



**STORMSHIELD**



GUIDE  
**SLS LOGPOINT**

# QUICK START GUIDE FOR STORMSHIELD SOURCES

Document last updated: September 11, 2025

Reference: [sls-logpoint-en\\_quick\\_start\\_guide\\_stormshield\\_sources](#)



## Table of contents

Change log .....	3
Getting started .....	4
Requirements .....	5
Deploying SLS Logpoint .....	6
Downloading the SLS Logpoint installation file .....	6
Deploying SLS Logpoint in a virtual environment .....	6
Activating SLS Logpoint .....	7
Accessing the SLS Logpoint user interface .....	7
Getting the SLS Logpoint Hardware Key .....	7
Registering the SLS Logpoint product on MyStormshield .....	8
Downloading the SLS Logpoint license on MyStormshield .....	8
Installing the SLS Logpoint license .....	8
Changing the "admin" user password .....	9
Getting logs from an SNS firewall .....	10
Configuring log collection and storage on SLS Logpoint .....	10
Adding a Stormshield Repo .....	10
Adding a Stormshield Normalization Policy .....	10
Adding a Stormshield Routing Policy .....	11
Adding a Stormshield Processing policy .....	12
Adding a Stormshield Log Collection Policy .....	13
Adding a new SNS firewall device to SLS Logpoint .....	13
Configuring log retrieval between the SNS firewall and SLS Logpoint .....	14
Through standard Syslog .....	14
Through Syslog-TLS .....	15
Adding Stormshield Dashboards to SLS Logpoint .....	17
Further reading .....	18



## Change log

Date	Description
September 11, 2025	New document



## Getting started

---

Welcome to the SLS Logpoint Quick Start Guide for Stormshield Sources.

This guide provides details on the steps and considerations for deploying SLS Logpoint.

SLS Logpoint is a SIEM solution (Security Information and Event Management) based on Logpoint SIEM.



# Requirements

---

## Compatibility

For more information about the SLS Logpoint Release Cycle, refer to the [Logpoint Release Cycle](#) webpage.

## System requirements

For more information about the SLS Logpoint system requirements, refer to the [System Requirements for Logpoint](#) webpage.



# Deploying SLS Logpoint

## Downloading the SLS Logpoint installation file

1. In your [MyStormshield](#) personal area, go to **Downloads** > **Downloads**.
2. From the list of categories, select **Stormshield Log Supervisor** > **Firmware**.
3. Download the installation image in the desired format by clicking on its name:
  - *iso*, for standard installation,
  - *ova*, package for VMWare platforms,
  - *vhd*, package for Microsoft Hyper-V platforms.
4. Save the file on your workstation.

## Deploying SLS Logpoint in a virtual environment

For more information about deploying SLS Logpoint, refer to the guide for your virtual environment:

- [ISO deployment](#),
- [OVA deployment](#),
- [VHD deployment](#).



# Activating SLS Logpoint

## Accessing the SLS Logpoint user interface

1. Make sure your virtual machine is powered on.
2. Access the SLS user interface by entering its IP address into a web browser.
3. Log in to the SLS Logpoint user interface. The default credentials are:
  - Username: *admin*
  - Password: *changeme*

### **i** NOTE

If you need to get or set the IP address of your SLS Logpoint instance:

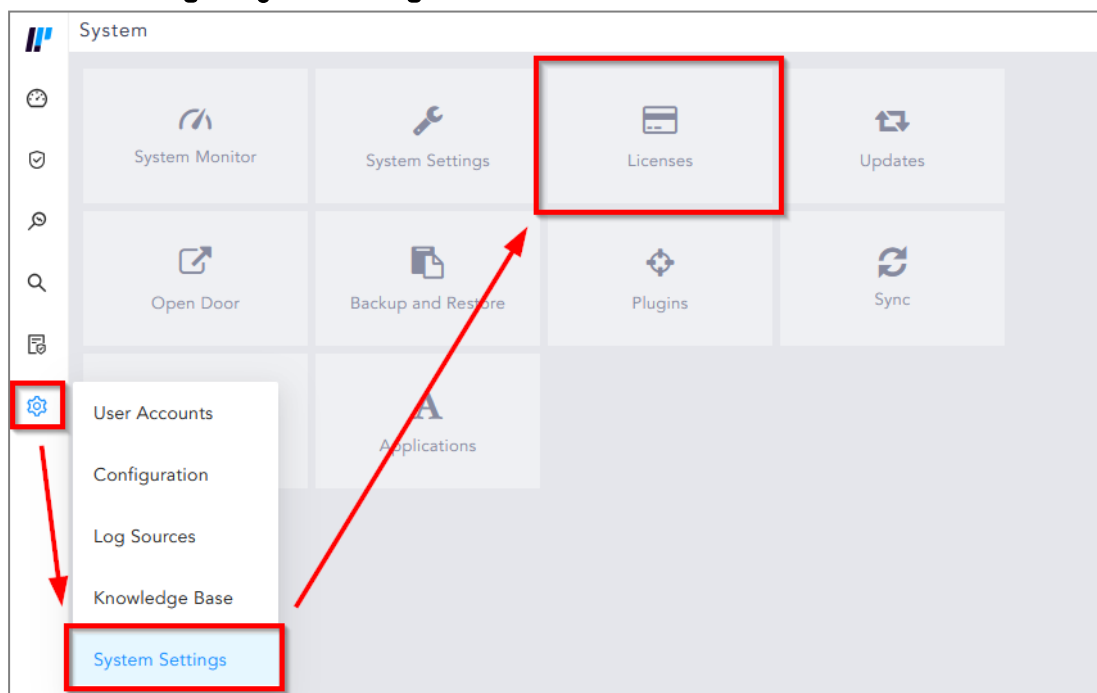
1. Open a VM Console. The default credentials are *li-admin* (username) and *changeme* (password).
2. Retrieve the IP address by using the "ip a" command. Define the IP address by using the "change-ip" command, then the "systemctl reboot" command.

## Getting the SLS Logpoint Hardware Key

Once connected to the SLS Logpoint user interface for the first time, it is requested to activate SLS Logpoint with a license provided by Stormshield, which contains the details of the purchased product, the number of sources it can handle, and the license's expiration date.

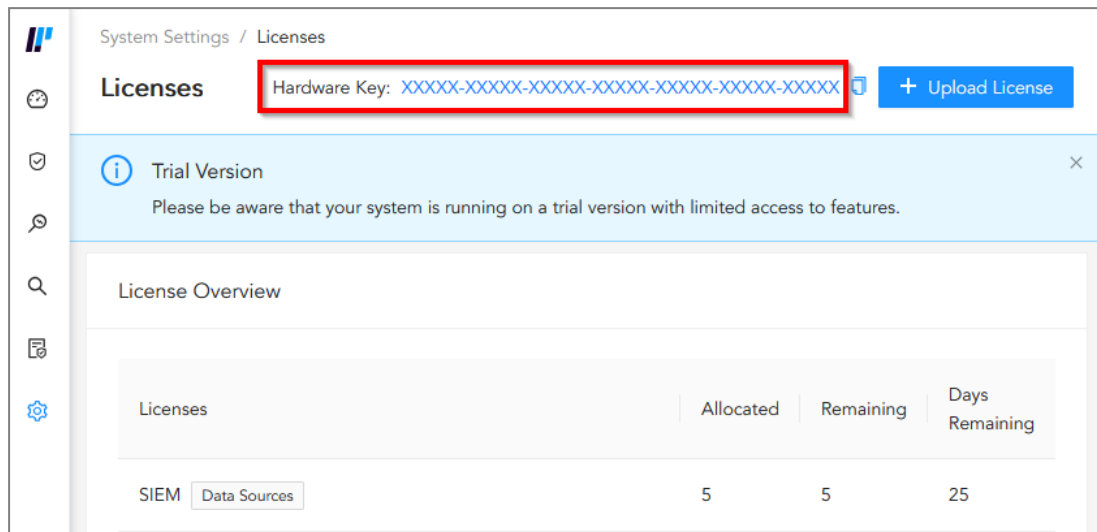
The license refers to the **Hardware Key** of the solution, which is unique. To retrieve your Hardware Key:

1. Go to  **Settings > System Settings > License**.





2. The **Hardware Key** can be found at the top of the window.



## Registering the SLS Logpoint product on MyStormshield

1. Contact your Stormshield reseller or partner to obtain an SLS Logpoint license.
2. Register your SLS Logpoint product in your [MyStormshield](#) personal area. You will be prompted to enter the SLS Logpoint **Hardware Key** and **Serial Number**. For more information, refer to the [Registering products](#) guide.

### **i** NOTE

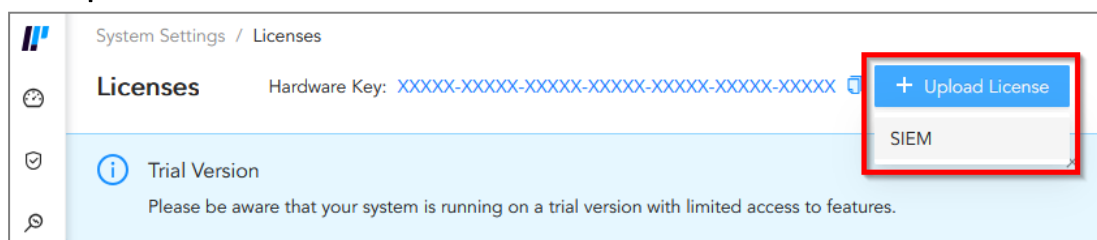
Once you have registered your SLS Logpoint on MyStormshield, it may take a few days for the license file to become available.

## Downloading the SLS Logpoint license on MyStormshield

From your [MyStormshield](#) personal area, download the license (.pak file). For more information, refer to the [Downloading a product's license file](#) webpage.

## Installing the SLS Logpoint license

1. On SLS Logpoint, go to **Settings** > **System Settings** > **License**.
2. Click **Upload License** > **SIEM**.




3. Browse to the .pak file containing the **License Key**.
4. Go through the **END USER LICENSE AGREEMENT (EULA)**.
5. Click **Submit** if you agree with the terms and conditions of the EULA.





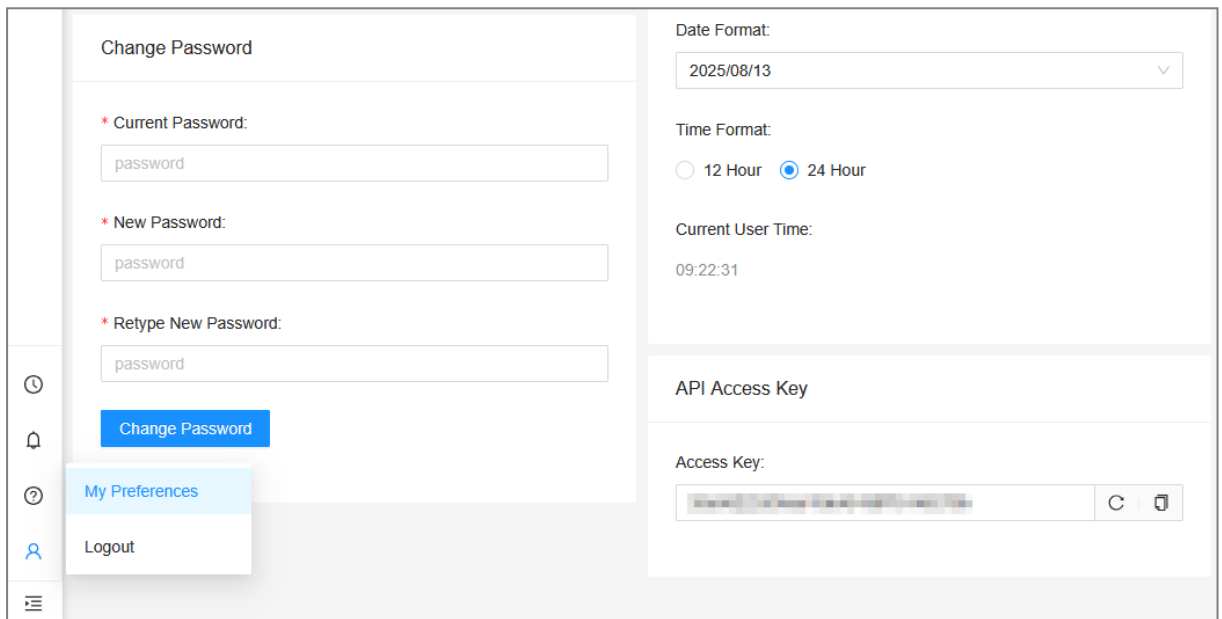
## Changing the "admin" user password

For security reasons, you must change the default password of the "admin" user.

1. Go to  **User > My Preferences**.
2. In the **Account** tab, **Current Password** field, enter *changeme*.
3. Enter the new password and confirm it.
4. Click **Change Password**.

### ! IMPORTANT

The password must be kept in a secure and protected location.





## Getting logs from an SNS firewall

### Configuring log collection and storage on SLS Logpoint

#### **i** NOTE

In the procedures below, the name "stormshield" is used as an example. You can choose different names; if you do so, adapt the procedures accordingly.

### Adding a Stormshield Repo

The **Repos** (repositories) store the streaming logs securely. You must create a new Stormshield repo to store incoming logs from your SNS firewalls.

1. Go to **Settings > Configuration > Repos** and click **Add**.
2. In the **Repo Name** field, enter "stormshield".
3. In the **Retention (day)** field, define a retention period. Retention specifies the number of days for which logs are kept in storage before they are removed.
4. Click **Submit**.

**ADD REPO**

**REPO INFORMATION**

Repo Name: stormshield

Repo Path: /opt/immune/storage/ Retention (day): 5

**AVAILABILITY**

A copy of above repo will be created in the selected remote LogPoints. If somehow the repo is not accessible, its copy will be used in search. This will hence maintain the higher availability of the repo.

Remote LogPoint: None Available for (day): 1

Submit Cancel

### Adding a Stormshield Normalization Policy

A normalization policy combines **Compiled Normalizers** and **Normalization Packages** to translate raw log messages into SLS Logpoint taxonomy. A Stormshield compiled normalizer and a Stormshield Network Security normalization package are available when adding a new normalization policy.

1. Go to **Settings > Configuration > Normalization Policies** and click **Add**.
2. In the **Policy Name** field, enter "stormshield".
3. In the **Compiled Normalizer** section, search for "Stormshield", then move "StormshieldCompiledNormalizer" to the **Selected** box.



4. In the **Normalization Packages** section, search for "Stormshield", then move "**LP\_Stormshield Network Security**" to the **Selected** box.
5. Click **Submit**.

**CREATE NORMALIZATION POLICY**

**NORMALIZATION POLICY INFORMATION**

Policy Name:  
stormshield

Compiled Normalizer:

Available: stormshield

Selected: StormshieldCompiledNormalizer

Normalization Packages:

Available: stormshield

Selected: LP\_Stormshield Network Security

View Signatures Submit Cancel

## Adding a Stormshield Routing Policy

Routing policies allow selectively directing incoming logs to different repos in the system. You must create a new Stormshield routing policy to route incoming logs from your SNS firewalls to your Stormshield repository.

1. Go to **Settings > Configuration > Routing Policies** and click **Add**.
2. In the **Policy Name** field, enter "stormshield".
3. In the **Catch all** field, select the "stormshield" repo previously created.
4. Click **Submit**.



S.N.	Type	Key	Value	Repo	Operation	Actions
------	------	-----	-------	------	-----------	---------

### Adding a Stormshield Processing policy

A processing policy integrates a normalization policy and a routing policy into a single policy. You must create a new Stormshield processing policy that integrates the Stormshield normalization policy and the Stormshield routing policy into a single processing policy.

1. Go to **Settings > Configuration > Processing Policies** and click **Add**.
2. In the **Policy Name** field, enter "stormshield".
3. In the **Normalization Policy** field, select the "stormshield" normalization policy previously created.
4. In the **Enrichment Policy** field, select "None".
5. In the **Routing Policy** field, select the "stormshield" routing policy previously created.
6. Click **Submit**.

S.N.	Type	Key	Value	Repo	Operation	Actions
------	------	-----	-------	------	-----------	---------



## Adding a Stormshield Log Collection Policy

Log Collection Policies are the rules that SLS Logpoint uses to collect the logs. You must create a new Stormshield log collection policy and configure it with a Syslog collector to be able to fetch incoming logs from your SNS firewalls.

1. Go to **Settings > Configuration > Log Collection Policies** and click **Add**.
2. In the **Name** field, enter "stormshield".

CREATE LOG COLLECTION POLICY

LOG POLICY INFORMATION

Name: stormshield

Description:

Save Cancel

3. Click **Save**.  
A window prompts you to configure collectors/fetchers for this policy.
4. Click **Yes** to configure a collector/fetcher for this policy.
5. In the **Available Collectors Fetchers** window, click **Syslog Collector**.
6. In the **Syslog Collector** window:
  - a. In the **Parser** field, leave the default setting as "SyslogParser".
  - b. In the **Processing Policy** field, select the "stormshield" policy previously created.
  - c. In the **Charset** field, leave the default setting as "utf\_8".
7. Click **Submit**.

SYSLOG COLLECTOR

SYSLOG COLLECTOR

Parser: SyslogParser

Processing Policy: stormshield

Charset: utf\_8

Delete Submit Cancel

## Adding a new SNS firewall device to SLS Logpoint

You must add the SNS firewalls you want to fetch logs from by adding them as devices on SLS Logpoint.

1. Go to **Settings > Configuration > Devices** and click **Add**. You can add multiple devices by using the "Bulk" or "Import" features.
2. Enter the **Name** of the device.



3. In the **IP address(es)** field, enter the IP address of the SNS firewall.
4. In the **Log Collection Policy** field, select the "stormshield" log collection policy previously created.
5. Choose the correct **Time Zone**.
6. Click **Submit**.

**CREATE DEVICE**

**DEVICE INFORMATION**

Name: Alpha

Device Address(es):

Device Groups:

Log Collection Policy: stormshield

Distributed Collector:

Time Zone: (GMT+01:00) Brussels, Copenhagen, Madrid, Paris

**RISK VALUES**

Confidentiality: Minimal

Integrity: Minimal

Availability: Minimal

Submit Cancel

## Configuring log retrieval between the SNS firewall and SLS Logpoint

You can choose to get logs from the SNS firewall either through [standard Syslog](#) or, more securely, through [Syslog-TLS](#).

### Through standard Syslog

1. On the SNS firewall web administration interface, go to **Configuration > Notifications > Logs – Syslog – IPFIX > Syslog**.
2. Select the object representing the IP address of the SLS Logpoint instance or create a new object if it does not exist yet.
3. Select the appropriate protocol (TCP or UDP). SLS Logpoint supports both the TCP and UDP protocols for the Syslog collector, as mentioned on the [Connections required by Logpoint](#) webpage. Depending on your needs, you may wish to choose one or the other.
4. Select the port number. The default SLS Logpoint listening port is 514.
5. Select the format.



## 6. Apply the configuration.

The screenshot shows the 'NOTIFICATIONS / LOGS - SYSLOG - IPFIX' configuration page. The 'SYSLOG' tab is active. On the left, under 'SYSLOG PROFILES', there is a table with columns 'Status' and 'Name'. The 'SLS' profile is highlighted with a green background and has a status of 'Enabled'. Below it are three disabled profiles: 'Syslog Profile 1', 'Syslog Profile 2', and 'Syslog Profile 3'. On the right, the 'Details' section for the 'SLS' profile is shown. It includes fields for 'Name' (SLS), 'Comments' (SLS), 'Syslog server' (SLS\_Server), 'Protocol' (UDP), 'Port' (syslog), 'Certification authority' (Syslog-CA), 'Server certificate' (sls.syslog), 'Client certificate' (empty), and 'Format' (RFC5424).

Continue to [Adding Stormshield Dashboards to SLS Logpoint](#).

## Through Syslog-TLS

### Downloading the SNS Certificate Identity as a P12 file

1. On the SNS firewall web administration interface, go to **Configuration > Objects > Certificates and PKI**.
2. Add a **Server identity** with **RSA** as **Key type**.
3. Download the **Identity** as a **P12 file**.

The screenshot shows the 'OBJECTS / CERTIFICATES AND PKI' section of the Stormshield web administration interface. The 'DETAILS' tab is active for the 'sls.syslog' identity. A red box highlights the 'Download' button and the 'as P12 file' option in the dropdown menu. The 'Validity' section shows 'Issued: Feb 16 12:43:29 2021 GMT' and 'Expires: Feb 14 12:43:29 2031 GMT'. The 'Issued for' section shows 'Issuer: C=AW,ST=test state,L=test city,O=Te'.

### Extracting the private key and certificates from the P12 file

1. Open a terminal emulator on your workstation.
2. Use the following commands. Customize the name of the .p12, .key, and .crt files as needed.
  - a. Extract the private key from the P12 file and output it in an unencrypted format:

```
openssl pkcs12 -in sls.syslog.p12 -out sls.syslog.key -nocerts -nodes
```
  - b. Extract the intermediate and root certificates from the P12 file and output them in a .crt file:

```
openssl pkcs12 -in sls.syslog.p12 -out sls.syslog.crt -nokeys -clcerts
```



### Importing the .crt and .key files into SLS Logpoint

1. Go to **Settings** > **System Settings** > **System Settings**.
2. On the **Syslog** tab, click **Browse...** to import the **Certificate** (.crt file) and the **Key** (.key file).
3. Click **Save**.

### Configuring a Syslog-TLS connection on the SNS firewall

1. On the SNS firewall web administration interface, go to **Configuration** > **Notifications** > **Logs** – **Syslog** – **IPFIX** > **Syslog**.
2. Select the object representing the IP address of the SLS Logpoint instance or create a new object if it does not exist yet.
3. Choose *TLS* Protocol.
4. Fill in the certificate information that you previously downloaded as a P12 file.
5. Select *legacy\_long* format.





6. Apply the configuration.

The screenshot shows the 'NOTIFICATIONS / LOGS - SYSLOG - IPFIX' configuration page. The 'SYSLOG' tab is active. On the left, under 'SYSLOG PROFILES', there is a table with columns 'Status' and 'Name'. The 'SLS' profile is highlighted with a green background and has a status of 'Enabled'. Below it are three 'Syslog Profile' entries, all with a status of 'Disabled'. On the right, the 'Details' section for the 'SLS' profile is shown. It includes fields for 'Name' (SLS), 'Comments' (SLS), 'Syslog server' (SLS\_Server), 'Protocol' (TLS), 'Port' (syslog-tls), 'Certification authority' (Syslog-CA), 'Server certificate' (sls.syslog), 'Client certificate' (empty), and 'Format' (legacy\_long).

## Adding Stormshield Dashboards to SLS Logpoint

Your SLS Logpoint starts to receive incoming logs from your SNS firewalls. You must add Stormshield dashboards to visualize this data. Stormshield dashboards are available when adding a new dashboard.

1. Go to **Dashboards > All Dashboards**.
2. Click the icon.
3. Go to the **Vendor Dashboards** tab.
4. In the list, select all "SNS" dashboards.
5. Click **OK**.
6. In the **Ask Repos** window, select all dashboards, then click **Choose Repos**.
7. In the **Repo Selector** window, select the "stormshield" repo previously created.
8. Click **Done**.

The screenshot shows the 'REPO SELECTOR' window. At the top, there is a 'Group by - LogPoint' dropdown and two checkboxes: 'All repos from all LogPoints' and 'Select all current'. Below this is a search bar. The main area shows a list of repositories under the 'LogPoint' group. The 'stormshield' repository is selected, indicated by a checkmark. At the bottom, there are buttons for 'Reload', 'Fetch Remote', 'Done', and 'Cancel'.

9. Click **OK** to add the SNS dashboards.



## Further reading

---

For more information on:

- How to install and configure SLS Logpoint, refer to the [Install and Upgrade Logpoint documentation](#).
- How to configure SLS Logpoint, refer to the [Logpoint System Settings documentation](#).
- How to collect and store logs with SLS Logpoint, refer to the [Logpoint Data Integration documentation](#).

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



**STORMSHIELD**

[documentation@stormshield.eu](mailto: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.*