GUIDE

STORMSHIELD LOG SUPERVISOR

OVA DEPLOYMENT GUIDE

Version 2

Document last updated: July 4, 2024

Reference: sls-en-deployment_guide_ova

Table of contents

Change log ... 3

Getting started ... 4

Requirements ... 5

Deploying SLS OVA ... 6

- Selecting an OVA ... 6
- Selecting a Name and Folder ... 7
- Selecting a Computing Resource ... 7
- Reviewing the Template Details ... 8
- Selecting Storage ... 8
- Selecting Networks ... 9
- Wrapping up the Configuration ... 9

Activating SLS ... 10

- Accessing the SLS user interface ... 10
- Getting the SLS Hardware Key ... 10
- Registering the SLS product ... 10
- Downloading the SLS license (.pak file) ... 11
- Installing the license ... 11
- Changing the "admin" user password ... 12
- Updating SLS to the latest patch ... 13

Getting the logs from an SNS firewall ... 14

- Adding a new device on SLS ... 14
- Configuring logs retrieval ... 15
  - Getting the logs through standard Syslog ... 15
  - Getting the logs through Syslog-TLS ... 15

Getting the logs from SES Evolution ... 18

- Adding a new device on SLS ... 18
- Configuring logs retrieval ... 19
  - Getting the logs through standard Syslog ... 19
  - Getting the logs through Syslog-TLS ... 20

Further reading ... 22

Change log

Date	Description
July 4, 2024	New document

Getting started

Welcome to the Stormshield Log Supervisor OVA version 2 Deployment Guide.

This guide discusses the steps and considerations for deploying the SLS OVA on the VMWare ESXi server.

With the SLS OVA, you can use:

- **Virtualization** to transform data centers into simplified cloud computing infrastructures and use flexible and reliable IT services. VMware vSphere virtualizes and aggregates the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the data center.
- **Managed Infrastructure** to utilize large collections of infrastructures such as CPUs, storage, and networking as a seamless and dynamic operating environment without worrying about the complexity of a data center.

For a better assessment of this guide, we expect you to have a basic understanding of the VMware vSphere and its core services.

In the documentation, Stormshield Log Supervisor is referred to in its short form SLS, Stormshield Network Security in its short form SNS, and Stormshield Endpoint Security Evolution in its short form SES Evolution.

IMPORTANT
This document covers only SLS version 2 deployments.

Requirements

Compatibility

For more information about the SLS Life Cycle management policy and compatibilities, refer to the Product life cycle Log Supervisor guide.

Minimum recommended specifications

- CPU: Quad-core
- RAM: 7GB
- Disk space: 169GB

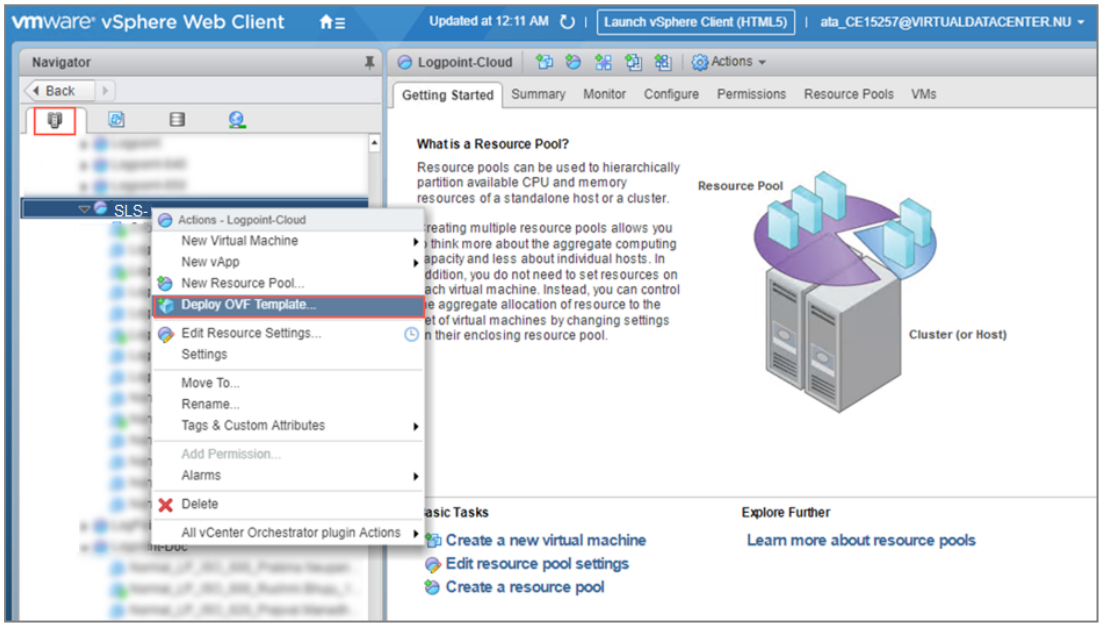
NOTES

- These recommended specifications **only apply** to launch SLS on a new installation. If you are updating your SLS, these recommended specifications **may not apply**. For updating your SLS, please refer to the Update Guide.
- The chosen specifications must be consistent with the infrastructure in which SLS will be deployed and the amount of sources and logs that SLS will manage.

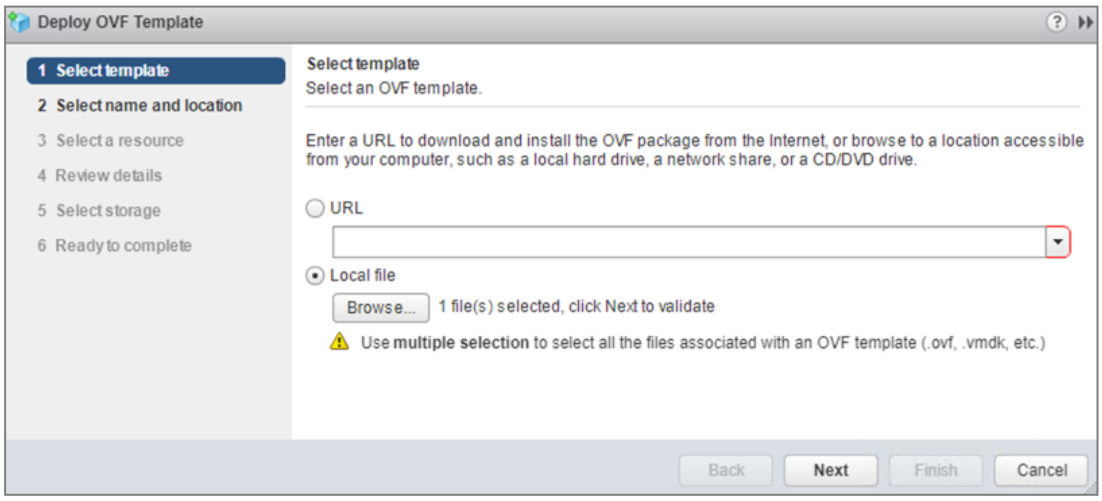
Deploying SLS OVA

Selecting an OVA

1. Download the provided SLS *.ova* file from your MyStormshield personal area, in **Downloads > Downloads > Stormshield Log Supervisor > Firmware**.
2. Log in to your vSphere client.
3. Click the **Host and Cluster** icon.
4. Select the required resource pool to install the OVA.
5. Right-click the required resource pool and click **Deploy OVF Template**.

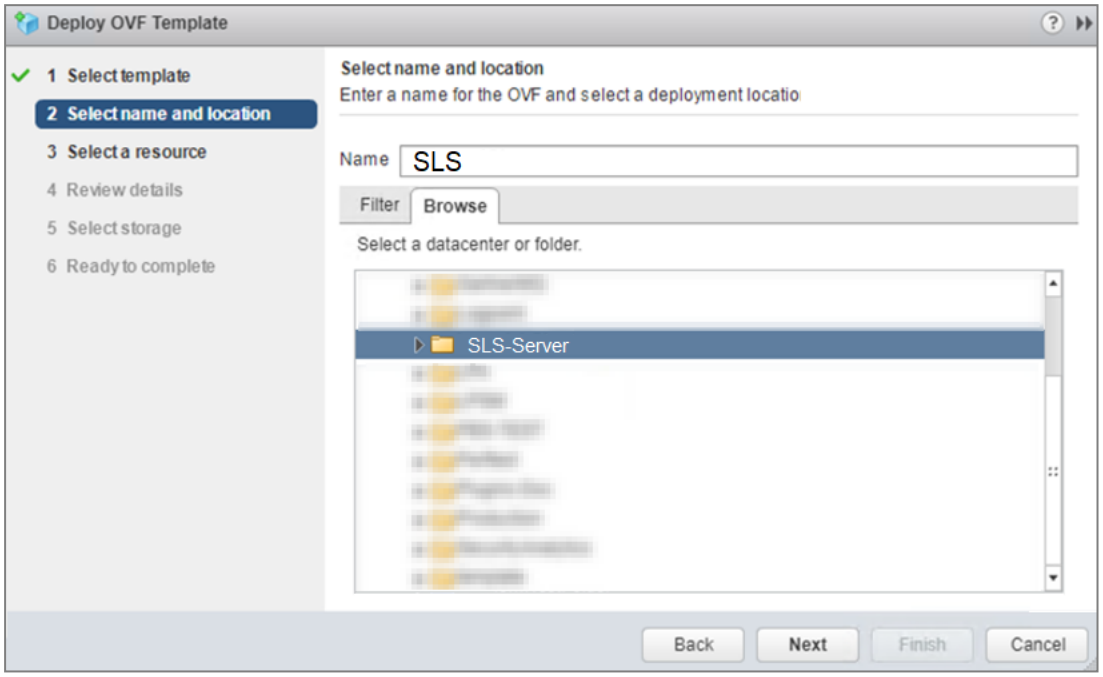


6. Select the **Local file** option.
7. Click **Choose files**, browse the OVA file and click **Next**.



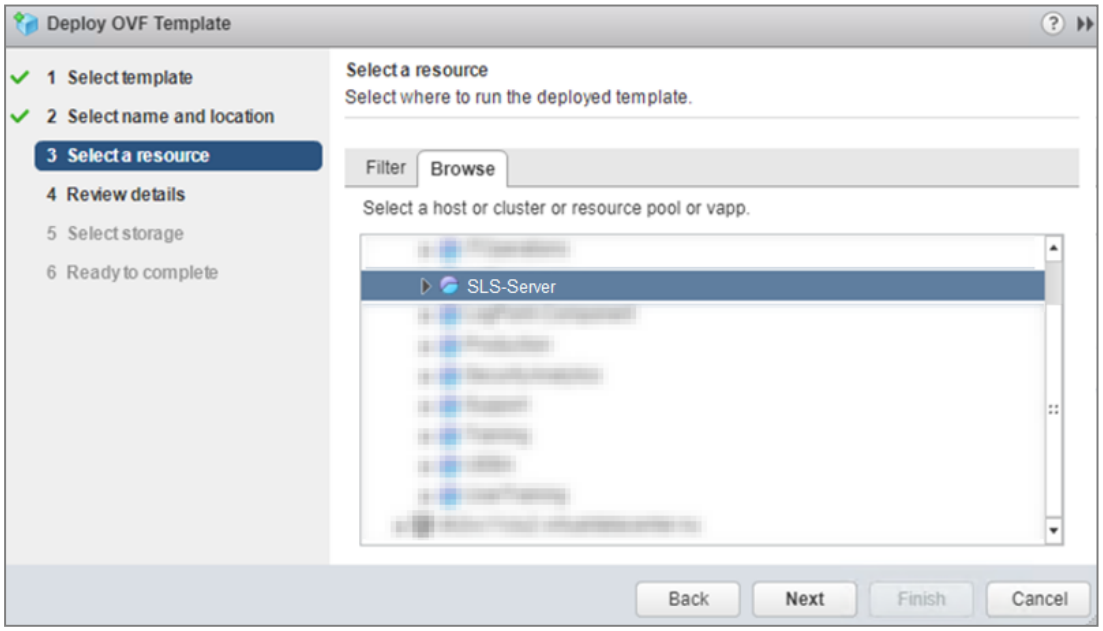
Selecting a Name and Folder

1. Enter a **Virtual machine name**.
2. Select a **target location** for the virtual machine and click **Next**.



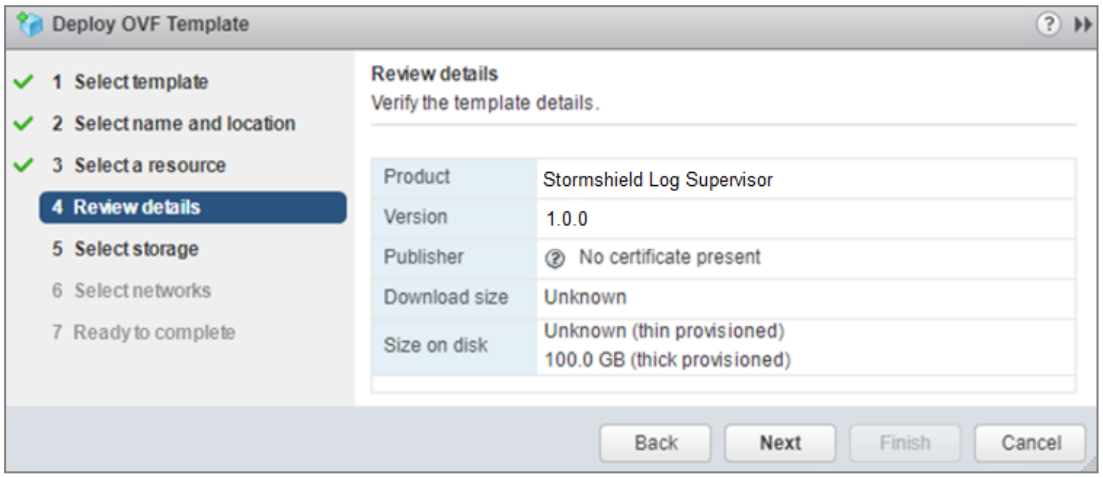
Selecting a Computing Resource

1. Select the **destination resource** for the virtual machine and click **Next**.



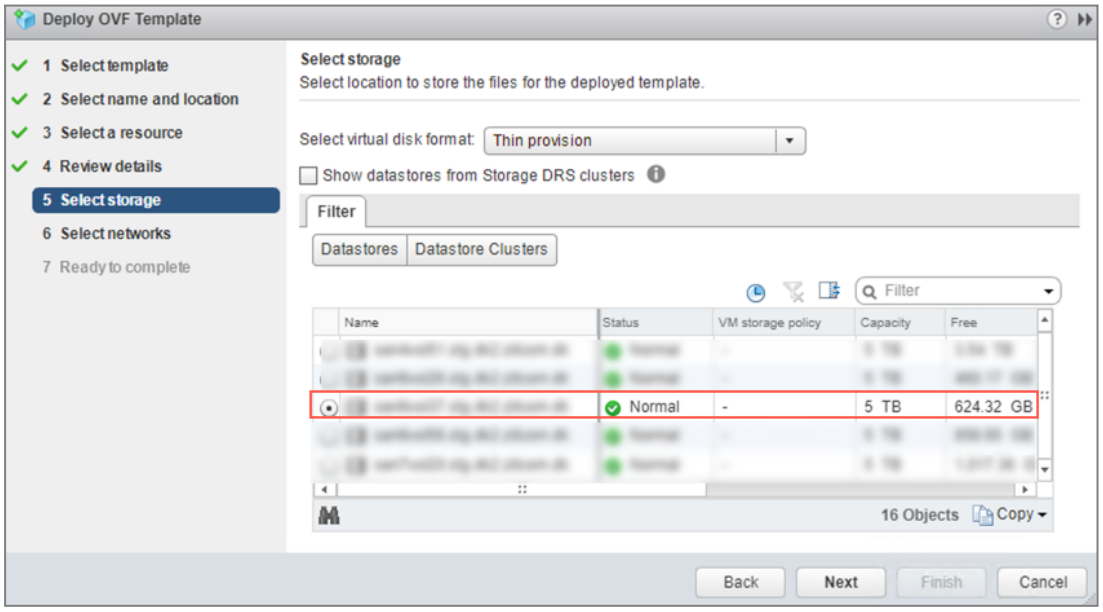
Reviewing the Template Details

1. **Review** the details of the OVA and click **Next**.



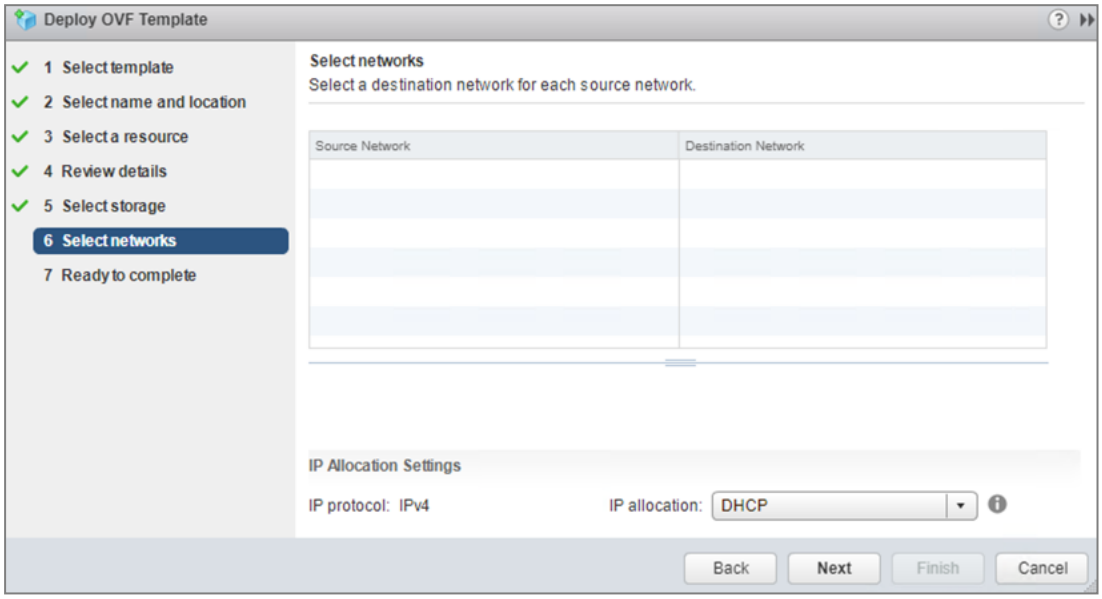
Selecting Storage

1. Select the **virtual disk format**:
   - Select the **Eager Zeroed Thick Provision** format to allocate the storage and clear all the data inside the disk array immediately.
   - Select the **Lazy Zeroed Thick Provision** format to allocate the storage immediately, and clear all the data of the disk array only on demand.
   - Select the **Thin Provision** format to allocate the storage and clear the data of the disk array only on demand.
2. Select a **VM Storage Policy** from the drop-down menu.
3. Select a **datastore** to deploy the virtual machine and click **Next**.



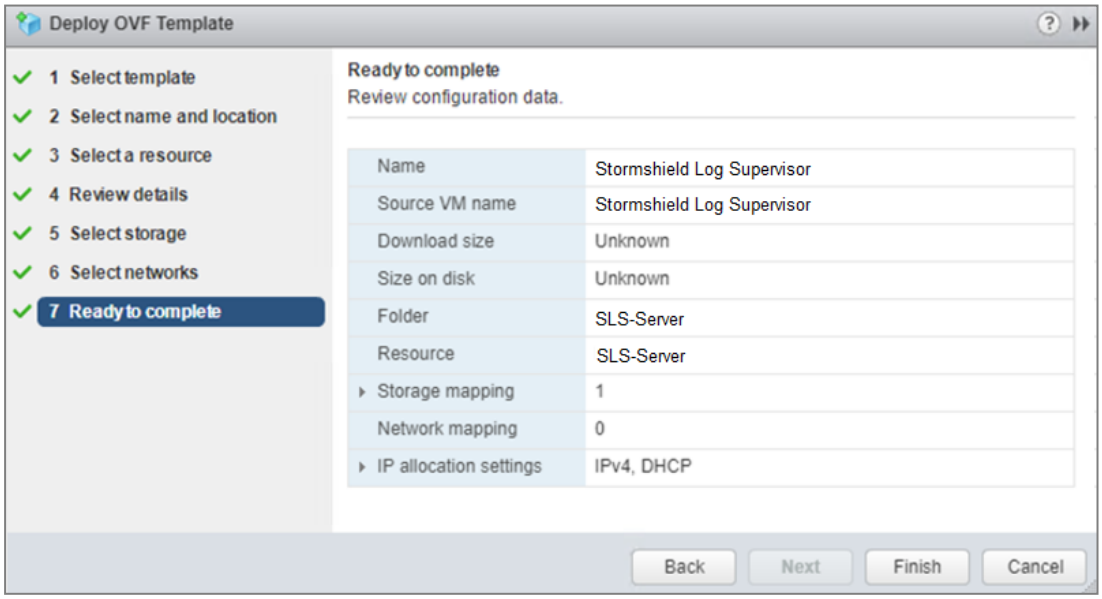
Selecting Networks

1. On the **IP Allocation Settings** section, select the **IP allocation** option for the virtual machine and click **Next**. If IP addresses are not distributed via a DHCP server, you must set the IP address while accessing the SLS instance. For more information, refer to Accessing the SLS user interface.



Wrapping up the Configuration

1. **Review** the configuration before creating a virtual machine. Click **Back** before finalizing the configuration if necessary.
2. Click **Finish** to create the virtual machine.



Activating SLS

Accessing the SLS user interface

1. Select the required virtual machine and go to **Actions >> Power >> Power On**.
2. Note down its IP address. If it is not displayed, see the instructions below.
3. Enter the IP address in a web browser (example: https://10.45.3.95).
4. Log in to the SLS user interface. The default credentials are *admin* (username) and *changeme* (password).

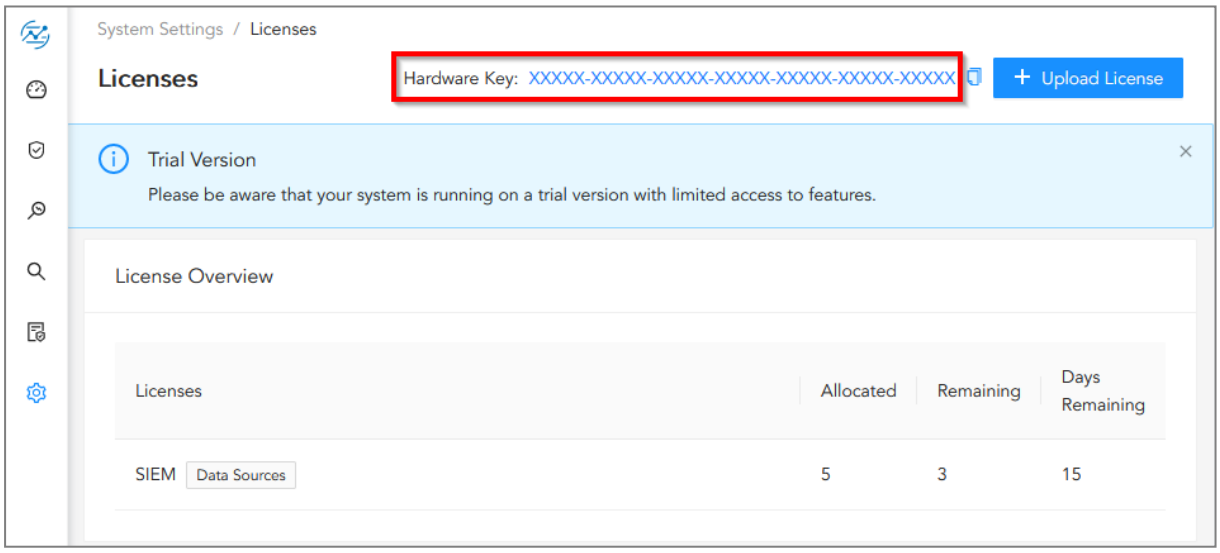
If you need to get or set the IP address of the SLS instance:

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 Hardware Key

Once connected to the SLS user interface for the first time, it is requested to activate SLS 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. You can find it here:



Registering the SLS product

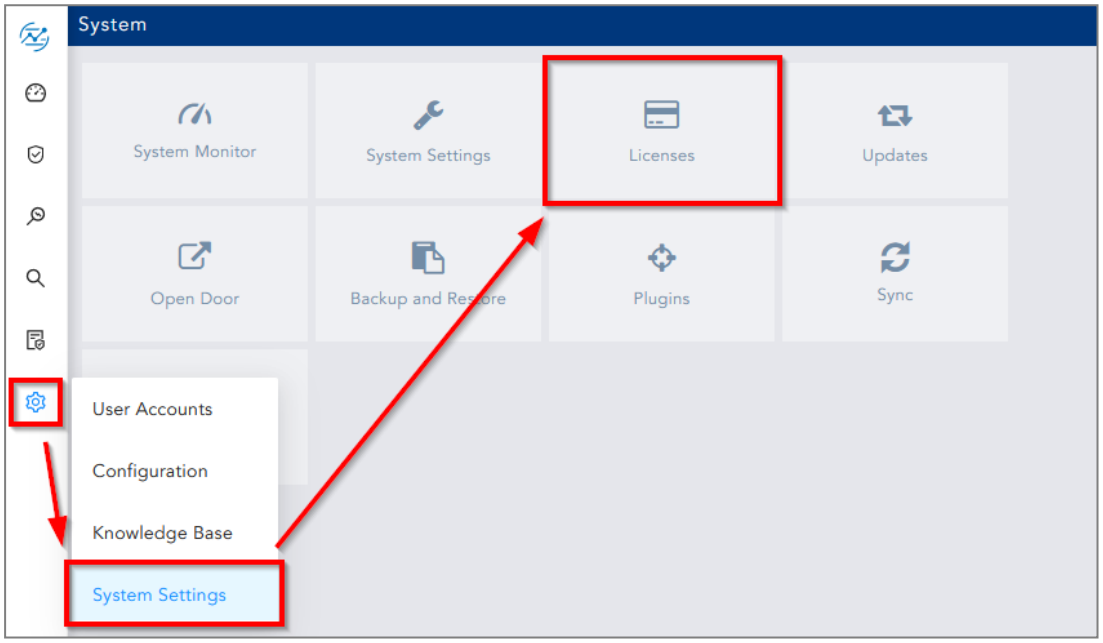
You must contact your Stormshield reseller or partner to obtain an SLS product. Then, register it in your MyStormshield personal area. You will be prompted to enter your SLS Hardware Key and SLS Serial Number. For more information, refer to the Registering products guide.

Downloading the SLS license (*.pak* file)

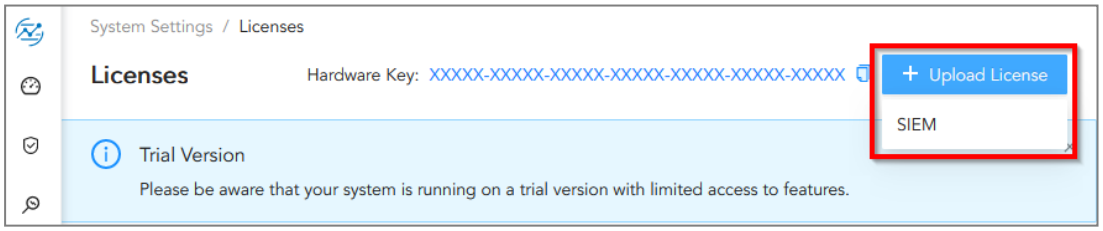
Download the license (*.pak* file) from your MyStormshield personal area. For more information, refer to the Downloading a product's license file page.

Installing the license

1. On SLS, go to **Settings >> System Settings** in the navigation bar on the left and click **License**.

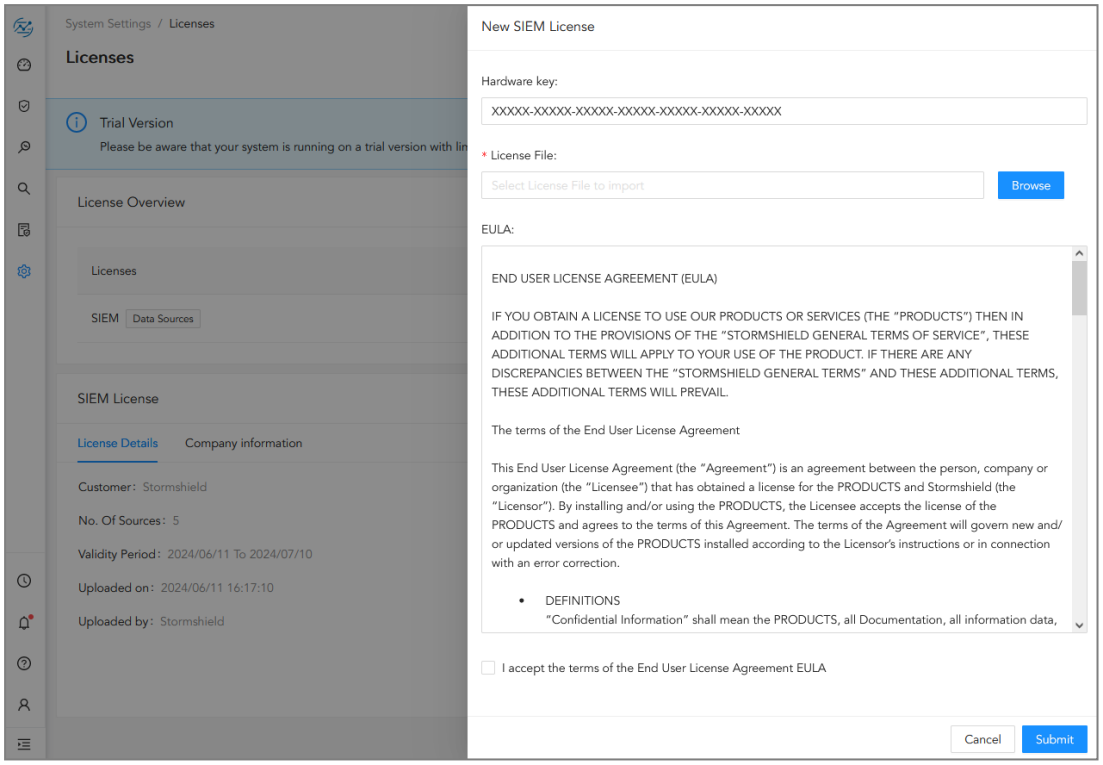


2. Click **Upload License > SIEM**.



3. Browse to the file containing the **License Key**.
4. Go through the **END USER LICENSE AGREEMENT** (EULA).

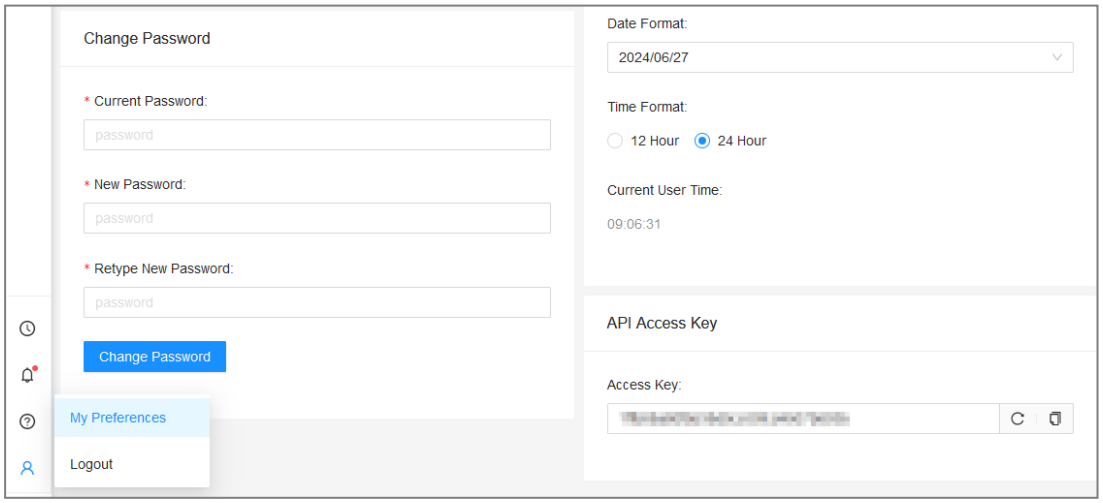
5. Click **Submit** if you agree with the terms and conditions of the EULA.



Changing the "admin" user password

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

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



Updating SLS to the latest patch

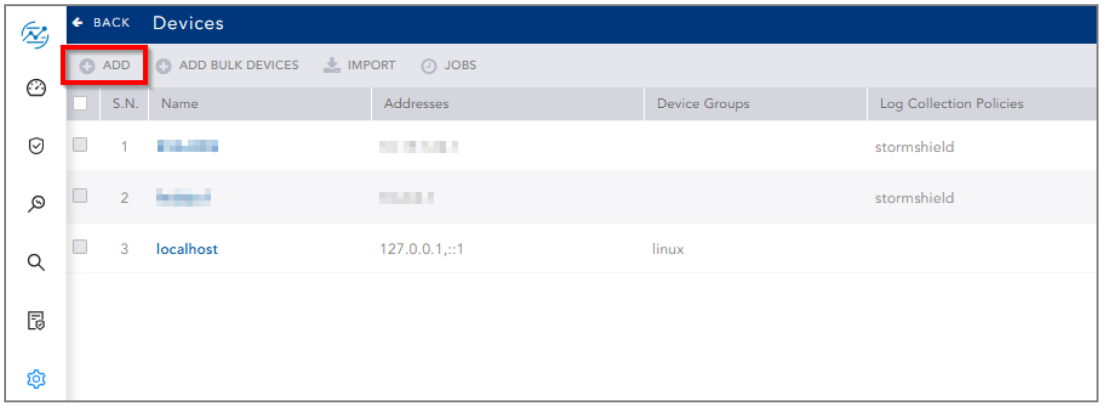
1. Identify the current SLS version installed. On SLS, click on ⓘ **Help > About SLS** in the navigation bar on the left and look for the version number.

2. Check the version release notes to see if a newer SLS version is available. If so, refer to the Update Guide to install it.

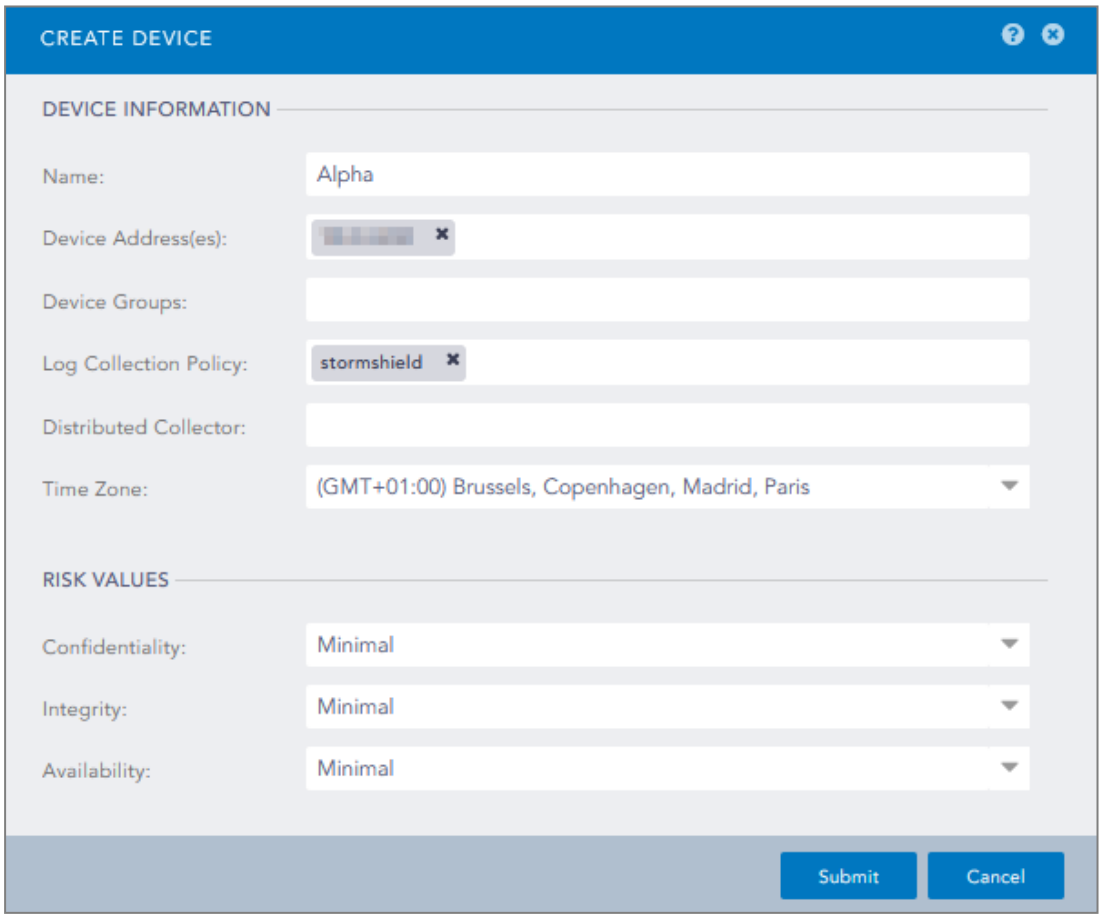
Getting the logs from an SNS firewall

Adding a new device on SLS

1. On SLS, go to **Settings >> Configuration >> Devices** and click **Add**.



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 *stormshield*.
5. Choose the correct **Time Zone**.
6. Click **Submit**.



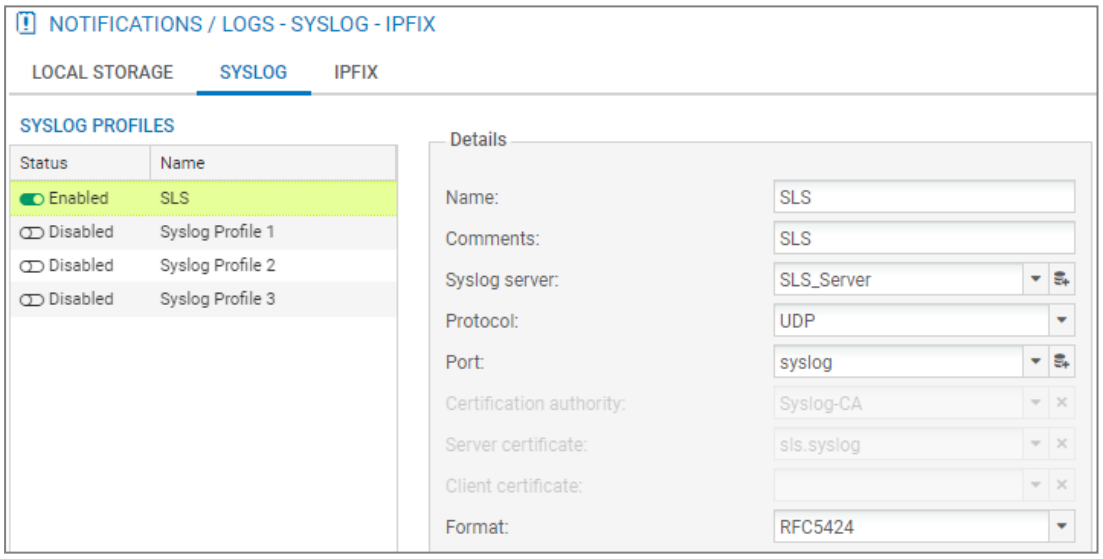
Configuring logs retrieval

You can choose to either get the logs from the SNS firewall through standard Syslog or more securely through Syslog-TLS.

Getting the logs through standard Syslog

Configuring a standard Syslog connection on the SNS firewall

1. On SNS, go to **Configuration > Notifications > Logs – Syslog – IPFIX > Syslog**.
2. Select the object representing the IP address of the SLS instance or create a new object if one has not been created yet.
3. Select the appropriate protocol (TCP or UDP).
4. Select the port number. The default listening port is *514*. You can retrieve the Syslog listening port by using the "`change-syslog-port`" command on a VM console. Note that using this command toggles the port between *514* and *601*. Use it again if necessary.
5. Select the format.
6. **Apply** the configuration.

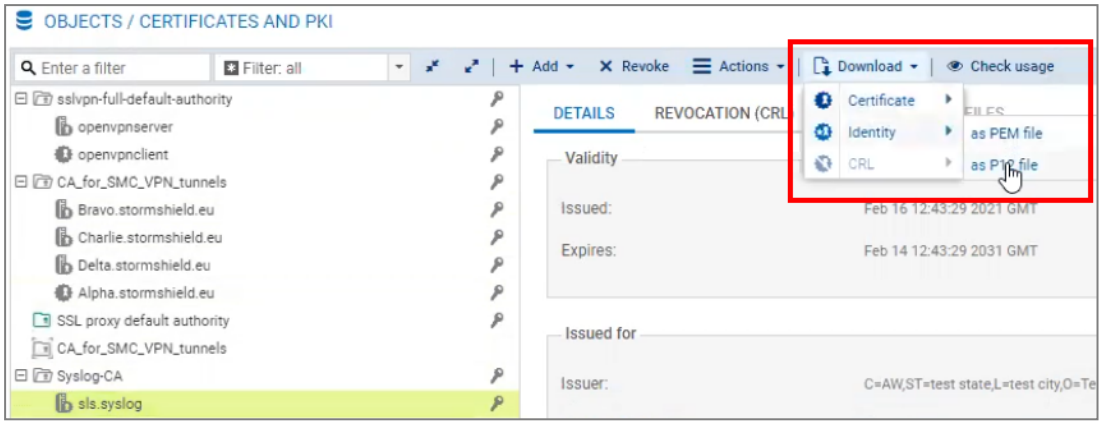


Getting the logs through Syslog-TLS

Downloading SNS Certificate Identity

1. On SNS, go to **Configuration > Objects > Certificates and PKI**.
2. Create a **Server Identity** with *RSA* as **Key type**.

3. Download the Server Certificate identity as a P12 file.



Extract the key from the certificate

On a terminal emulator, use the following commands. Customize the *.p12*, *.key* and *.crt* file names to match your case.

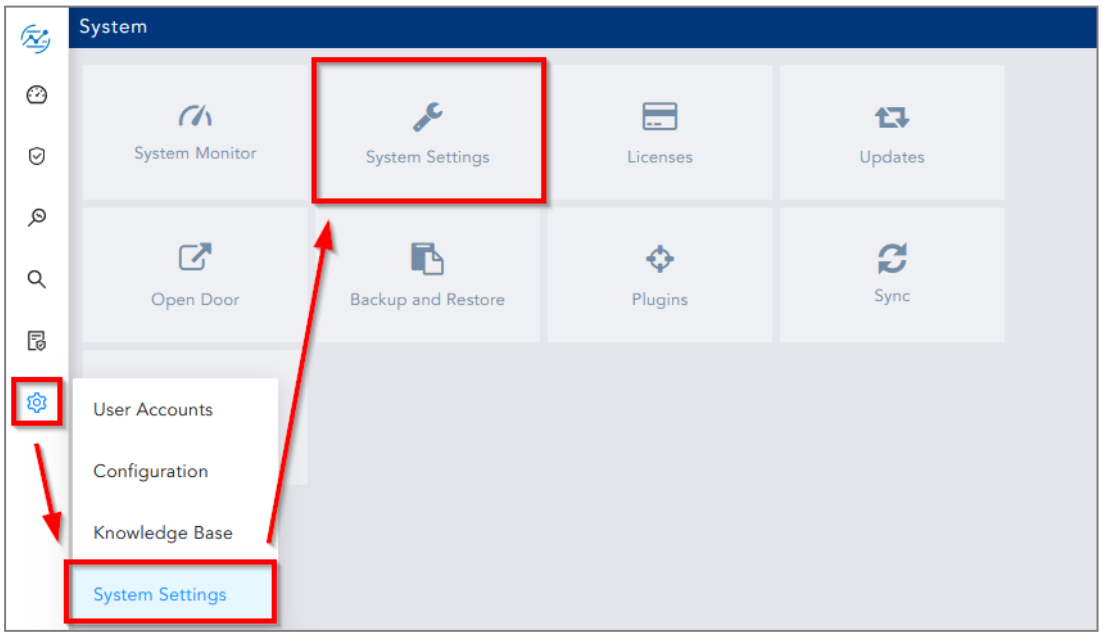
```
~/ SYSLOG-TLS ]$ openssl pkcs12 -in syslog2.sls.local.p12 -out
syslog2.sls.local.key -nocerts
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
~/SYSLOG-TLS ]$ openssl pkcs12 -in syslog2.sls.local.p12 -out
syslog2.sls.local.crt -nokeys -clcerts
Enter Import Password:
```

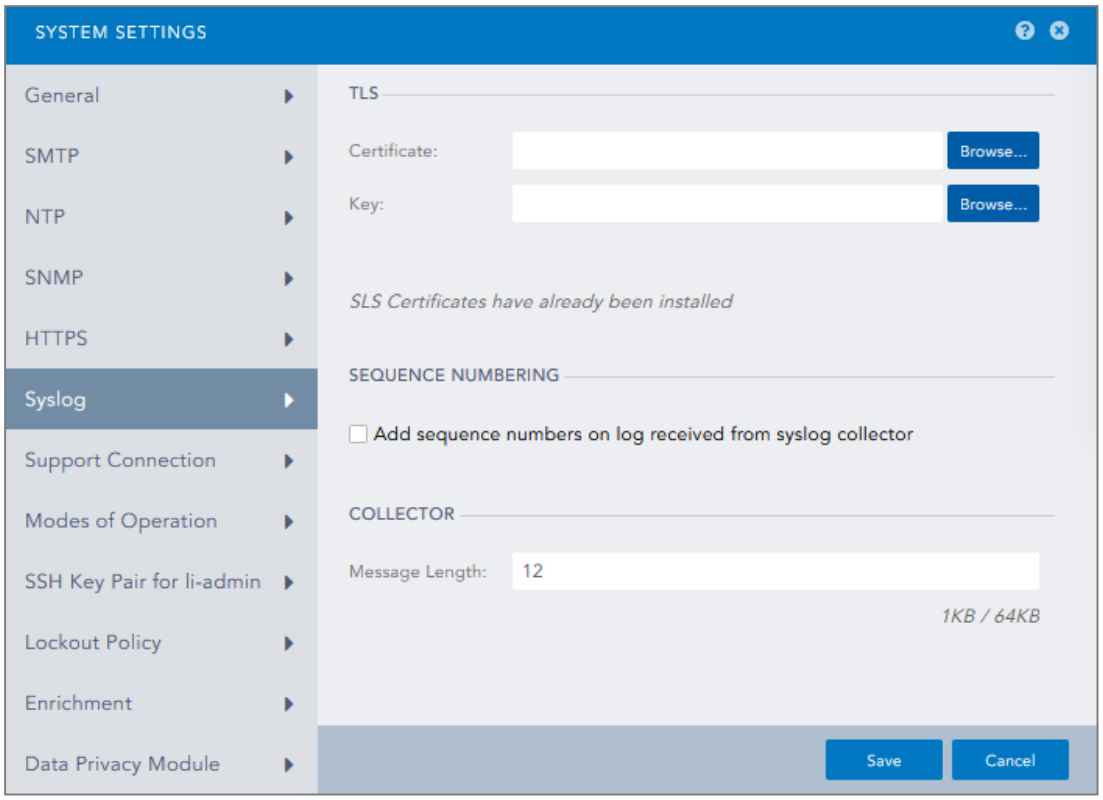
```
~/SYSLOG-TLS ]$ openssl rsa -in syslog2.sls.local.key -out syslog2.sls.local-
unprotected.key
Enter pass phrase for syslog2.sls.local.key:
writing RSA key
```

Importing the SNS Certificate Identity on SLS

1. On SLS, go to **Settings >> System Settings >> System Settings**.

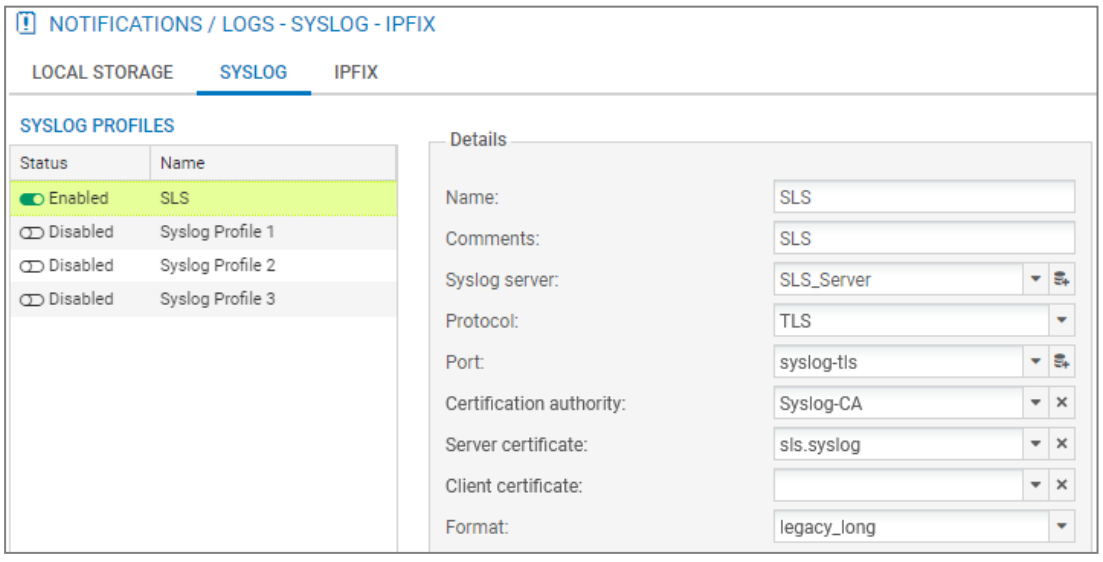


2. On the **Syslog** tab, import the **Certificate** (*.crt* file) and the **Key** (*.key* file).
3. **Save**.



Configuring a Syslog-TLS connection on the SNS firewall

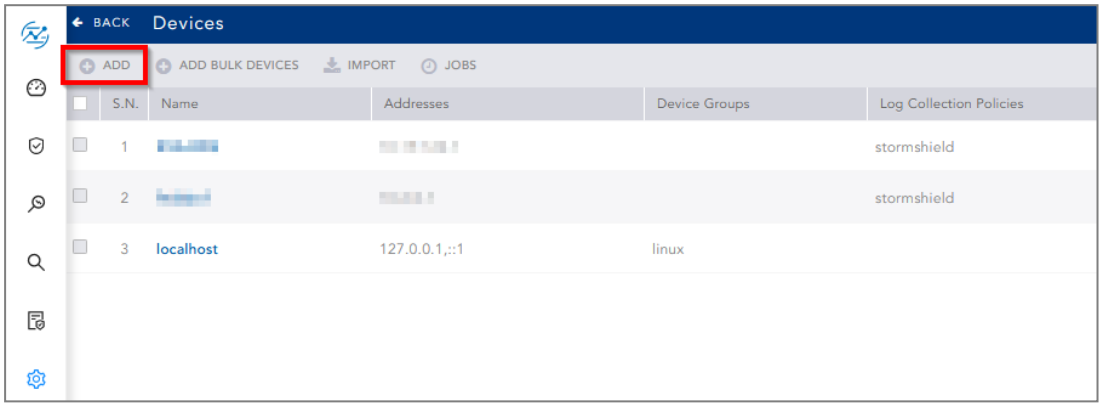
1. On SNS, go to **Configuration > Notifications > Logs – Syslog – IPFIX > Syslog**.
2. Select the object representing the IP address of the SLS instance or create a new object if one has not been created yet.
3. Choose *TLS* Protocol.
4. Fill in the certificate information.
5. Select *legacy_long* format.
6. **Apply** the configuration.



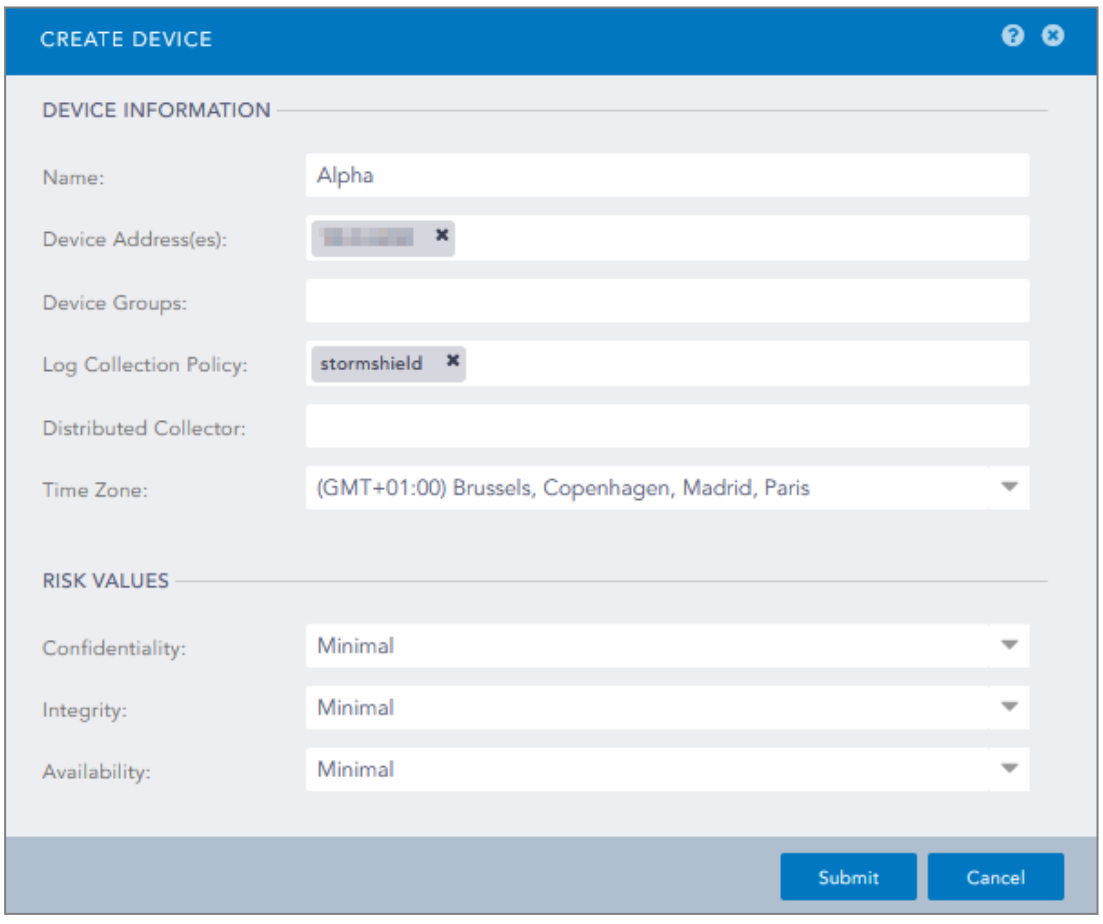
Getting the logs from SES Evolution

Adding a new device on SLS

1. On SLS, go to **Settings >> Configuration >> Devices** and click **Add**.



2. Enter the **Name** of the device.
3. In the **IP address(es)** field, enter he IP addresses of each machine that hosts an SES Agent handler that communicates with SLS.
4. In the **Log Collection Policy** field, select *stormshield*.
5. Choose the correct **Time Zone**.
6. Click **Submit**.



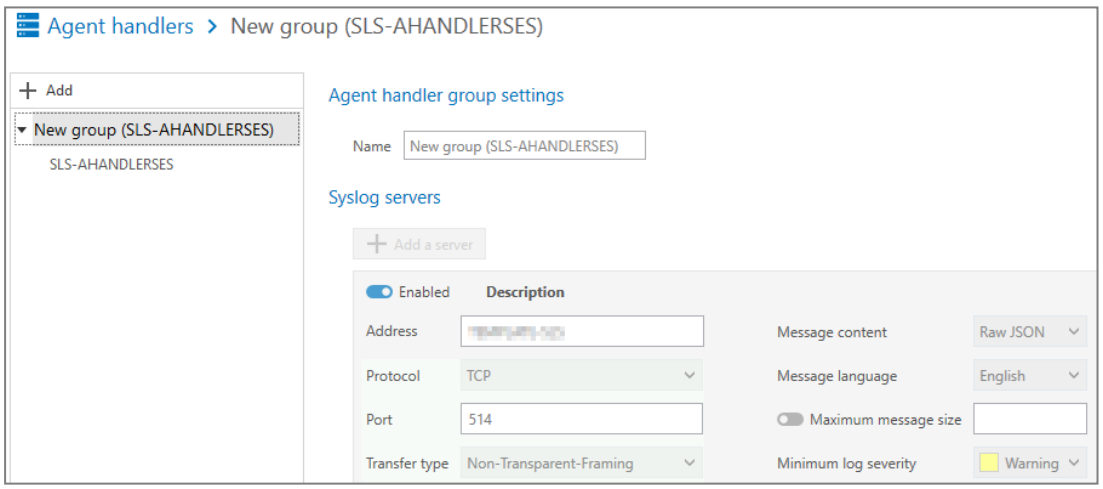
Configuring logs retrieval

You can choose to either get the logs from SES Agent handlers through standard Syslog or more securely through Syslog-TLS.

Getting the logs through standard Syslog

Configuring a TCP or UDP connection on the Agent handler

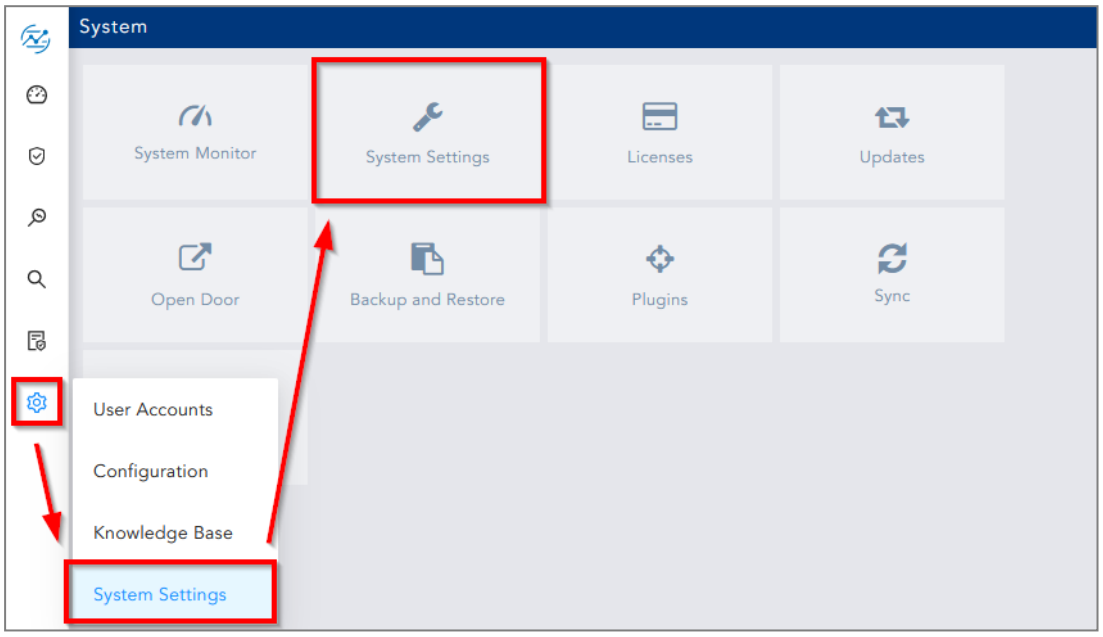
1. On the SES Evolution administration console, go to the **Agent handlers** menu and click the **+** icon.
2. Enter the **Name** of the Agent handler group.
3. In the **Address** field, enter the IP address of the SLS instance.
4. Select the appropriate **Protocol** (TCP or UDP).
5. Enter the **Port** number. The default listening port is *514*. You can retrieve the Syslog listening port by using the "`change-syslog-port`" command on a VM console. Note that using this command toggles the port between *514* and *601*. Use it again if necessary.
6. In the **Transfer type** field, choose *Non-Transparent-Framing*.
7. In the **Message content** field, choose *Raw JSON*.
8. Click **Save** in the upper banner.



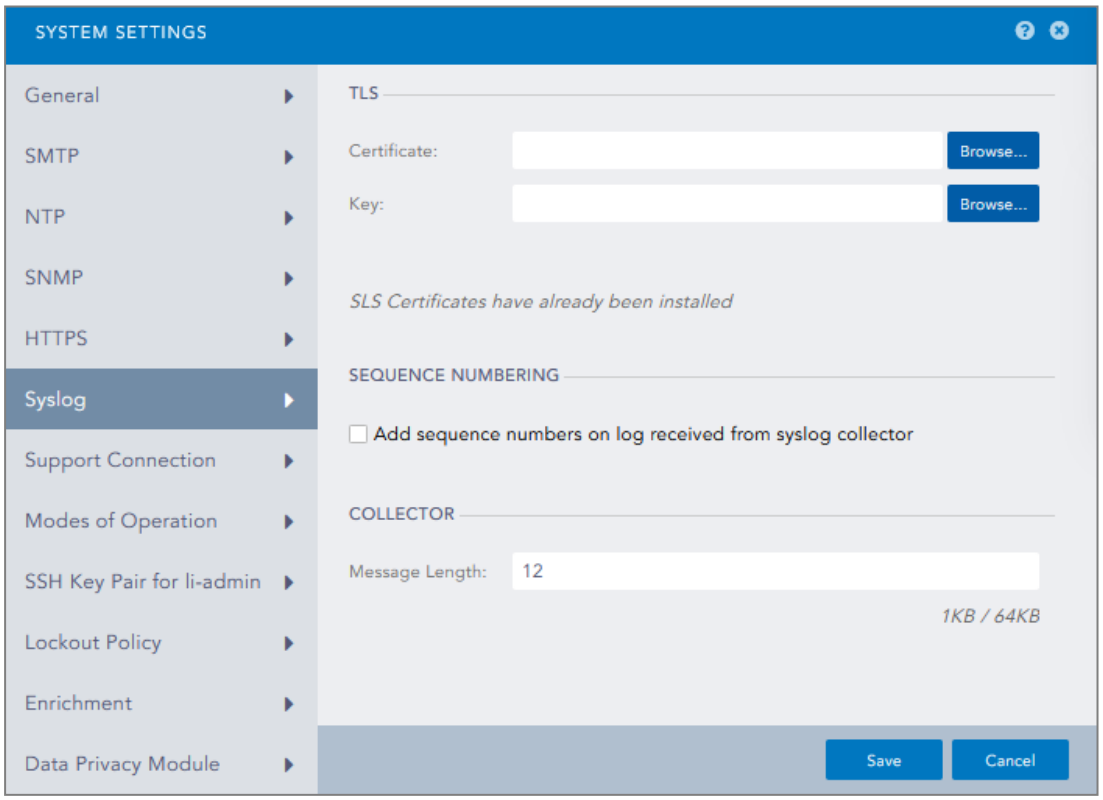
Getting the logs through Syslog-TLS

Generating and importing the Certificate Identity on SLS

1. On the host system used to generate certificates, generate a PEM X.509 certificate.
2. On SLS, go to **Settings >> System Settings >> System Settings**.



3. On the **Syslog** tab, import the **Certificate** (*.crt* file) and the **Key** (*.key* file).
4. **Save**.

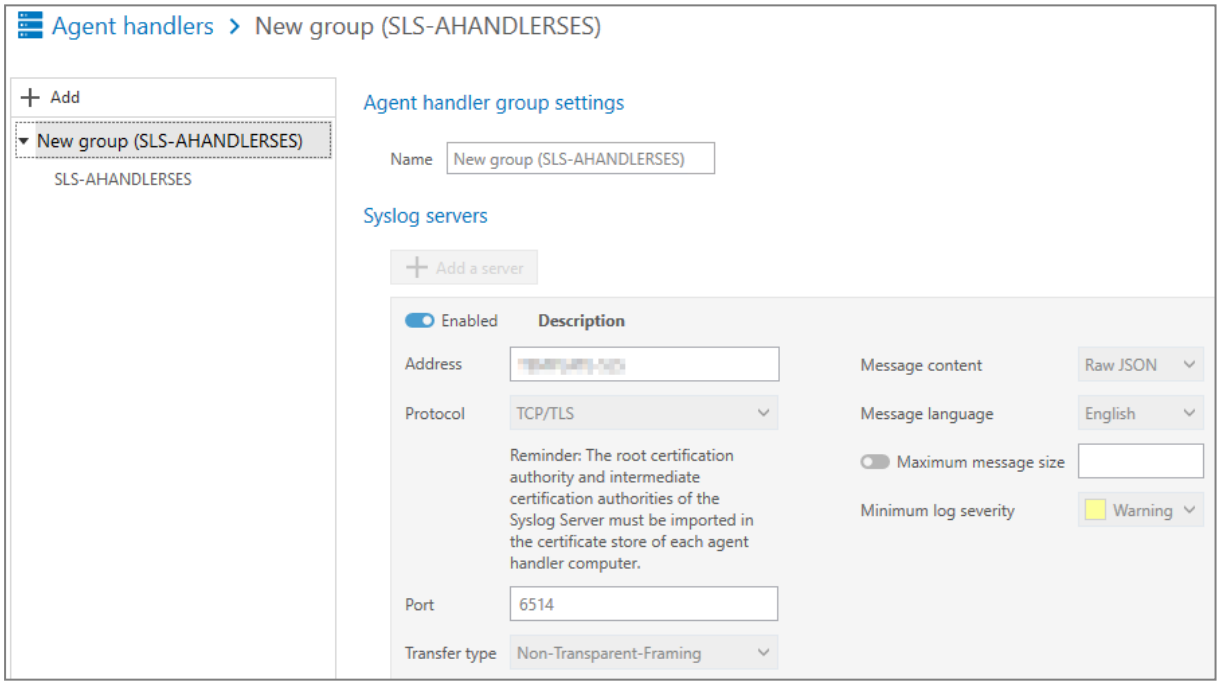


Importing the Root Certificate Authority

On each machine that hosts an SES Agent handler that communicates with SLS, install the root certificate in the Trusted root certification authorities or Third-party root certificate authorities certificate store.

Configuring a TCP/TLS connection on the Agent handler

1. On the SES Evolution administration console, go to the **Agent handlers** menu and click the **+** icon.
2. Enter the **Name** of the agent handler group.
3. In the **Address** field, enter the IP address of the SLS instance.
4. Select the *TCP/TLS* **Protocol**.
5. Enter the **Port** *6514*.
6. In the **Transfer type** field, choose *Non-Transparent-Framing*.
7. In the **Message content** field, choose *Raw JSON*.
8. Click **Save** in the upper banner.



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