2. **Track Manual Playbook Execution**: Track manually triggered playbooks. To do this, select a playbook from the list.



Playbook Integrations

Playbook Integrations lists all of the product instances created and installed in addition to all of the 3rd party integration sources. You use Playbook Integrations to create the link with a vendor, add their product to your SOAR, and then create a product instance, based on the vendor's product, and add which actions are part of the product instance.

A single vendor can have multiple inter-related products. The grouping of products according to their respective vendors helps identify the parent organization and also helps perform bulk operations.



Vendors & Installed Integrations Overview {#Vendors & Installed Integrations Overview}

To view all vendors configured for SLS SOAR:

1. Go to `Settings >> SOAR Settings` from the navigation bar and click **Playbook Integrations**
2. Use the search field at the top to find a specific vendor. You can also sort the list.

The list includes the number of actions the product instance has.

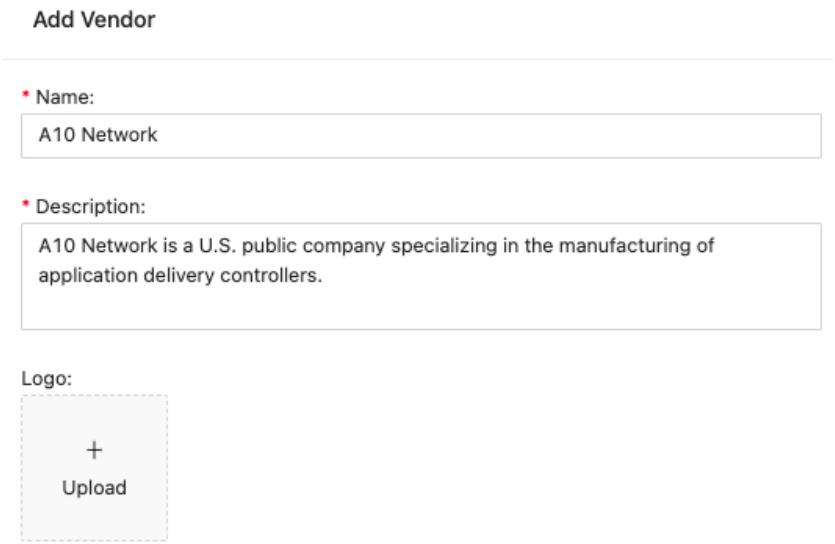
From the list you can:

- Click on the vendor name to view configuration details.
- Click the ellipsis (...) to modify the configuration.
- Deactivate it if you don't want to use it and don't want to delete it yet.

Add New Integration

You can add a new vendor if it isn't already setup.

1. In the **Installed Integrations** list, click **Manage Vendors** at the top.
2. In **Vendors**, click **Create New Vendor**.



> **NOTE**
> You can check whether the vendor already exists. Use the search field to find it.

3. Enter the details and upload a logo and click **Save**.

Add New Product

When a vendor integration is added to SOAR, you can then add which products you want to use and base your product instances on.

1. In the **Installed Integrations** list, click **Browse all Integrations**.
2. Click **Create New Integration**.
3. In **Edit Integration Template** enter general product details.
4. **Parameters** are global product parameters or those parameters that your product instances will start with. Click **Add Row** to add the first one. Repeat for each, additional parameter you want to add.
5. Click **Save** when you are done.

Add New Product Instance

You can add as many product instances, based on a vendor product, as you need. This allows you to make modifications to individual product instances, and use different ones in different playbooks, based on what you want a playbook to do. When you add a new product instance it is termed Integration Template and becomes part of the **Integration Template** list. When you add new product instances, you use the original Integration template, apply new parameters to it and then use it as another product instance.

1. In the **Playbook Integrations** list, click **Browse All Integrations**.
2. You can scroll through the list, use **Search**, or filter the list to find the right one.
3. Click the ellipsis (....) and then **Configure New Instance**.
4. Add the parameters and click **Save**.

Modify Existing Product Instances

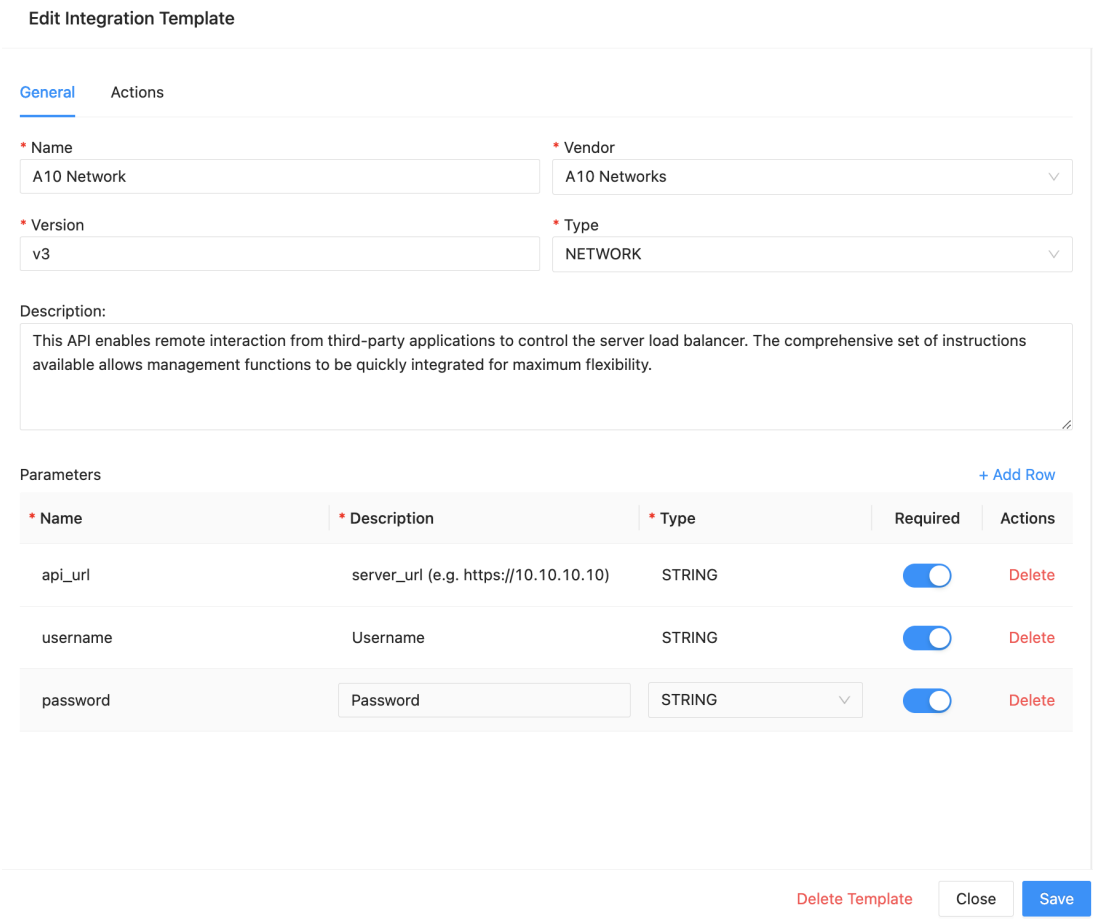
You can modify the parameters of existing product instances if you need to.

1. In **Playbook Integrations**, find the product instance in the list.
2. In the column to the right of **Active**, click the ellipsis (...).
3. Click **Configure Instance**.
4. Make the changes you need.
5. Click **Save**.

Configure or Modify Product Instance Parameters

> **NOTE**
> The process for adding or modifying parameters is the same for both new and existing integrations.

1. In the **Installed Integrations** list, click **Browse all Integrations**.
2. You can scroll through the list, use **Search**, or filter the list to find the right one.
3. Click **Edit Integration Template**.
4. In addition to the general parameters, you can also configure the **Actions** including adding new ones.
   - Modify existing actions directly from the **Parameters** list.



5. To add new actions, click **Actions** at the top of **Edit Integration Template**.
6. Use **General** to enter
   - The **Name** of the product instance.
   - The **Vendor** or Integration the product instance is based on.
   - The **Version** of the product instance. This is particularly important when you know you will be setting up multiple product instances.
   - Select the action **Type** and **Activation Type** from the drop-downs.
7. To add parameters, click **Add Row**.
8. Click **Add** to add **Request Params**.
9. Enter the parameter's **Name** and **Description**.
10. Select the action **Type**.
11. Click **Required** if relevant.
12. Enter the **Default Value**.
13. Click **Save**.
14. Click **Config**.
15. Enter the exact **URL** of the action.
16. Select the request **Method** from the drop-down.
17. Enter the **Request** data.
18. Select the **Request Content Type** from the drop-down.
19. Select the **Response Content Type** from the drop-down.
20. Click **Add** to add **Headers**
21. Enter the header's **Name** and **Value**.
22. If you want to test whether the action works, click **Test Action**.
23. Click **Save** when you are done.

Export Existing Vendor Product Instance

You can export a product instance and use it in another SOAR if you want.

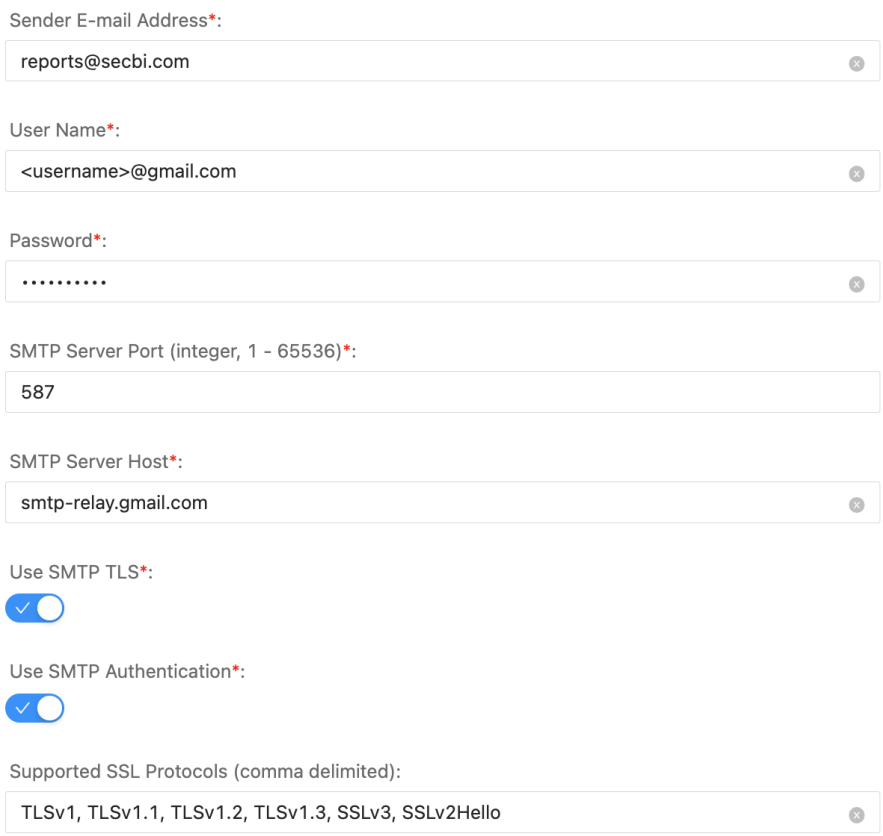
1. In **Playbook Integrations**, find the product instance in the list.
2. In the column to the right of **Active**, click the ellipsis (...).
3. The product instance is generated as a .zip file. Go to your downloads folder to find it.

E-Mail Configurations

SOAR sends email alerts when an incident is trigerred in SLS. The **E-Mail Configurations** lets you modify the SMTP server settings like **Sender E-mail Address**, **User Name** and **Password**. The recipient addresses are added from **Playbooks**.

To set up **E-mail Configurations**:

1. Go to `Settings >> SOAR Settings` from the navigation bar and click **E-Mail Configurations**.



2. In **Sender E-mail Address**, enter the email address through which the alerts are sent.
3. Enter the **User Name** of the sender.
4. Enter a **Password**.
5. Enter the **SMTP Server Port** you want to use for communication. It should be an integer value between 1 and 65536. Use either port 587 or 2525 if you are not sure which port to set here.
6. In **SMTP Server Host**, enter the email host you are using. E.g. Gmail, MailChimp, AOL.
7. Select **Use SMTP TLS** if you want the message sent to be encrypted.
8. Select **Use SMTP Authentication** if you need to show your server host that you have permission to send email through the mail server.
9. Click **Save**.

> **NOTE**
> The configurations are auto-saved.

Retention

You can setup how long SOAR data is saved and manage how often often data is cleaned up. You can only setup or change the number of **days** data is stored. You can't control data retention according to weeks or hours, for example.

Default Settings

Go to `Settings >> SOAR Settings` from the navigation bar and click **Retention**.

- **PLAYBOOKS_HISTORY** is for internal SLS use only.
- **CASES_RETENTION** is how long SOAR cases are saved.
- **PLAYBOOKS_EXECUTION_RETENTION** is how long to save playbook monitoring data.
- **SOAR_STATS_RETENTION** is how long to save data statistics about SOAR playbooks.
- **EXECUTION_TRACKING_RETENTION** is how long to save data about Execution Tracking.
- **SLS_WIDGETS_REPORTING** is how long to save data forwarded from SOAR to SIEM used in the SOC Operation Dashboard.

In the list, to the right of each retention type is an ellipsis (...) click it to edit how long data should be stored.

Further reading

Additional information and answers to questions you may have about SLS are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu