



STORMSHIELD



GUIDE

STORMSHIELD LOG SUPERVISOR

GETTING STARTED WITH SOAR GUIDE

Version 2

Document last updated: April 17, 2025

Reference: `sls-en_soar_getting_started_gde`



Table of contents

Change log	3
Getting started	4
SOAR Work Flow	4
Deployment	5
Licensing	5
Enabling SOAR in SLS	5
Adding a SOAR License	6
Install & Upgrade	7
System Requirements	7
Components of SOAR	7
Playbooks	7
Cases	7
SOAR Settings	8
Further reading	8



Change log

Date	Description
April 17, 2025	Section "Licensing" modified
March 3, 2025	New document



Getting started

Welcome to the SLS version 2 Getting Started with SOAR Guide.

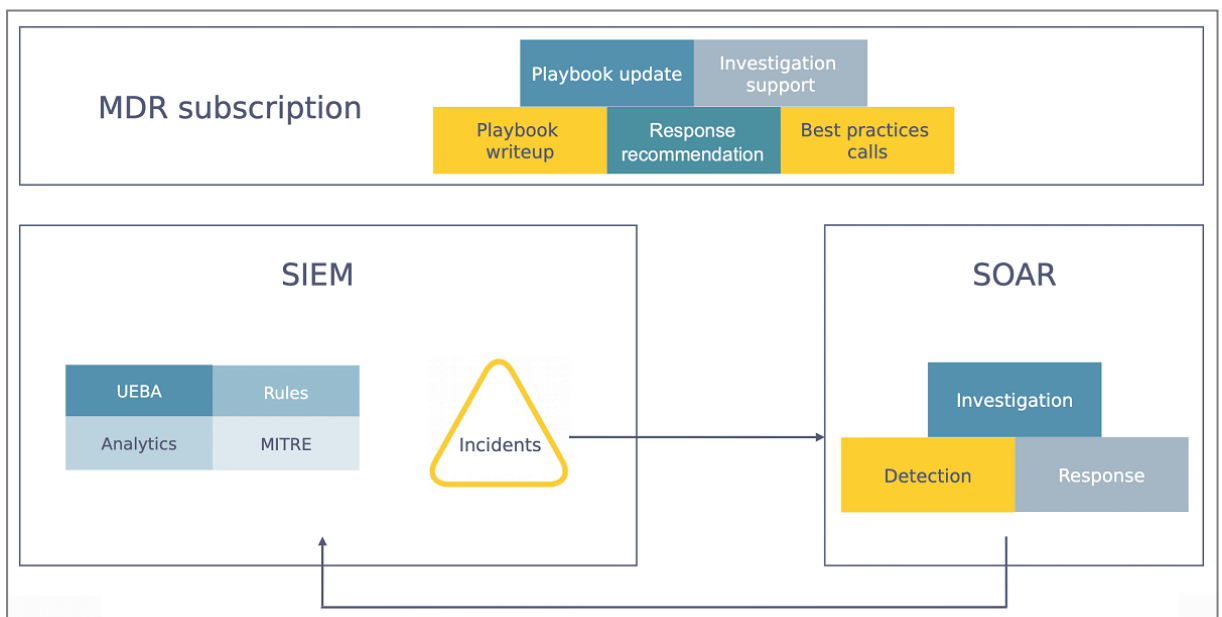
SLS SOAR (Security Orchestration, Automation, and Response) is seamless integration with SLS SIEM to improve the efficiency of threat detection and response. It minimizes the response time and manual intervention over threat alerts by implementing a standard workflow consisting of automated activities for incident response. The key functionality provided by SLS SOAR are:

- Collection of security threat data and alerts from multiple sources.
- Prioritization and execution of incident response according to a standard workflow.
- Automation of incident response to rapidly investigate, contain, and remove cyber threats.

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.

SOAR Work Flow

SLS SOAR receives incidents generated by SLS SIEM in response to alerts from multiple sources. You can trigger *Playbooks* based on the incidents and create *Cases* for further investigation using automation through *Playbooks*. You can manually investigate an incident by following the case details and timeline. The playbook automatically executes the actions required to detect, investigate, and respond to the incidents. To facilitate the process of detection, investigation, and response, SLS SOAR also fetches normalized and raw logs from SLS SIEM.





Deployment

SLS SOAR has been seamlessly integrated with SLS SIEM to minimize your additional effort for deployment and configuration. You can access SLS SIEM and SLS SOAR from a common authentication and interface. Similarly, user permission and authorization are common for SLS SIEM and SLS SOAR.

Licensing

After a fresh installation, you can add a one seat SOAR license to your SLS. However, you must first enable SOAR in SLS. Then you'll be able to add an SLS SOAR license.

Enabling SOAR in SLS

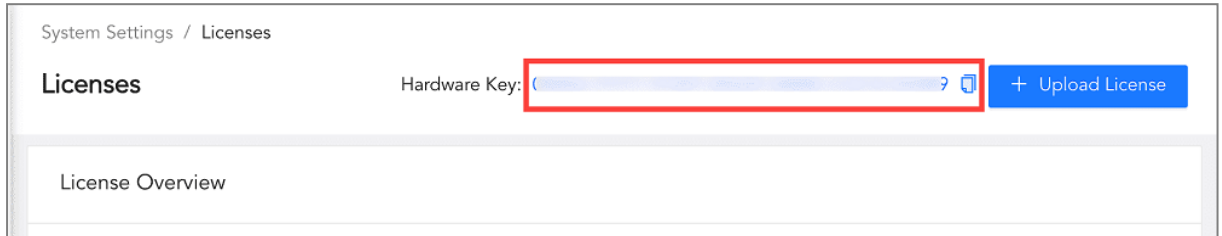
1. Go to Settings >> System Settings from the navigation bar and click System Settings.
2. Select **General**.
3. Select **Enable SOAR in SLS** to enable incident investigation with Playbooks and Cases.
4. Click **Save**.

The screenshot shows the 'SYSTEM SETTINGS' window with the 'General' tab selected. The left sidebar lists various settings categories: General, SMTP, NTP, SNMP, HTTPS, Syslog, Support Connection, Modes of Operation, SSH Key Pair for li-admin, Lockout Policy, Enrichment, and Data Privacy Module. The main content area for 'General' includes a note about time ranges, radio buttons for 'Collection Timestamp (col_ts)' and 'Log Timestamp (log_ts)' (the latter is selected), a dropdown for 'Over Scan Period (in minutes)' set to 10, and a dropdown for 'Time Zone' set to '(GMT+01:00) Brussels, Copenhagen, Madrid, Paris'. Below these, there is a section for 'SOAR' with a checkbox labeled 'Enable SOAR in SLS' which is highlighted with a red rectangle. Further down is a 'USAGE DATA' section with a checkbox 'Share Usage Data' and a paragraph explaining that anonymous usage data is collected to improve the product, while PII is not. At the bottom, there are 'Save' and 'Cancel' buttons. A footer note states: 'Each section needs to be saved separately. Please save your changes before moving to next tab.'



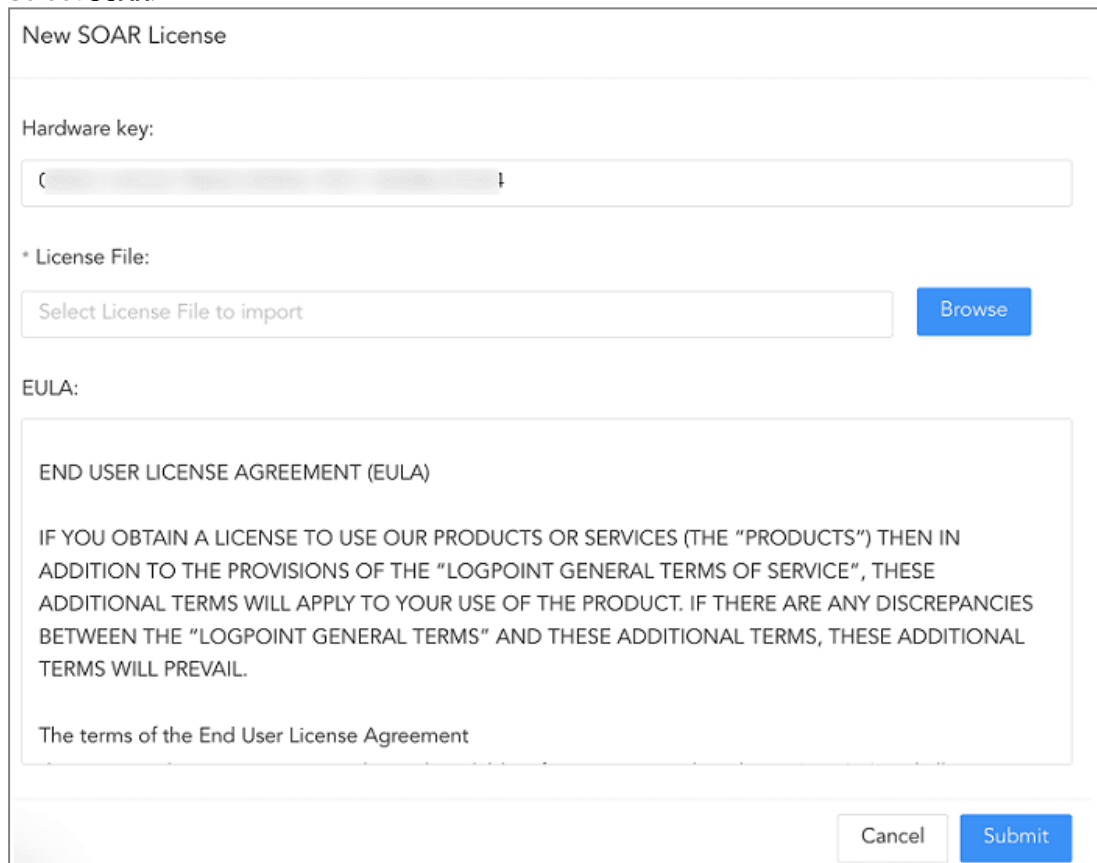
Adding a SOAR License

Before adding a license, contact Stormshield and provide your **Hardware Key**. Stormshield will give you your specific SOAR license. You can find the **Hardware Key** at Settings >> System Settings >> Licenses.



To add a license:

1. Go to Settings >> System Settings >> Licenses from the navigation bar.
2. Click **Upload License**.
3. Select **SOAR**.



4. **Browse** to your **License**.
5. Accept the terms of the End User License Agreement.
6. Click **Submit**.



Install & Upgrade

When a new SLS SIEM is released, SOAR is automatically upgraded. You don't need to install those new versions of SOAR.

! IMPORTANT
SOAR requires vCPU to have AVX support.

System Requirements

For SOAR systems running a few hundred playbooks per day:

Available Memory	10 GB
Additional Disk Space	25 GB
CPUs	2

For SOAR systems running around 1000 playbooks per day:

Available Memory	16 GB
Additional Disk Space	100 GB
CPUs	5

Components of SOAR

You can access the components of SLS SOAR from the navigation bar.

Playbooks

A set of automated actions to follow a standard process that assists you in detecting, investigating, and responding to a security threat alert.

For more details, go to the [Playbook guide](#).

Cases

Cases enlist the details of the threat alert like **Name**, **Status**, **Severity**, **Duration**, **Creation Date**, and **Active**. It also provides an *Investigation Timeline* that provides detailed information over the chain of events associated with a threat alert.



SOAR Settings

You can configure the **Vendors, Products, Actions, API Key, Licensing, My Products, Lists Management, System Health, Execution Tracking, and Import** settings from the **SOAR Settings**.

For more details, go to the [SOAR Settings guide](#).

IMPORTANT

SOAR is disabled by default. You can enable it by selecting the **Enable SOAR in SLS** checkbox from `Settings >> System Settings >> System Settings >> General`.

Further reading

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



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.