GUIDE
SLS GUARDSIX

QUICK START GUIDE FOR STORMSHIELD SOURCES

Document last updated: April 1, 2026
Reference: sls-guardsix-en_quick_start_guide_stormshield_sources

Table of contents

Change log

Date	Description
April 1, 2026	Logpoint has been renamed guardsix
September 11, 2025	New document

Getting started

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

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

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

If you are upgrading from SLS version 2 to SLS guardsix, please refer to the "**Migrating from SLS v2 to SLS guardsix guide**", which you can download from your MyStormshield area.

NOTE
The images used in this document are from a version when the guardsix SIEM solution was still called Logpoint. Some elements may differ in the latest SLS guardsix version.

Requirements

Compatibility

For more information about the SLS guardsix version compatibility and patch dependencies, refer to the **Version Compatibility Matrix** and **Patches Dependencies** sections of the guardsix SIEM documentation.

Hardware requirements

For more information about SLS guardsix hardware requirements, refer to the **Pre-deployment** section of the guardsix SIEM documentation.

Deploying SLS guardsix

Downloading the SLS guardsix 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 guardsix in a virtual environment

For more information about deploying SLS guardsix, refer to the Deploy and Install section of the guardsix SIEM documentation.

Activating SLS guardsix

Accessing the SLS guardsix 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 guardsix user interface. The default credentials are:
   - Username: *admin*
   - Password: *changeme*

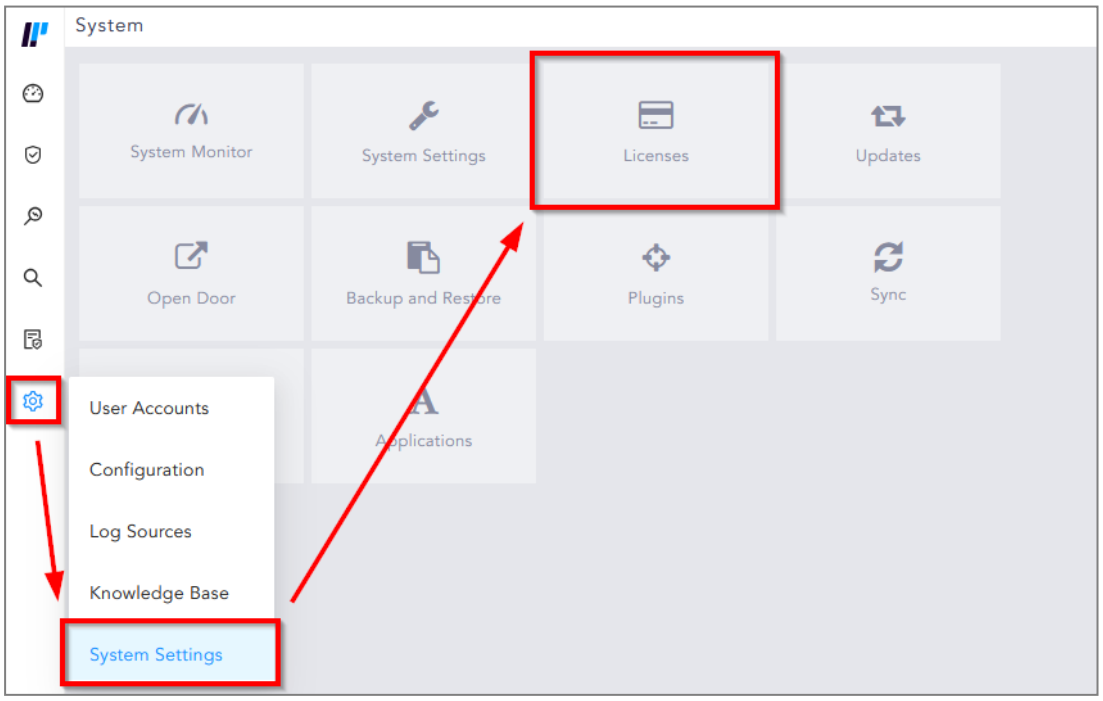
> **NOTE**
> If you need to get or set the IP address of your SLS guardsix instance:
>
> 1. Open a VM Console. The default credentials are *li-admin* (username) and *changeme* (password).
> 2. Retrieve the IP address by using the "`ip a`" command. Define the IP address by using the "`change-ip`" command, then the "`systemctl reboot`" command.

Getting the SLS guardsix Hardware Key

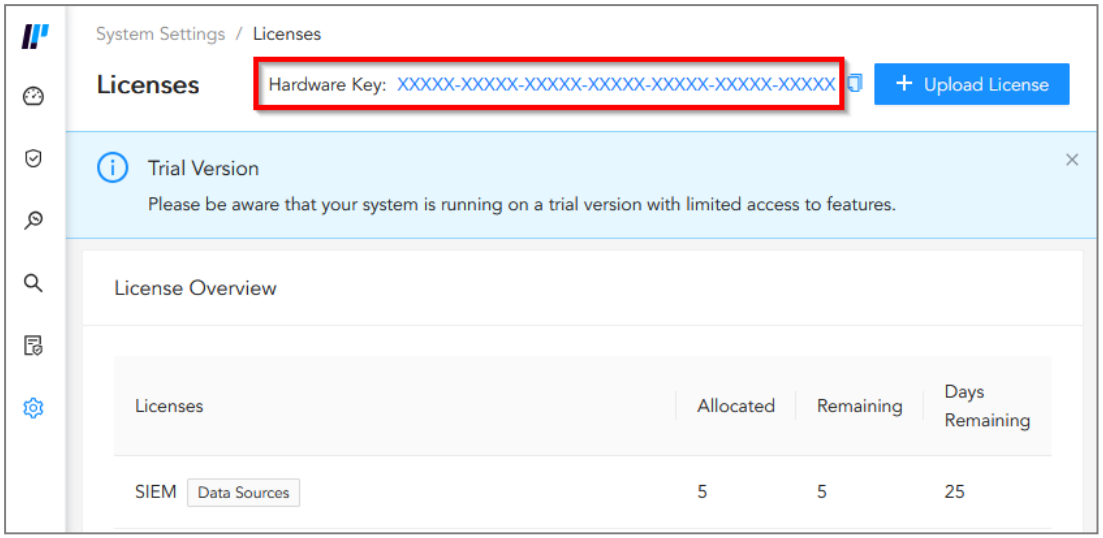
Once connected to the SLS guardsix user interface for the first time, it is requested to activate SLS guardsix with a license provided by Stormshield, which contains the details of the purchased product, the number of sources it can handle, and the license's expiration date.

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 guardsix product on MyStormshield

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

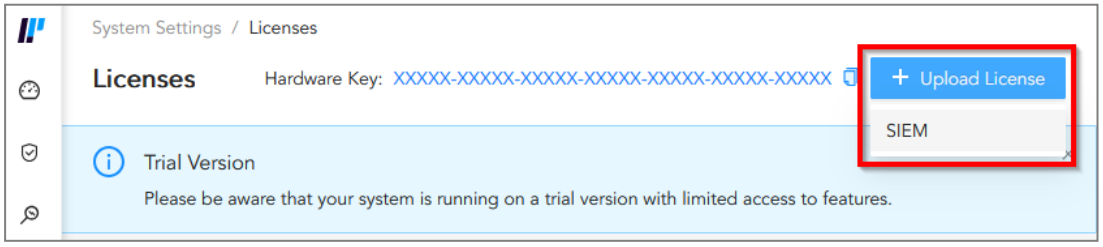
> **NOTE**
> Once you have registered your SLS guardsix on MyStormshield, it may take a few days for the license file to become available.

Downloading the SLS guardsix 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 guardsix license

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



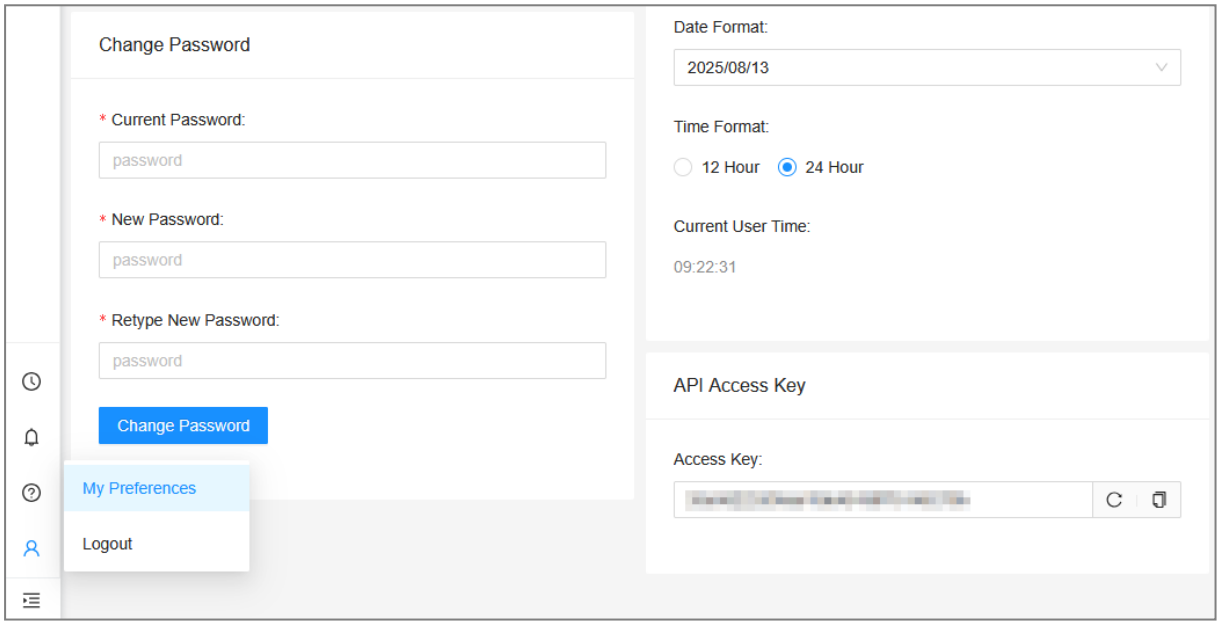
3. Browse to the .pak file containing the **License Key**.
4. Go through the **END USER LICENSE AGREEMENT** (EULA).
5. Click **Submit** if you agree with the terms and conditions of the EULA.

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

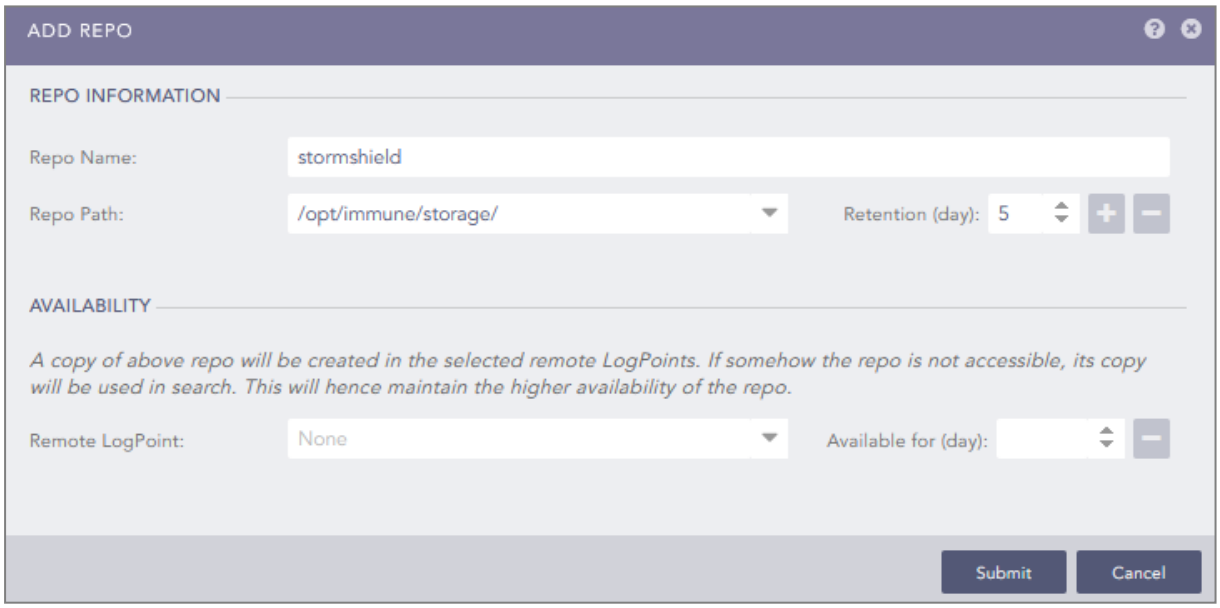
Configuring log collection and storage on SLS guardsix

> **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**.

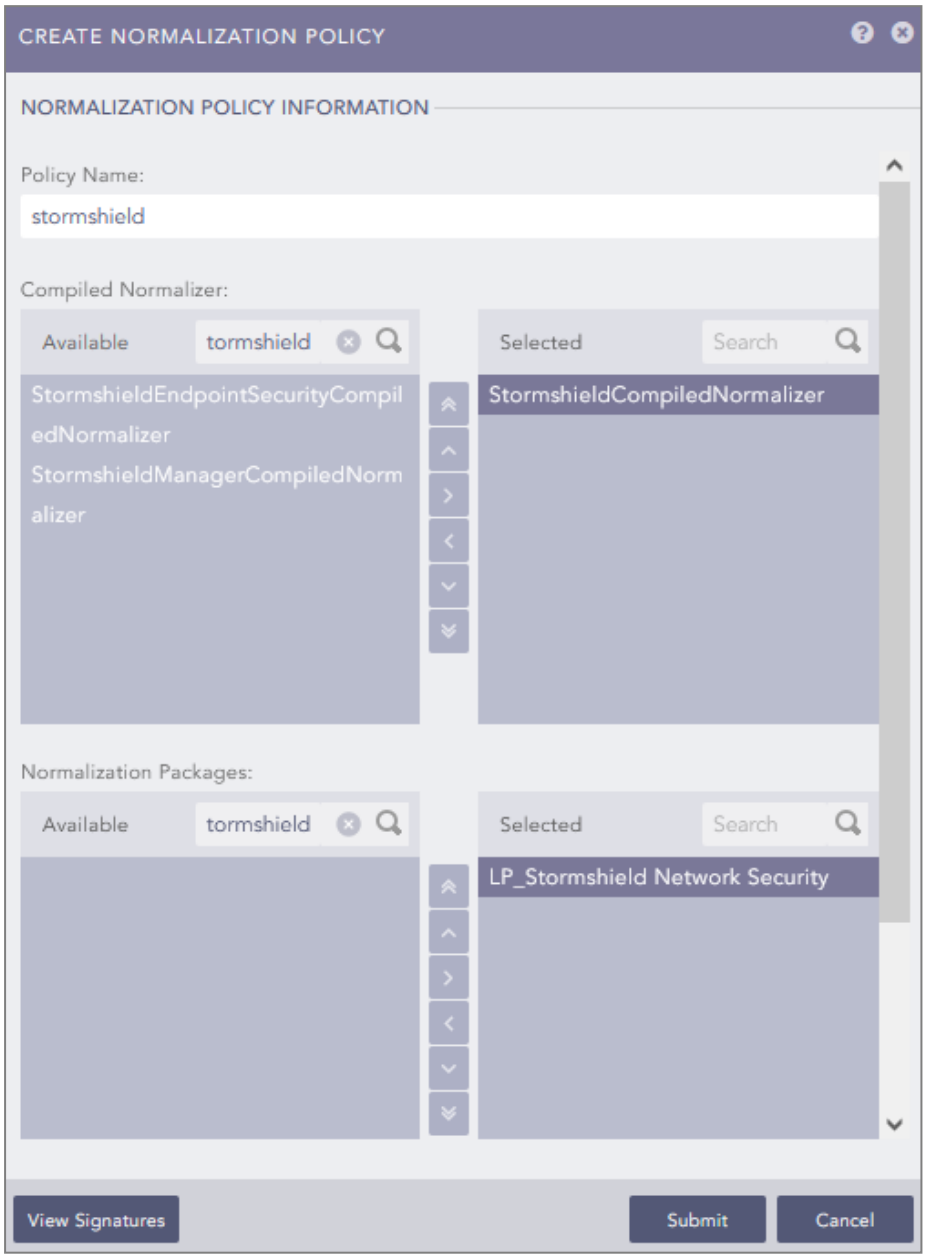


Adding a Stormshield Normalization Policy

A normalization policy combines **Compiled Normalizers** and **Normalization Packages** to translate raw log messages into SLS guardsix 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.

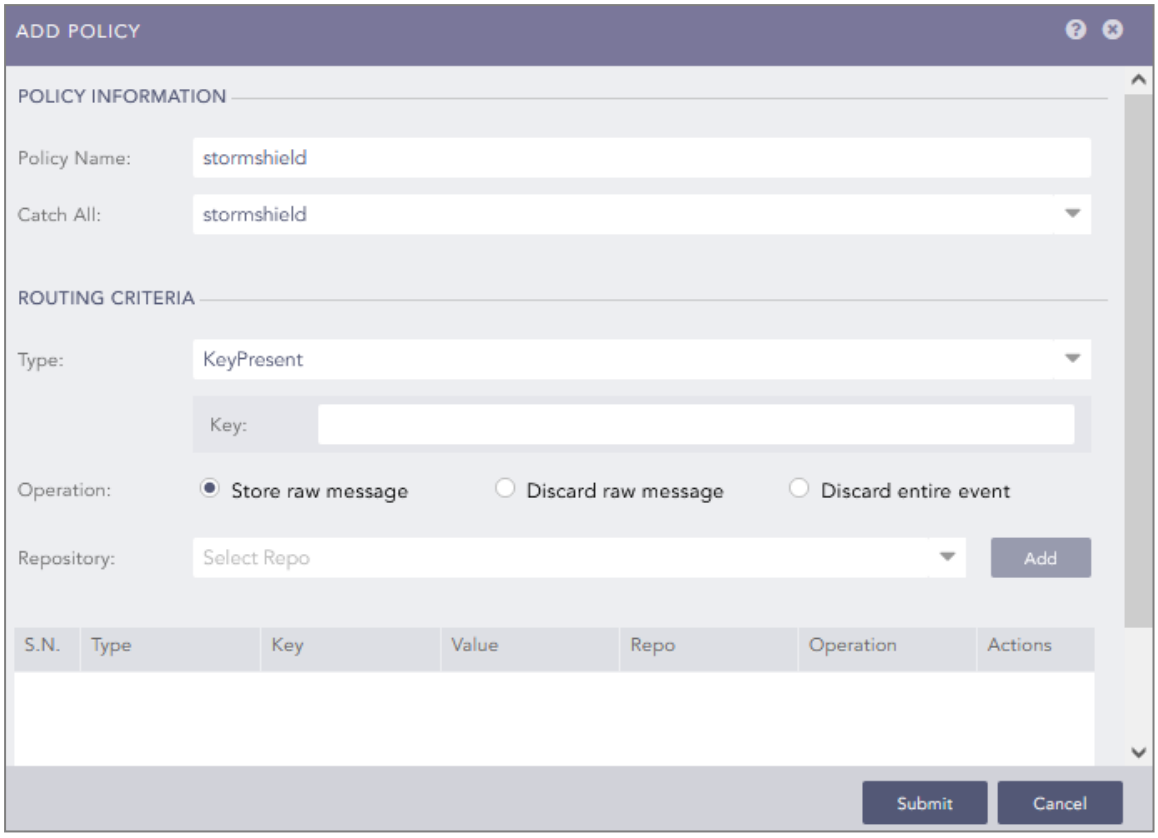
4. In the **Normalization Packages** section, search for "Stormshield", then move "**LP_ Stormshield Network Security**" to the **Selected** box.
5. Click **Submit**.



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.

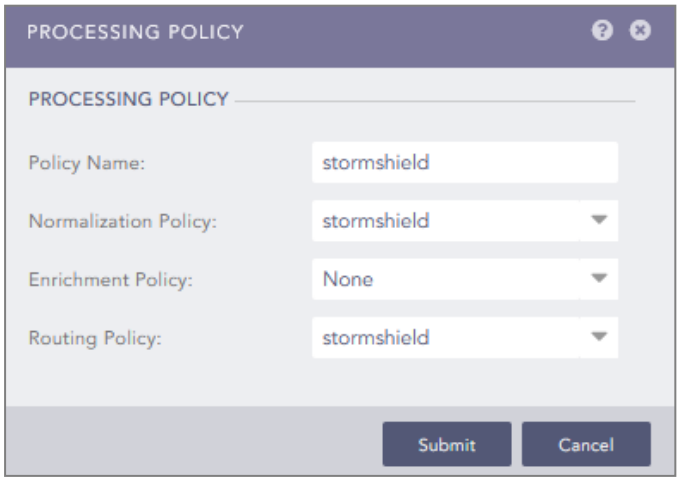
1. Go to ⚙ **Settings** > **Configuration** > **Routing Policies** and click **Add**.
2. In the **Policy Name** field, enter "*stormshield*".
3. In the **Catch all** field, select the "*stormshield*" repo previously created.
4. Click **Submit**.



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.

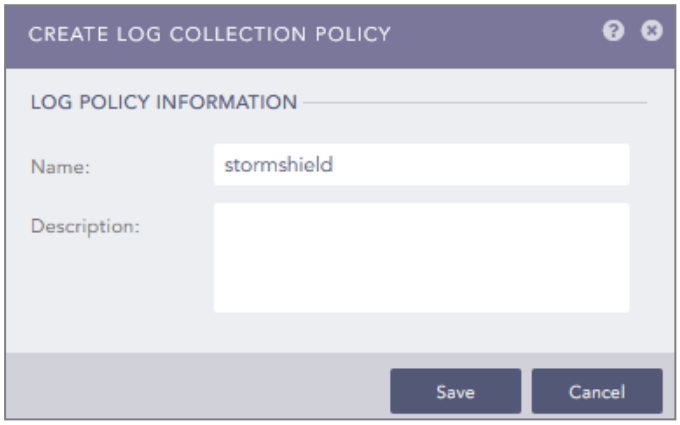
1. Go to **Settings** > **Configuration** > **Processing Policies** and click **Add**.
2. In the **Policy Name** field, enter "*stormshield*".
3. In the **Normalization Policy** field, select the "*stormshield*" normalization policy previously created.
4. In the **Enrichment Policy** field, select "*None*".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



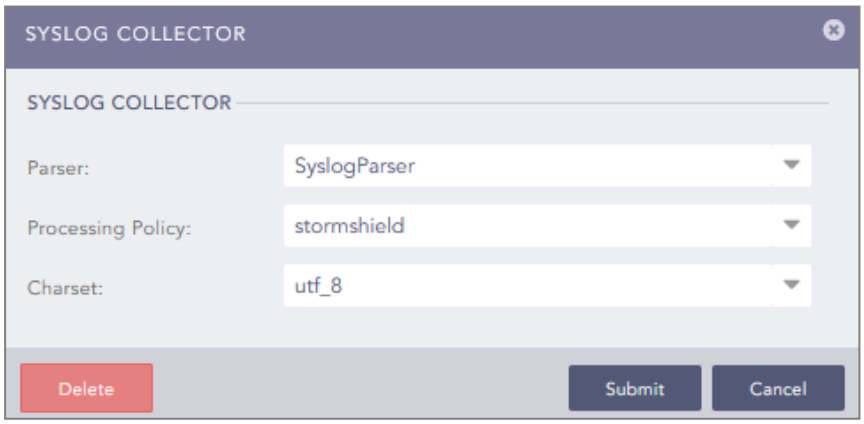
Adding a Stormshield Log Collection Policy

Log Collection Policies are the rules that SLS guardsix 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*".



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**.

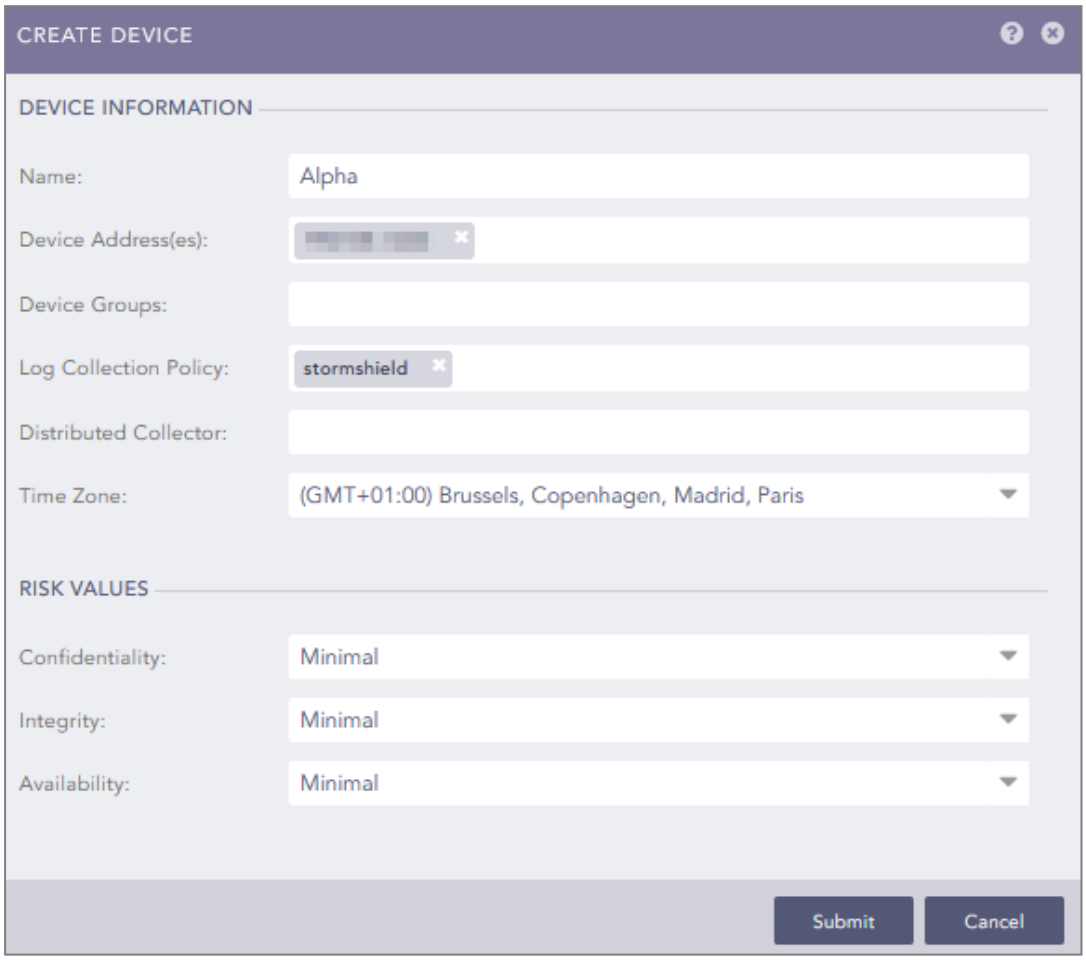


Adding a new SNS firewall device to SLS guardsix

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

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**.



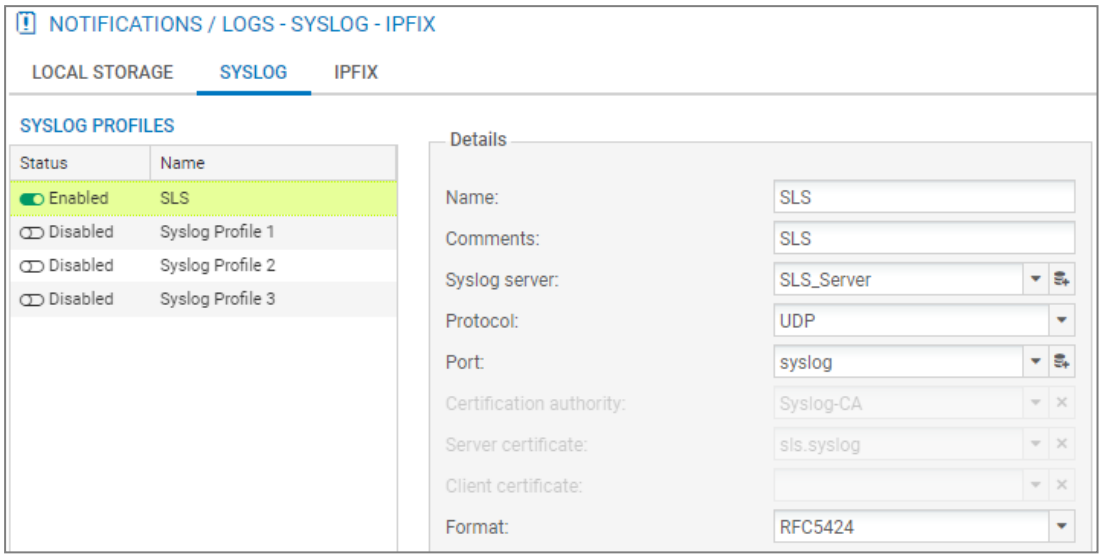
Configuring log retrieval between the SNS firewall and SLS guardsix

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 guardsix instance or create a new object if it does not exist yet.
3. Select the appropriate protocol (TCP or UDP). SLS guardsix supports both the TCP and UDP protocols for the Syslog collector, as mentioned in the Open Firewall Ports section of the guardsix SIEM documentation. Depending on your needs, you may wish to choose one or the other.
4. Select the port number. The default SLS guardsix listening port is *514*.

5. Select the format.
6. **Apply** the configuration.

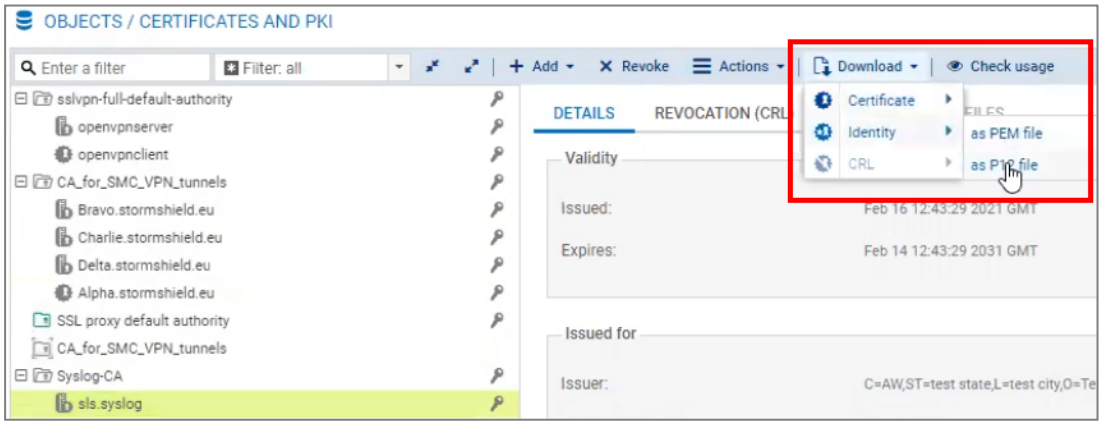


Continue to Adding Stormshield Dashboards to SLS guardsix.

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**.

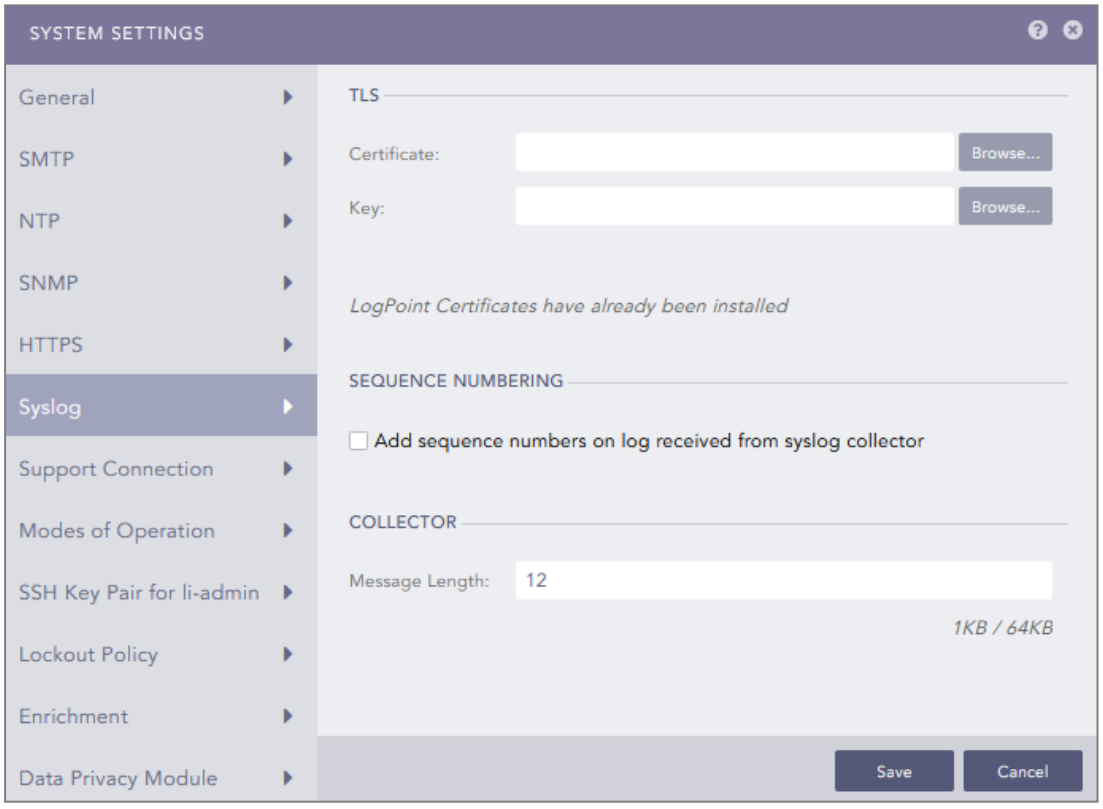


Extracting the private key and certificates from the P12 file

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 guardsix

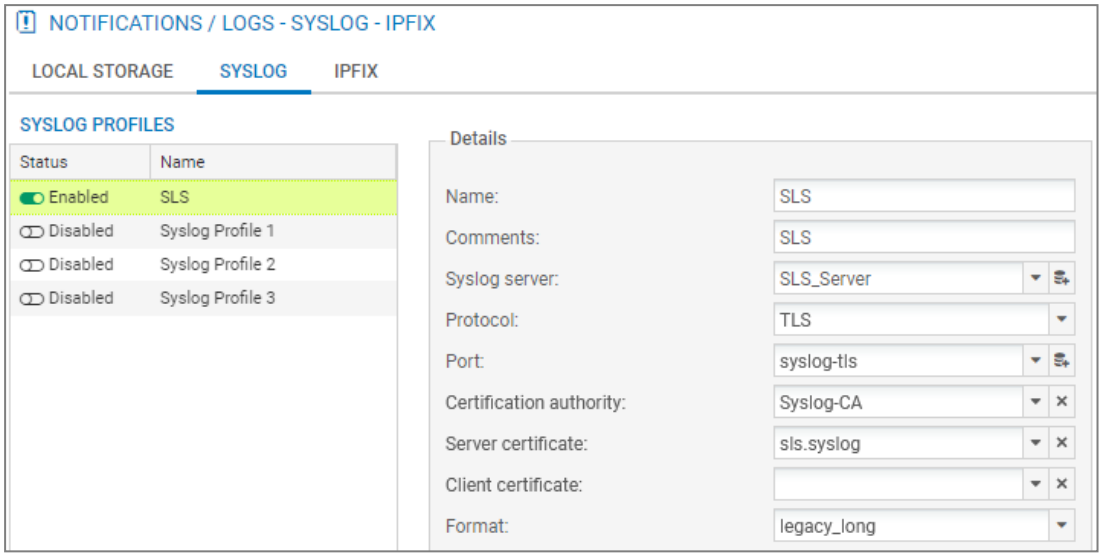
1. Go to **Settings** > **System Settings** > **System Settings**.
2. On the **Syslog** tab, click **Browse...** to import the **Certificate** (*.crt* file) and the **Key** (*.key* file).
3. Click **Save**.



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 guardsix 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.

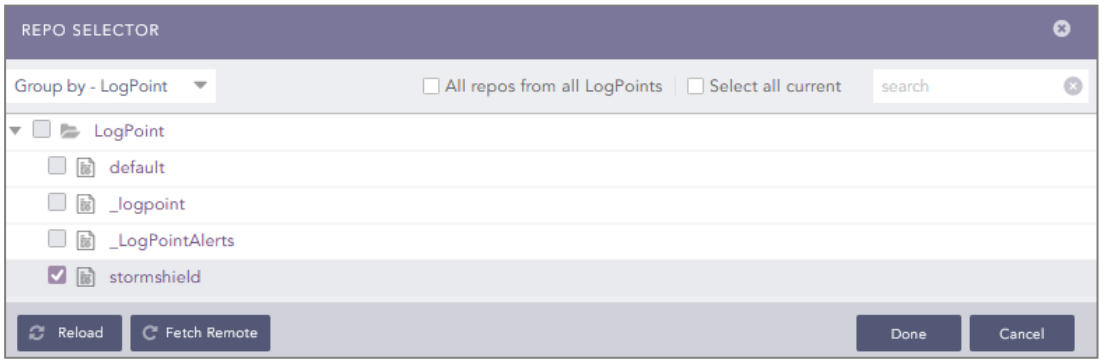
6. **Apply** the configuration.



Adding Stormshield Dashboards to SLS guardsix

Your SLS guardsix 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**.



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

Further reading

For more information on SLS guardsix, refer to the SLS guardsix documentation.

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

documentation@stormshield.eu