GUIDE

STORMSHIELD LOG SUPERVISOR

OVA DEPLOYMENT GUIDE

Version 1

Document last updated: July 13, 2023

Reference: sls-en-deployment_guide_ova

Table of contents

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.

Change log

Date	Description
July 13, 2023	- Section 2 Requirements added - Section 3.6 Selecting Networks modified - Section 4.1 Accessing the SLS user interface modified - Section 4.2 Getting the SLS Hardware Key modified - Section 4.3 Registering the SLS product modified - Section 4.4 Downloading the SLS license added - Section 4.5 Installing the license modified - Section 4.6 Changing the "admin" user password added - Section 4.7 Updating SLS to the latest patch added - Section 6 Getting the logs from SES Evolution added - Section 7 Further reading added
August 30, 2022	- Section 4.3 Registering the SLS product modified
November 25, 2021	- SLS 1.1 Release - Added VMWare ESXi server 7.0 compatibility - End of support for VMWare ESXi server 6.5
May 6, 2021	- New document

1. Getting started

Welcome to the Stormshield Log Supervisor OVA version 1 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.

2. Requirements

2.1 Virtual Machine Compatibility

The SLS OVA allows you to launch an SLS virtual machine in:

- VMWare ESXi 6.7.
- VMWare ESXi 7.0.

2.2 Minimum recommended specifications

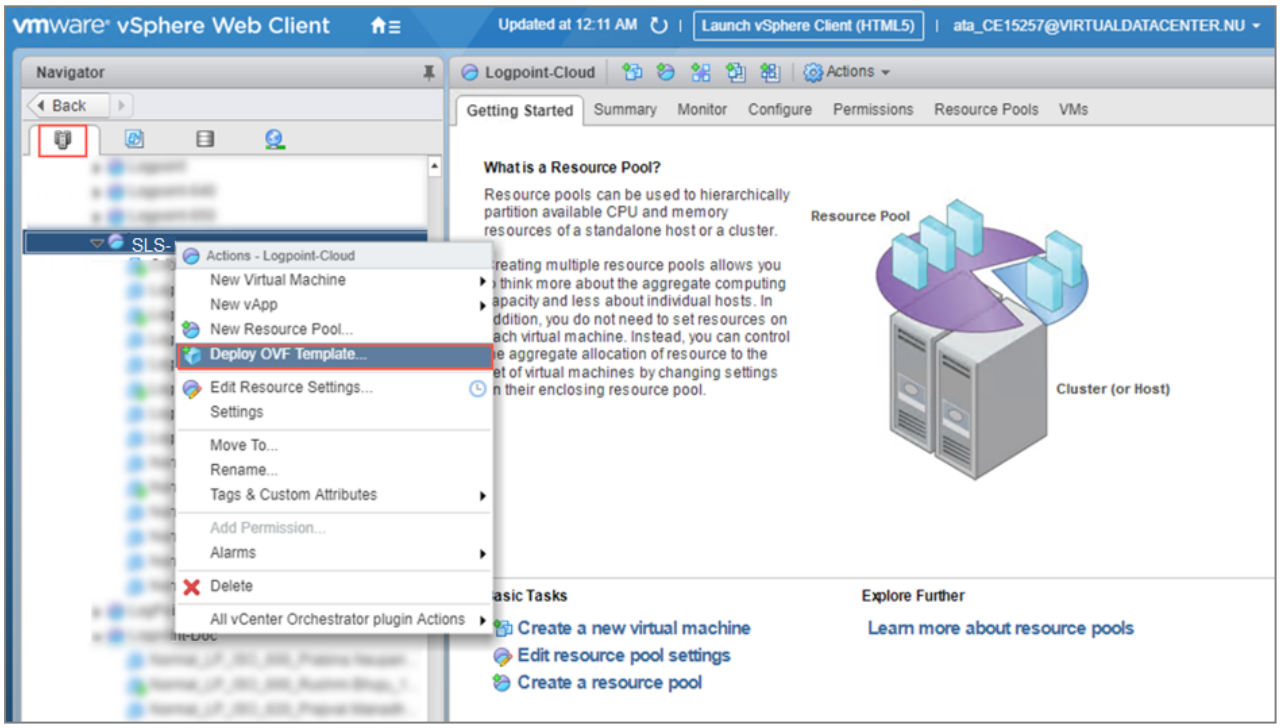
The minimum recommended specifications to launch SLS are:

- **CPU**: Minimum Quad-core.
- **Memory**: Minimum 7GB.
- **Disk**: Minimum 169GB.

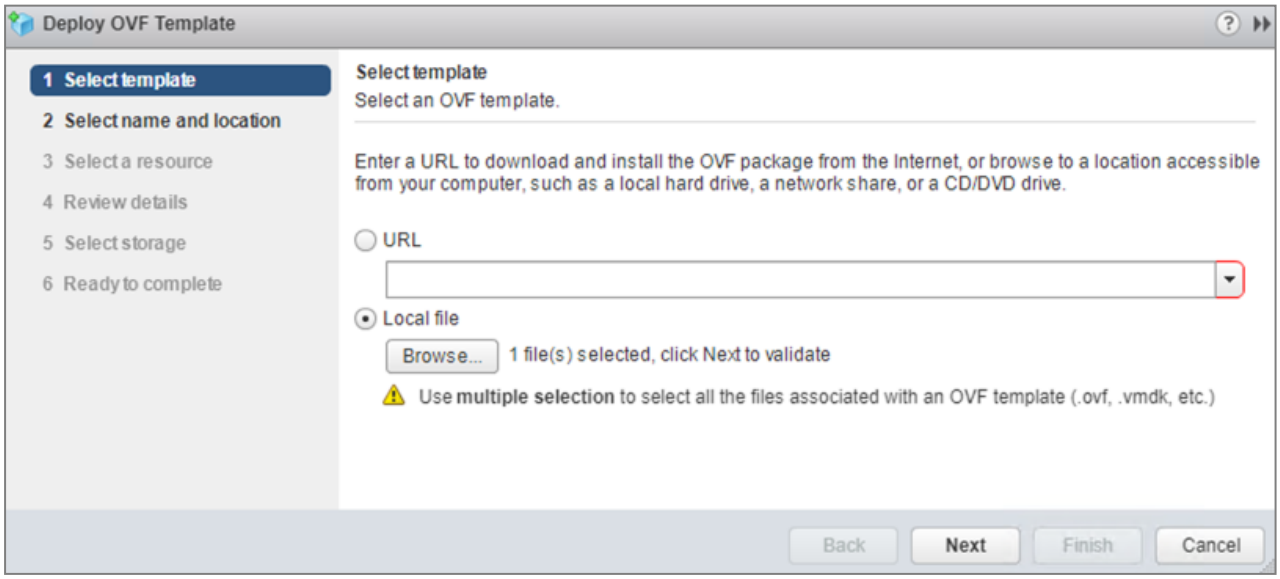
3. Deploying SLS OVA

3.1 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**.

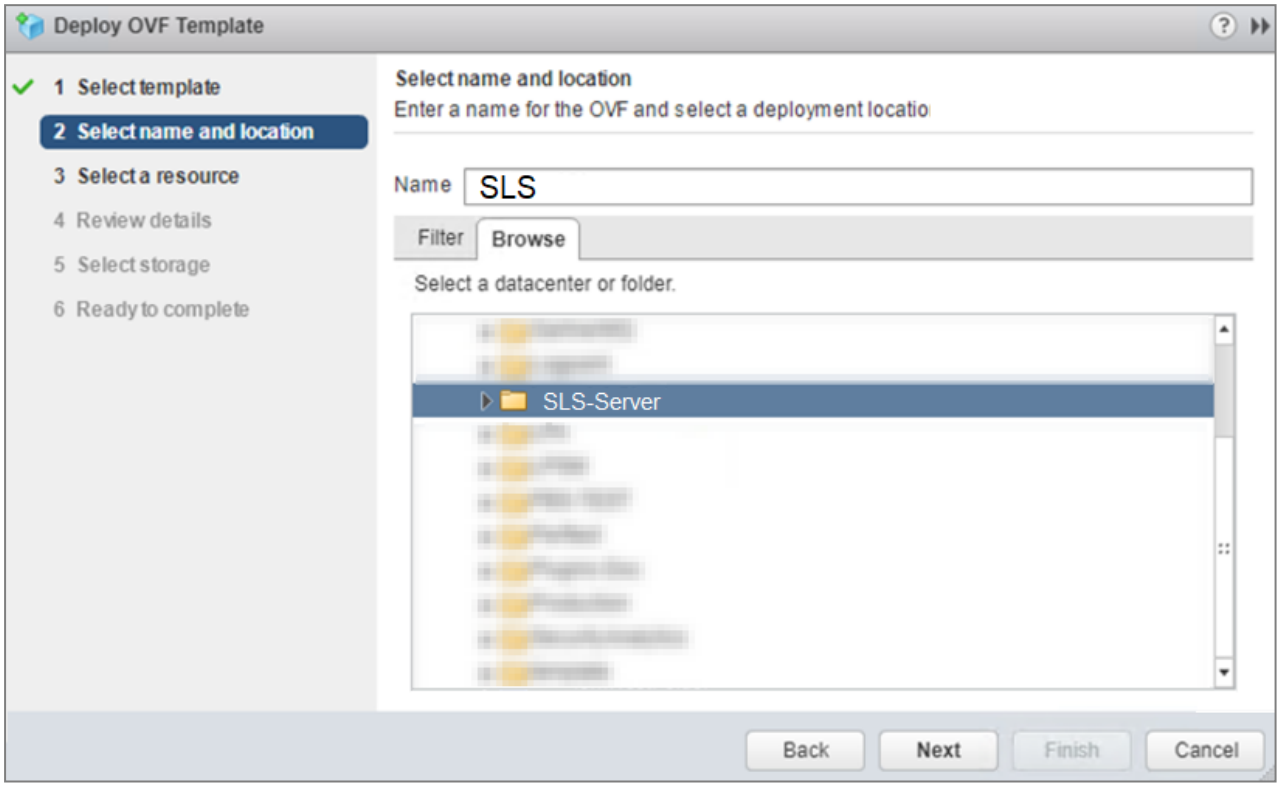


6. Select the **Local file** option.
7. Click **Choose files**, browse the OVA file and click **Next**.



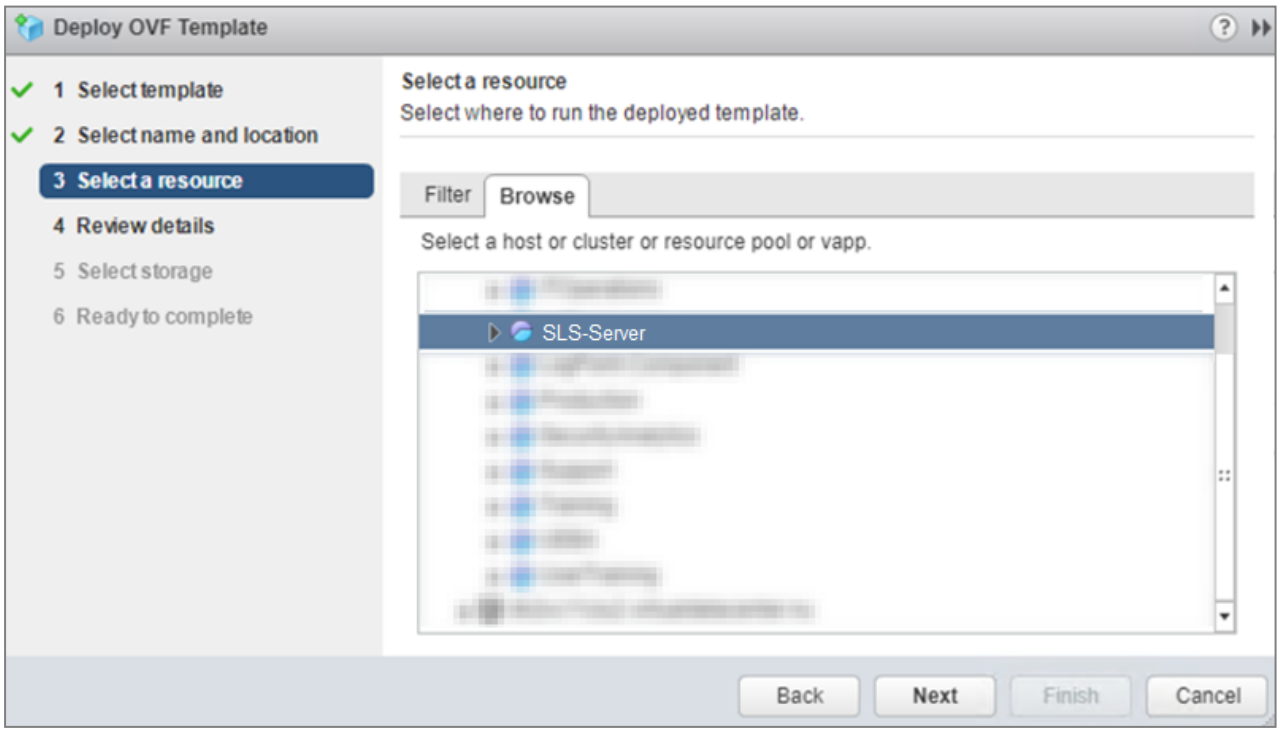
3.2 Selecting a Name and Folder

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



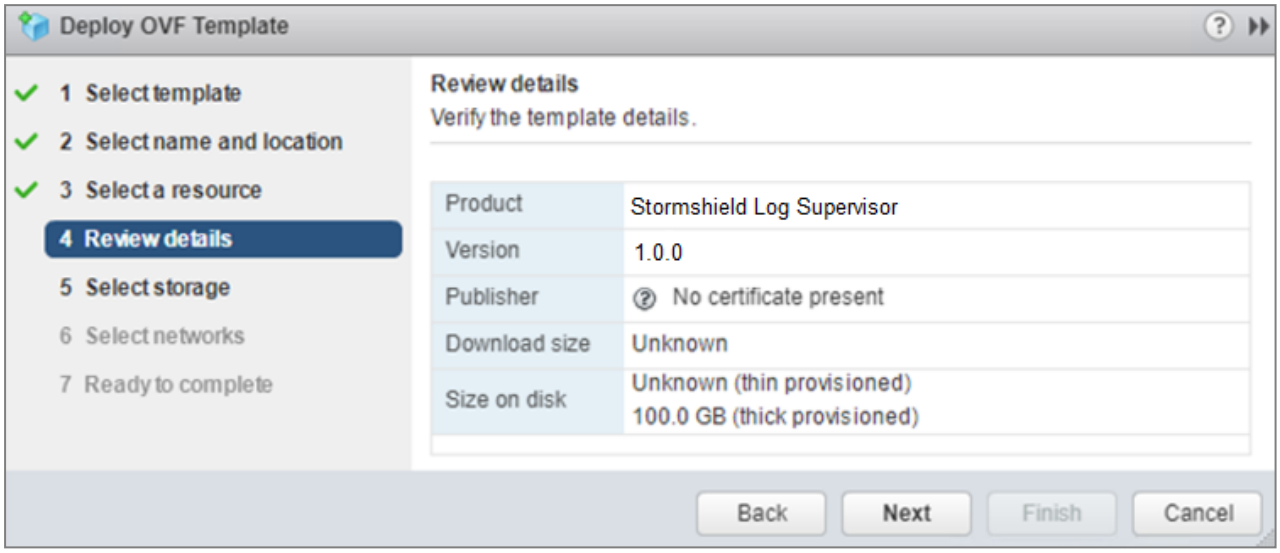
3.3 Selecting a Computing Resource

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



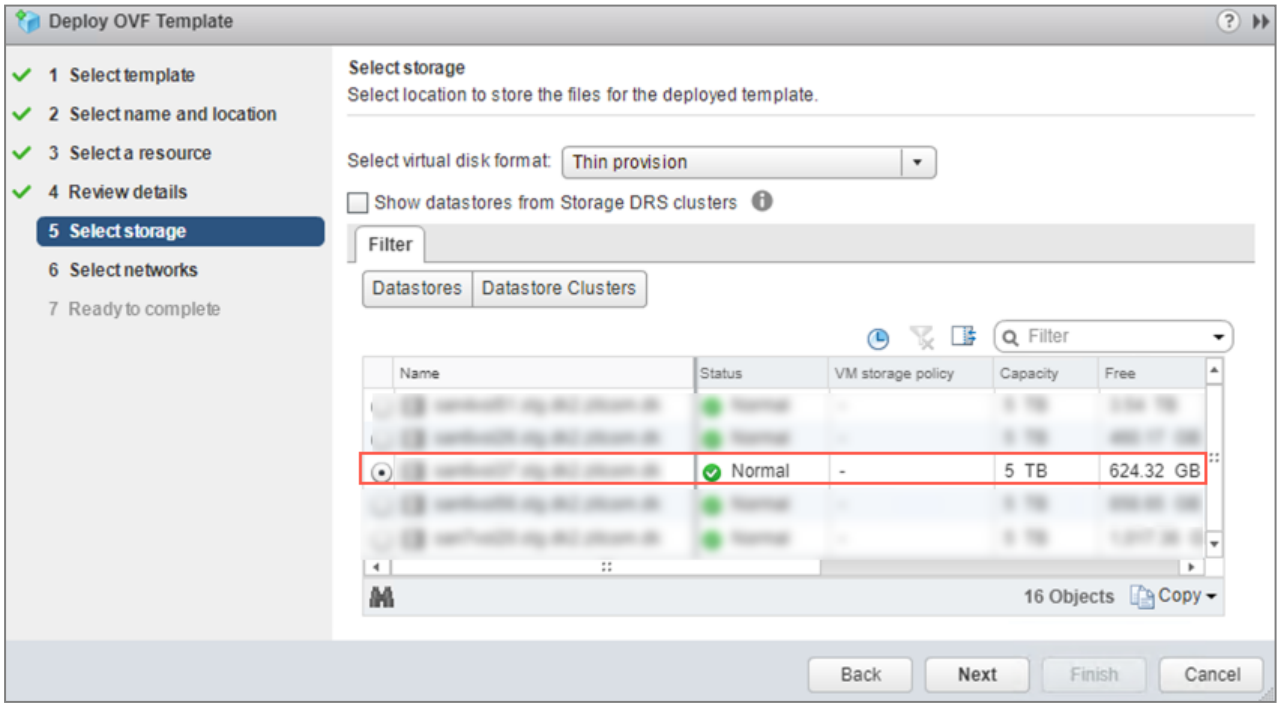
3.4 Reviewing the Template Details

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



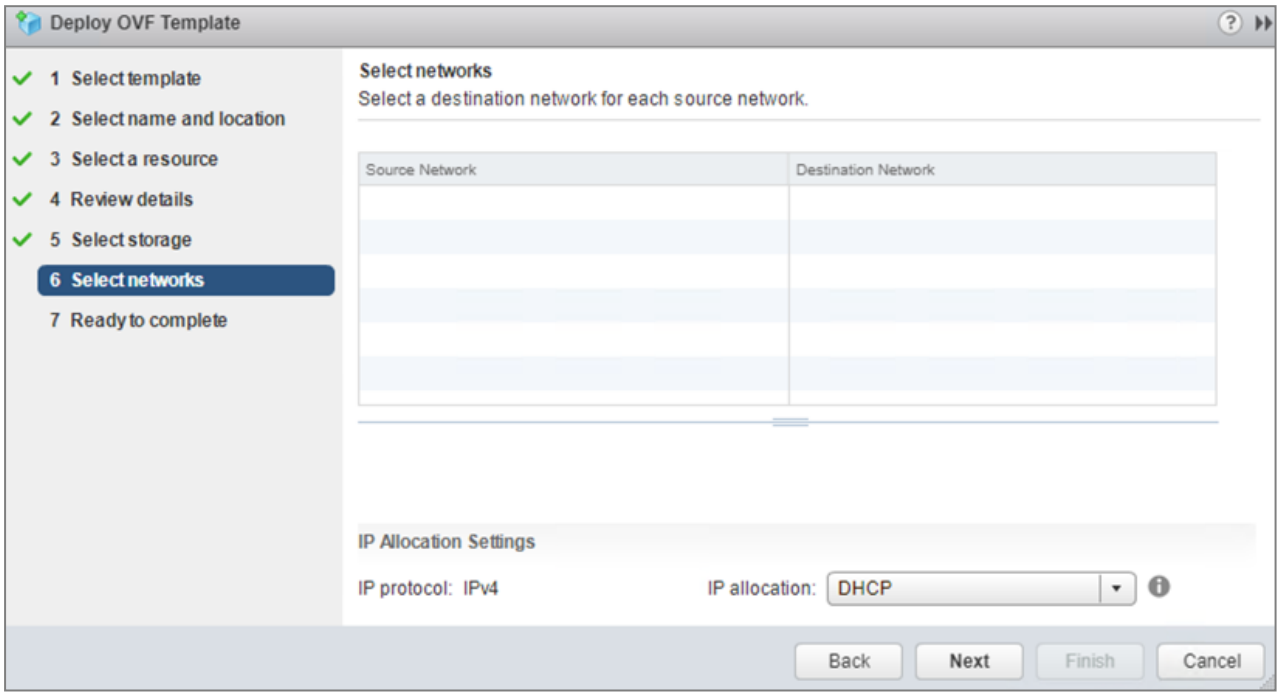
3.5 Selecting Storage

1. Select the **virtual disk format**:
   - **Eager Zeroed Thick Provision**: Select to allocate the storage and clear all the data inside the disk array immediately.
   - **Lazy Zeroed Thick Provision**: Select to allocate the storage immediately and clear all the data of the disk array only on demand.
   - **Thin Provision**: Select 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**.



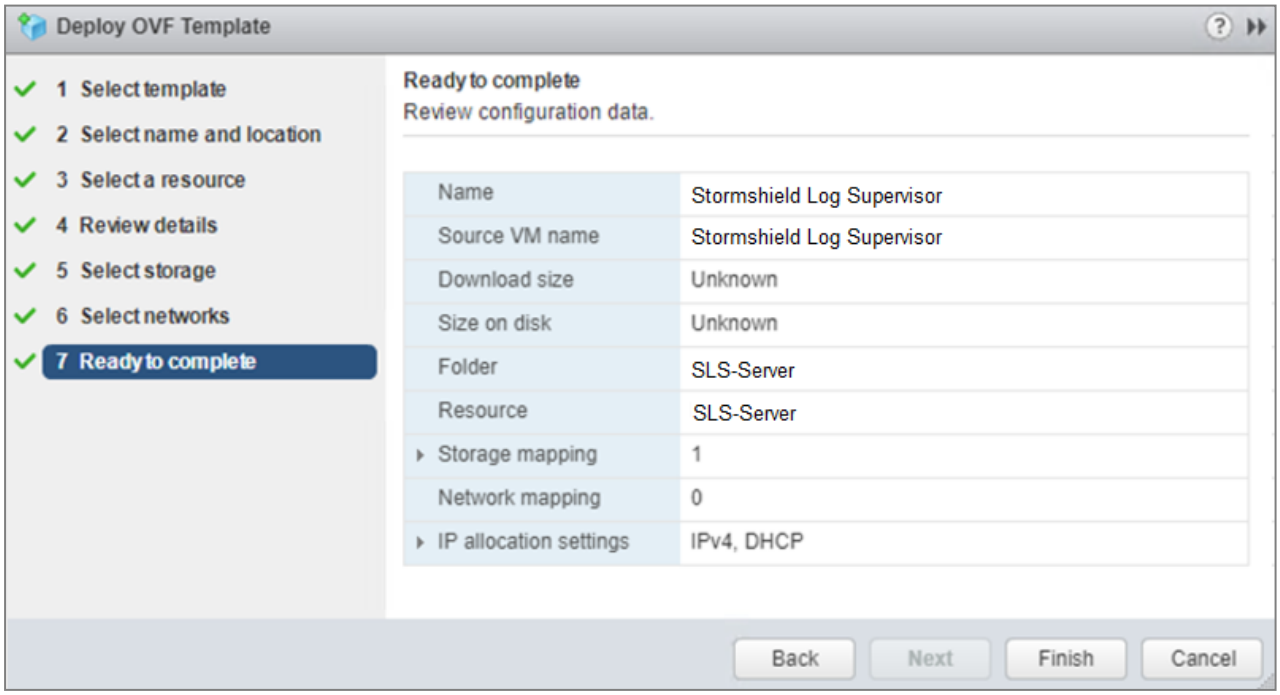
3.6 Selecting Networks

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 4.1 Accessing the SLS user interface.



3.7 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.



4. Activating SLS

4.1 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).

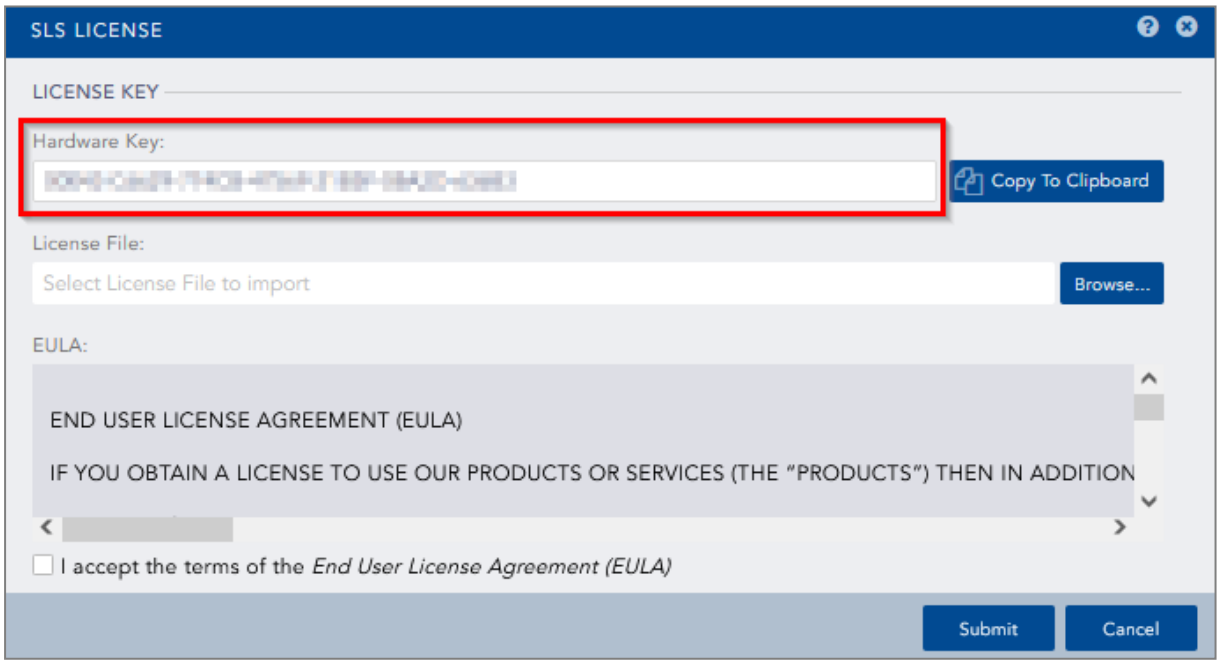
If you need to get or set the IP address of the SLS instance:

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.

4.2 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:



4.3 Registering the SLS product

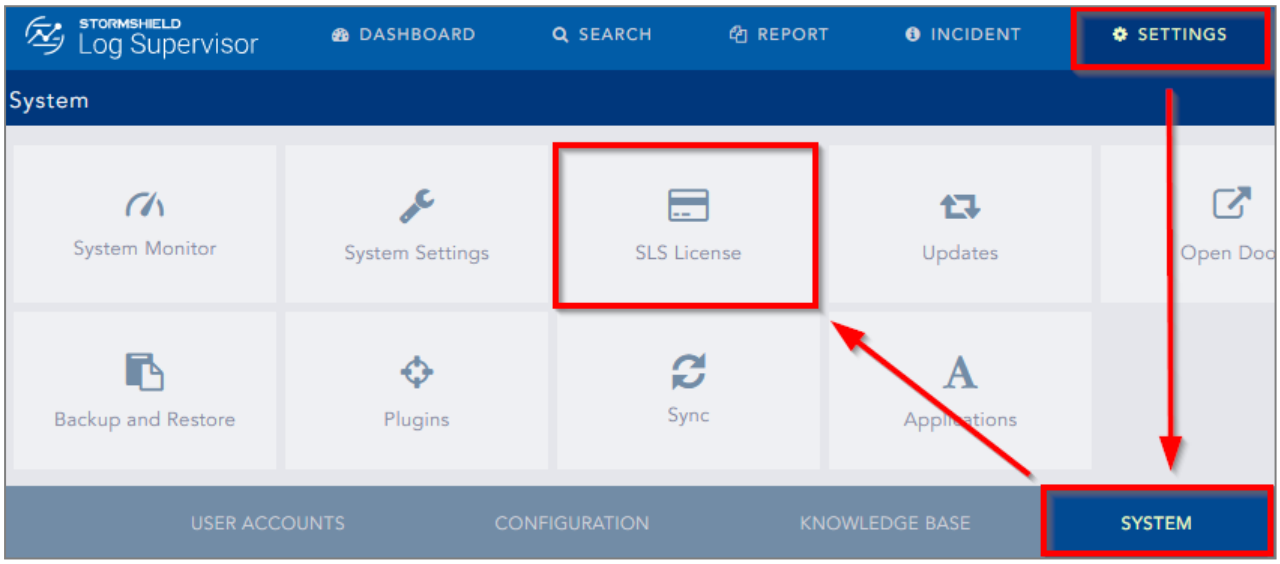
You must contact your Stormshield reseller or partner to obtain an SLS product. Then, register it in your MyStormshield personal area. You will be prompted to enter your SLS Hardware Key and SLS Serial Number. For more information, refer to the Registering products guide.

4.4 Downloading the SLS license (*.pak* file)

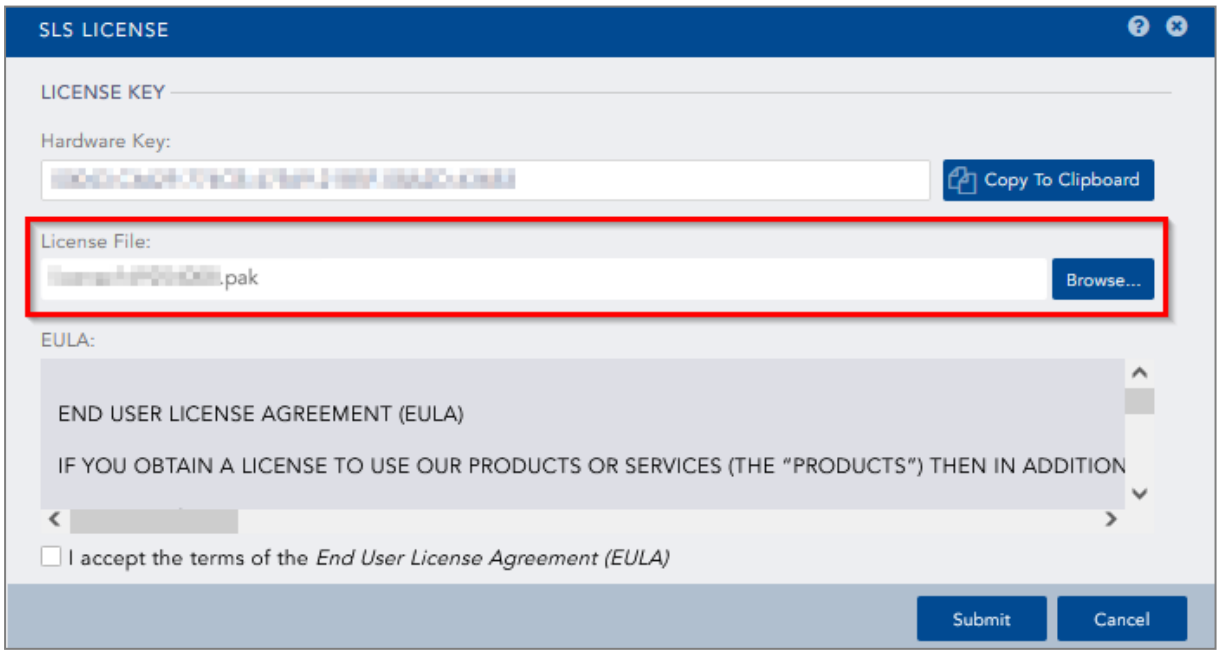
Download the license (*.pak* file) from your MyStormshield personal area. For more information, refer to the Downloading a product's license file page.

4.5 Installing the license

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



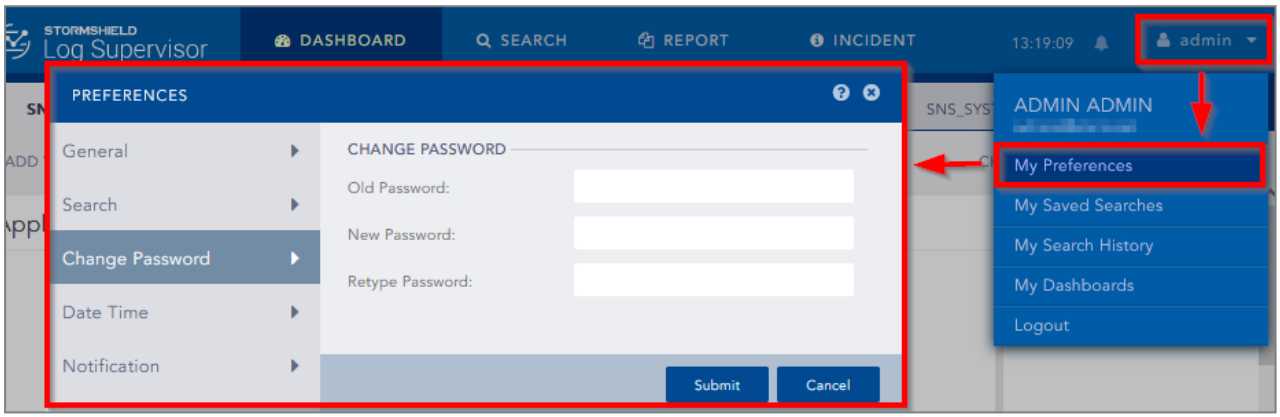
2. Click **Add License**.
3. Browse the file containing the **License Key**.
4. Go through the **END USER LICENSE AGREEMENT** (EULA). Mark the checkbox if you agree with the terms and conditions of the EULA.
5. Click **Submit**.



4.6 Changing the "admin" user password

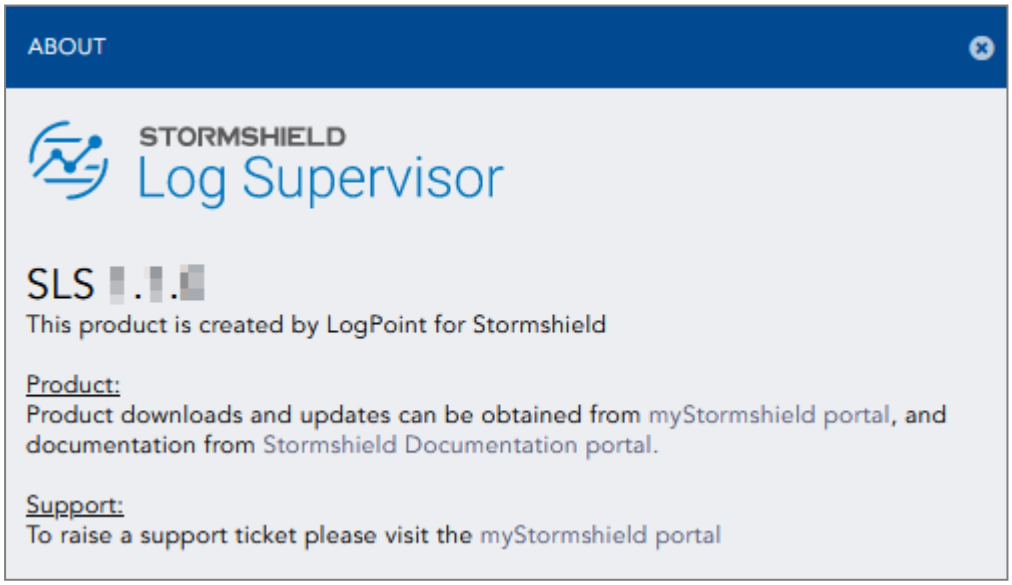
For security reasons, you must change the default password of the “admin” user.

1. Go to *User >> My Preferences* in the upper banner and click **Change Password**.
2. Enter *changeme* in the **Old Password** field.
3. Enter the new password and confirm it.
4. Click **Submit**.



4.7 Updating SLS to the latest patch

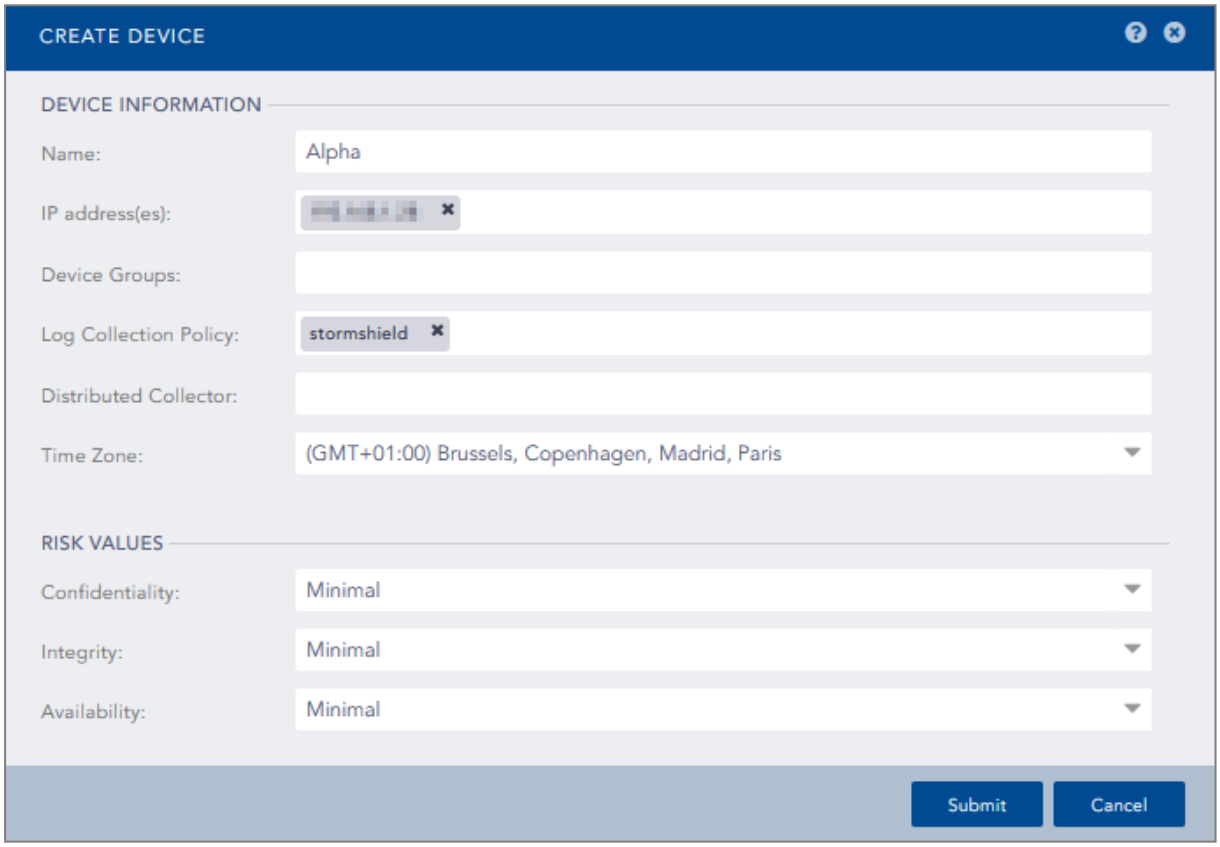
1. Identify the current SLS version installed. On the SLS user inteface, click on the Stormshield Log Supervisor logo in the upper banner and locate the version number.
2. Check the version release notes to see if a newer SLS version is available, what it contains, and how to install it.



5. Getting the logs from an SNS firewall

5.1 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**.



5.2 Configuring logs retrieval

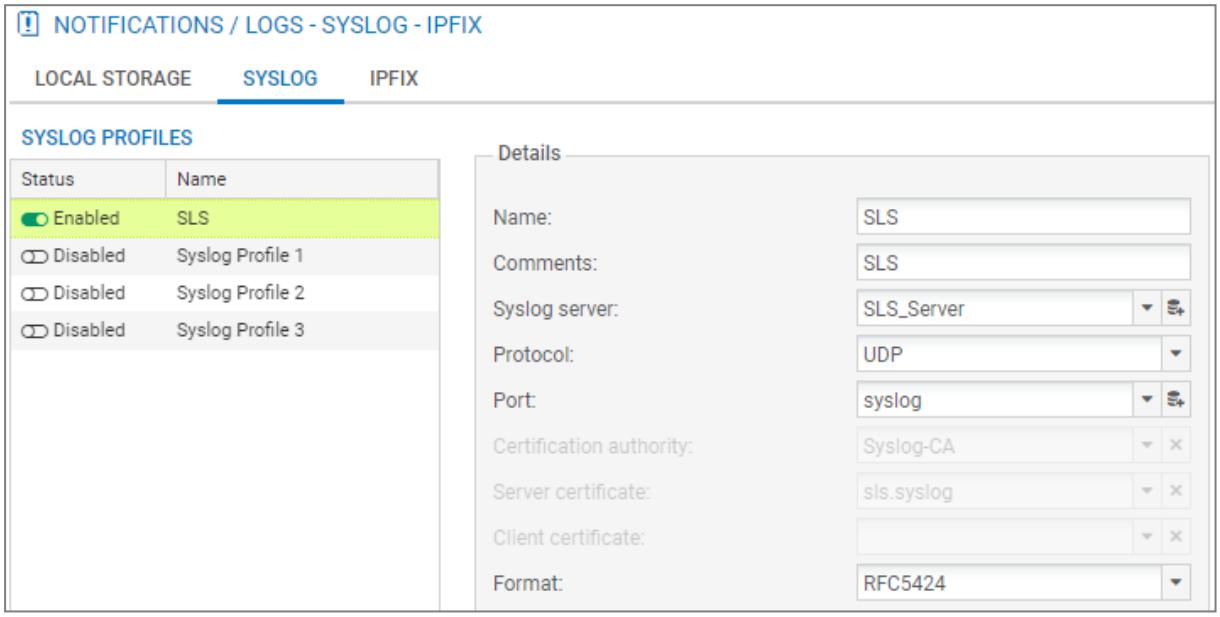
You can choose to either get the logs from the SNS firewall through standard Syslog or more securely through Syslog-TLS.

5.2.1 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).

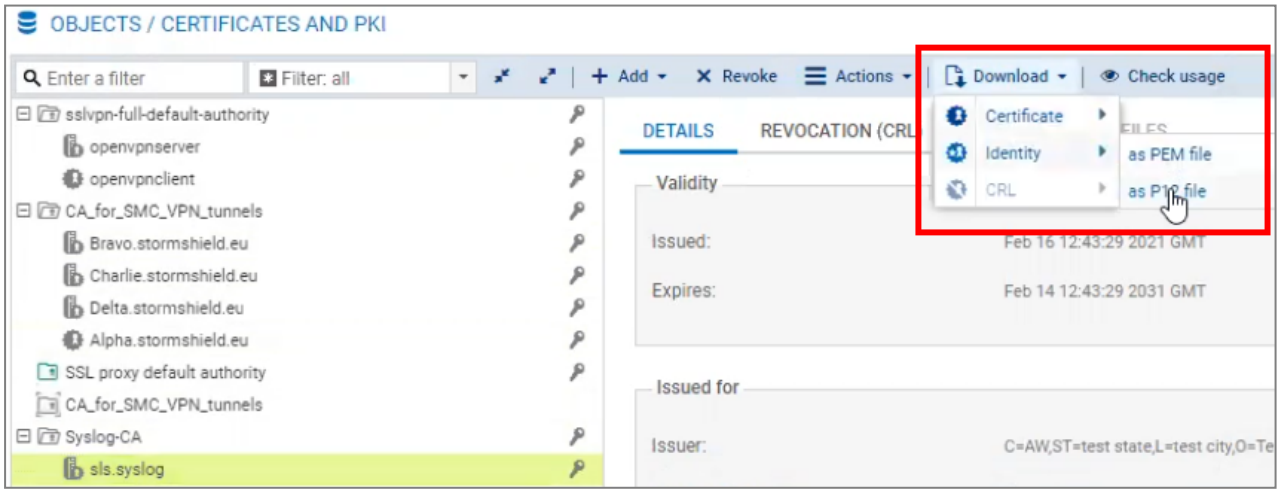
4. Select the port number. The default listening port is *514*. You can retrieve the Syslog listening port by using the "`change-syslog-port`" command on a VM console. Note that using this command toggles the port between *514* and *601*. Use it again if necessary.
5. Select the format.
6. **Apply** the configuration.



5.2.2 Getting the logs through Syslog-TLS

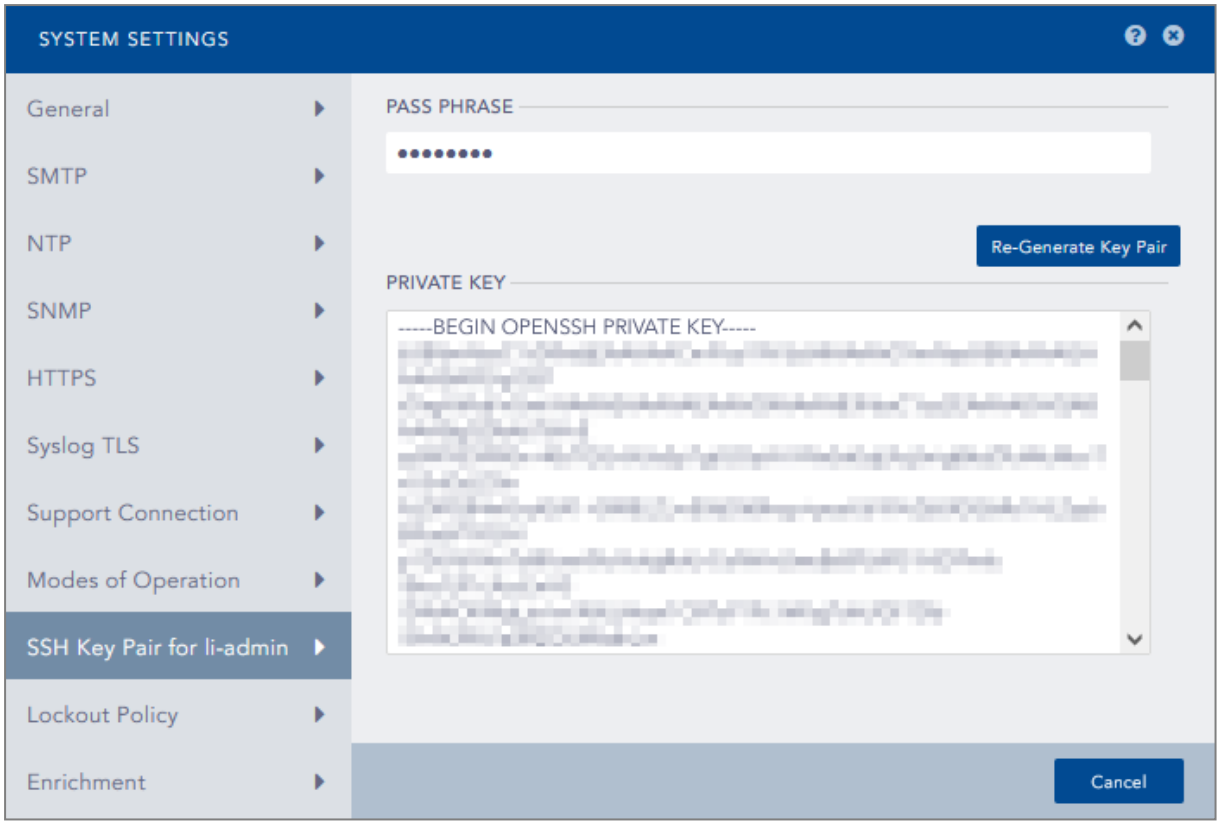
Downloading SNS Certificate Identity

1. On SNS, go to **Configuration > Objects > Certificates and PKI**.
2. Download the Server Certificate identity as a P12 file.



Establishing an SSH Connection with SLS

1. On SLS, go to *Settings >> System >> System Settings >> SSH Key Pair for li-admin*.
2. Provide a **Pass Phrase**.
3. Click **Re-Generate Key Pair**.
4. Copy the **Private Key** and save it in a file as a *.pem* file (e.g., Key_SLS.pem).



Copying the SNS Certificate Identity on SLS

1. Open WinSCP.
2. Fill in the IP address of the SLS instance.
3. Go to **Advanced Settings >> SSH >> Authentication**.
4. Select the *.pem* file and fill in the passphrase.
5. Copy the P12 file on SLS.

Importing the SNS Certificate Identity on SLS

1. Open PuTTY.
2. Fill in the SLS server IP address.
3. Go to **Advanced Settings >> Connection >> SSH >> Auth**.
4. Select the SLS key file.
5. Log in. The default credentials are *li-admin* (username) and *changeme* (password).
6. Use the command "`syslog_tls_cert --pkcs12=<p12 file>`" to import the P12 certificate for the Syslog-TLS connection.
7. Confirm.

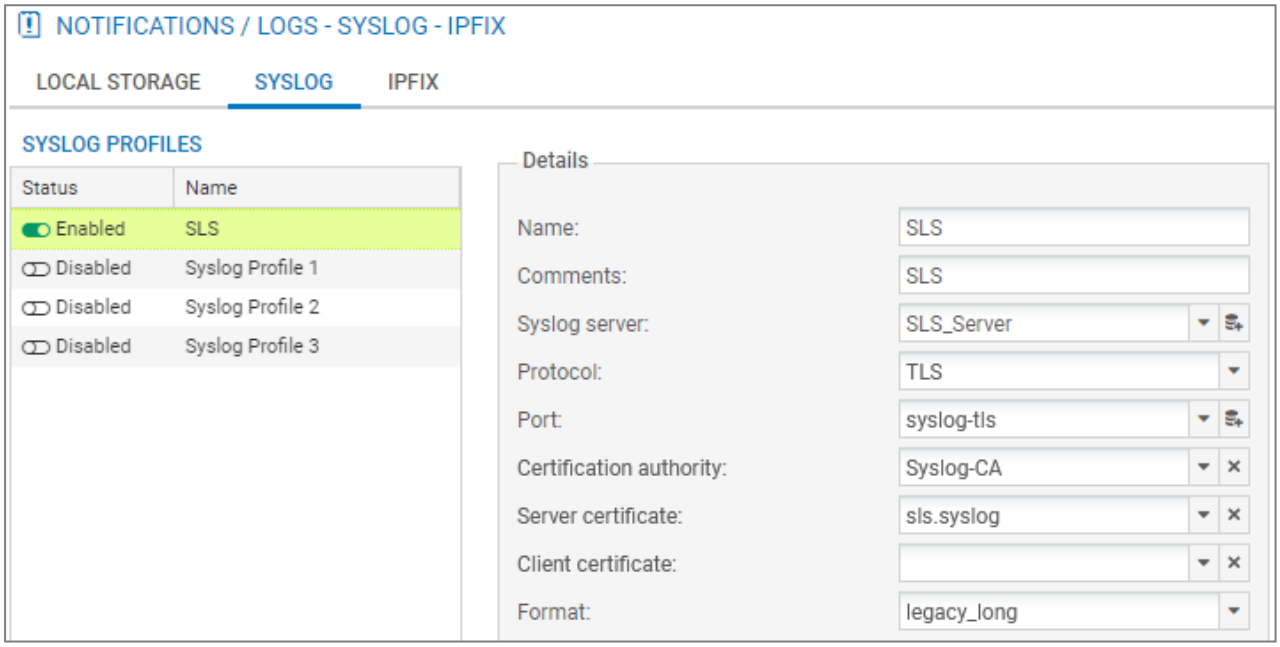
```
li-admin@Stormshield:~$ syslog_tls_cert
This command installs a custom certificate for tls syslog service.

Command format:
  syslog_tls_cert --pkcs12=<p12 file>                  : install from a PKCS12 f
ile
  syslog_tls_cert --pem=<cert file> --pkey=<pkey file> : install from PEM files

li-admin@Stormshield:~$ syslog_tls_cert --pkcs12=sls.syslog.p12
```

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.

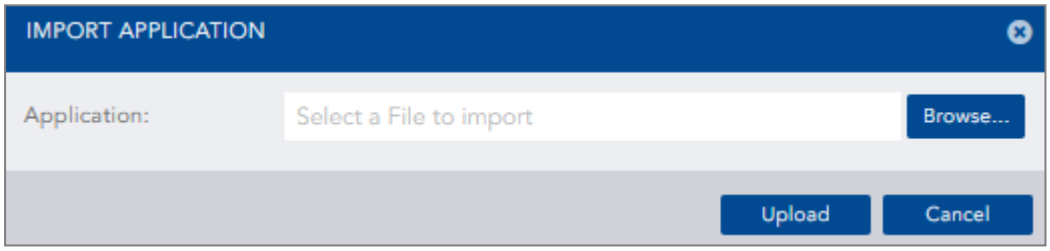


6. Getting the logs from SES Evolution

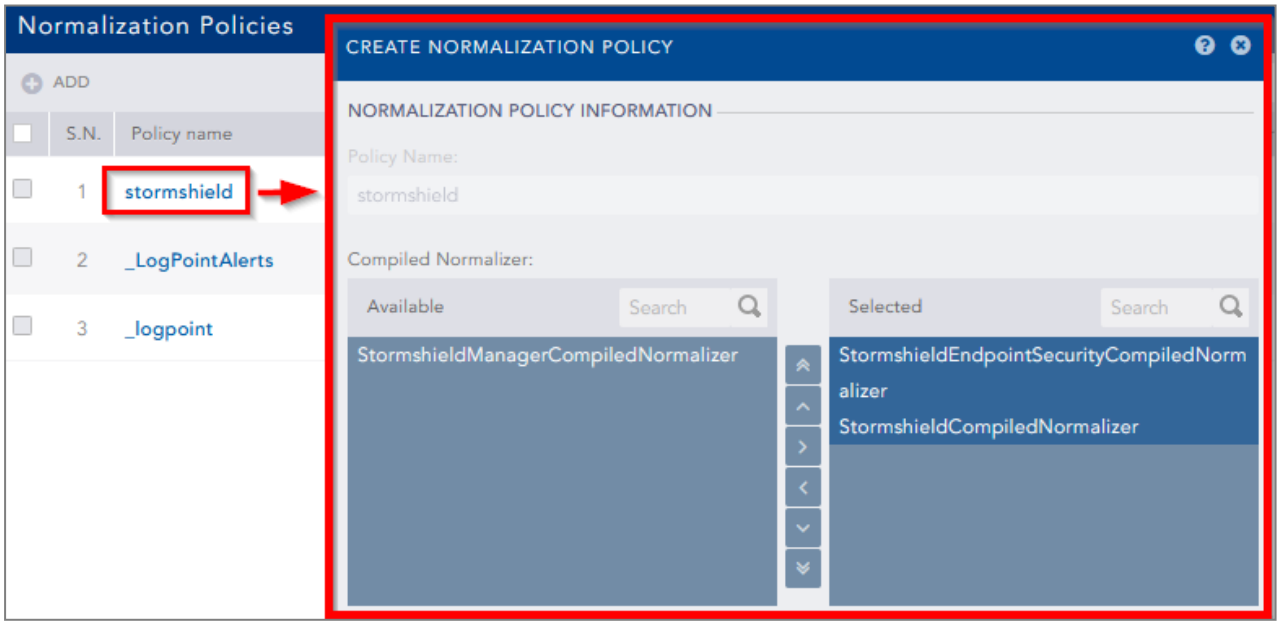
IMPORTANT
SLS must be in version 1.1.1 to get logs from SES Evolution. To determine the current SLS version and how to install 1.1.1 patch if necessary, see 4.7 Updating SLS to the latest patch.

6.1 Installing the new Stormshield application on SLS

1. Download the new application (*.pak* file) from your MyStormshield personal area, in **Downloads > Downloads > Stormshield Log Supervisor > Resources**.
2. On SLS, go to *Settings >> System >> Applications* and click **Import**.
3. Browse to the *.pak* file and click **Upload**.



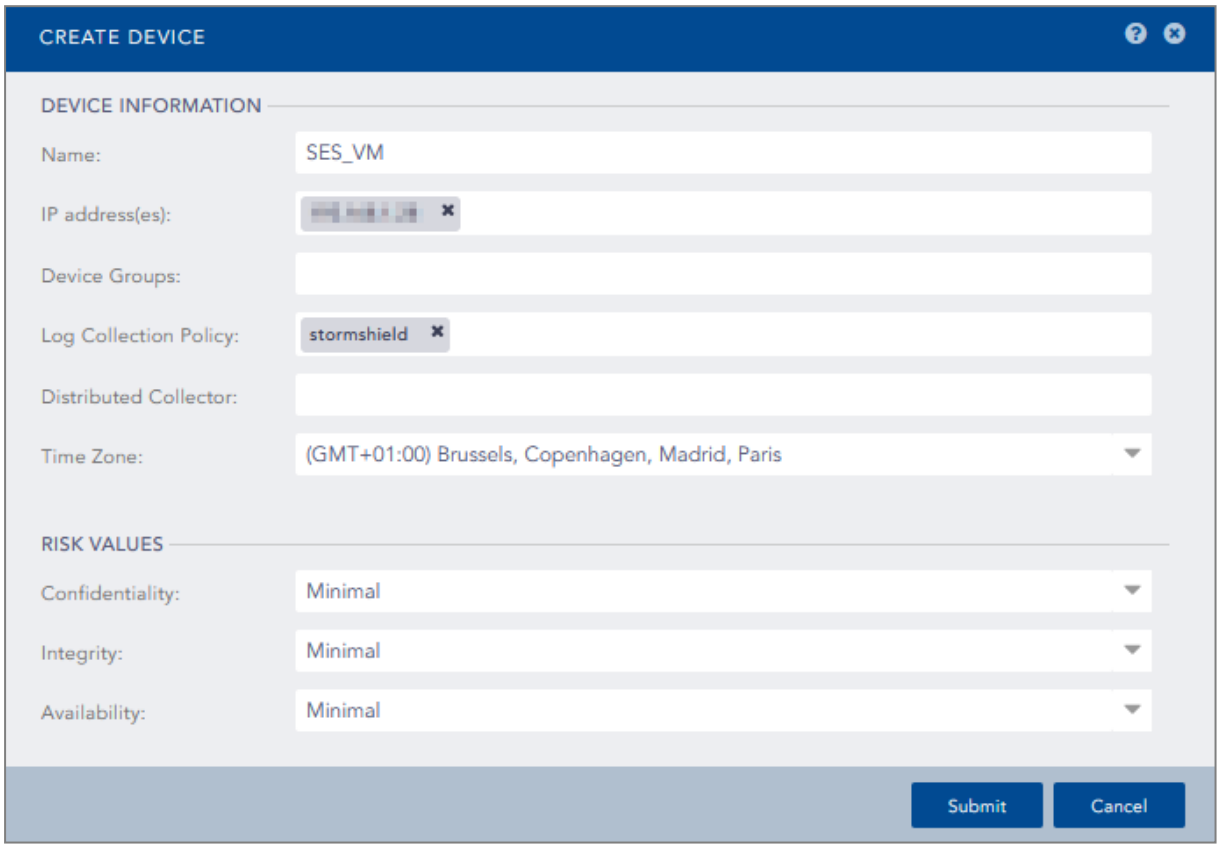
4. Go to *Settings >> Configuration >> Normalization Policies*.
5. Click on the *stormshield* policy name.
6. Select **StormshieldEndpointSecurityCompiledNormalizer**.
7. Click **Submit**.



6.2 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 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**.



6.3 Configuring logs retrieval

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

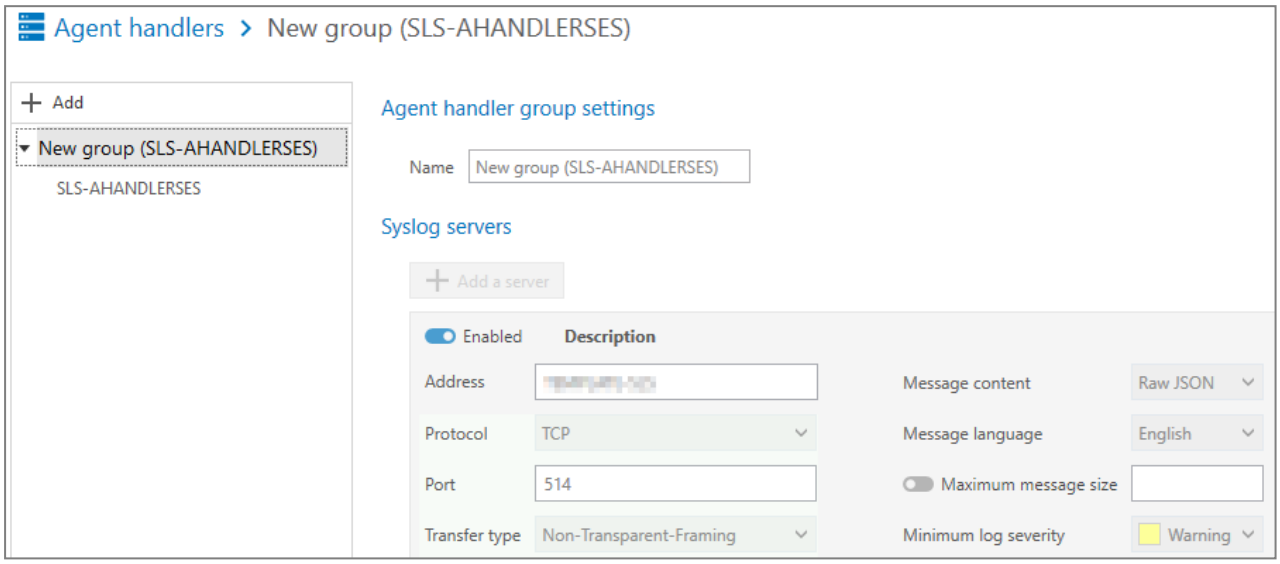
6.3.1 Getting the logs through standard Syslog

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.

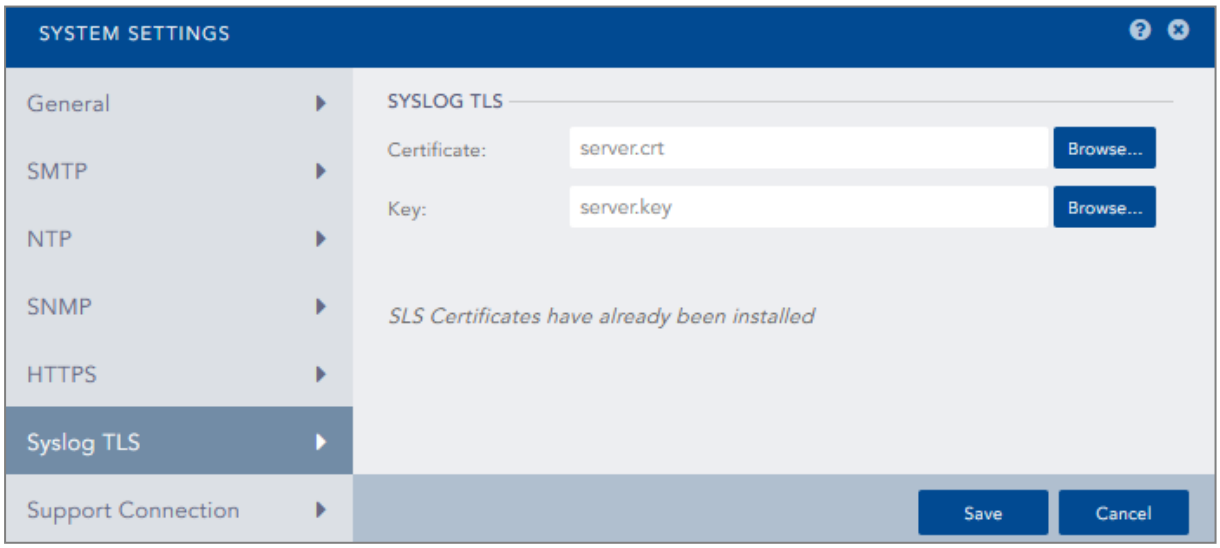
Continue to 6.4 Configuring SES dashboards on SLS.



6.3.2 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 >> System Settings >> Syslog TLS*.
3. Provide the certificate (*.crt* file) and the private key (*.key* file).
4. Click **Save**.

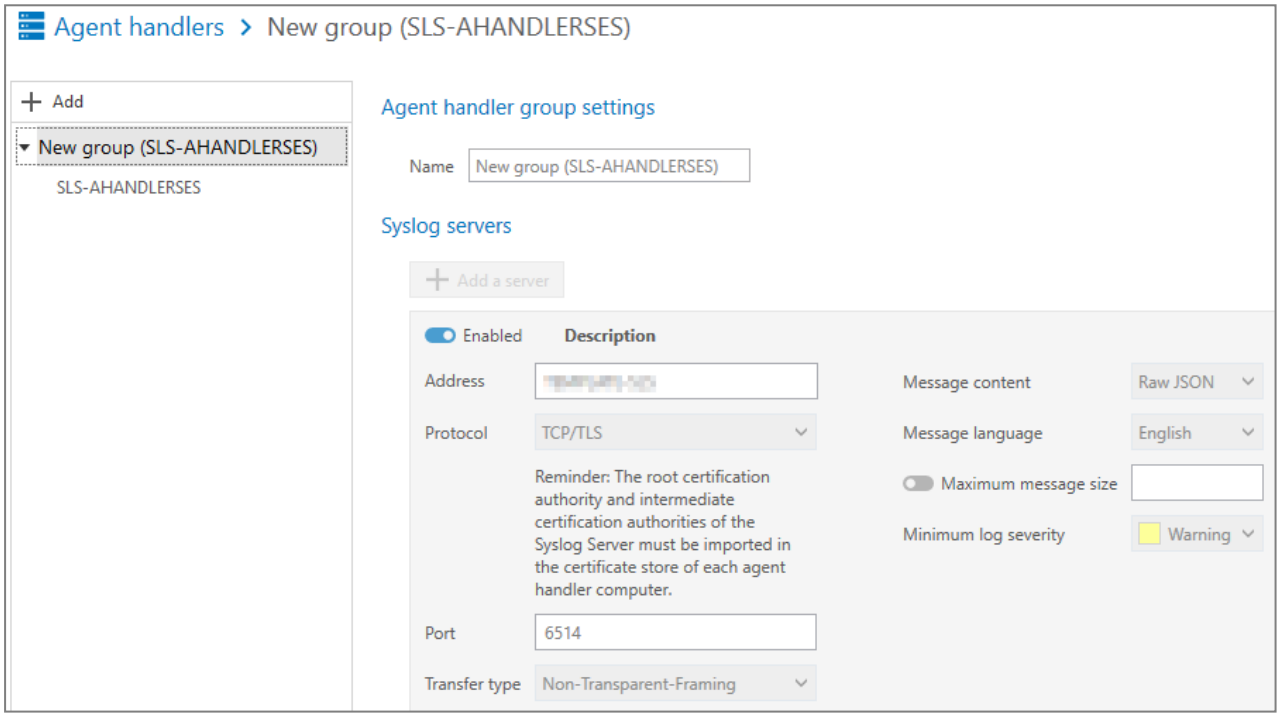


Importing the Root Certificate Authority

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.

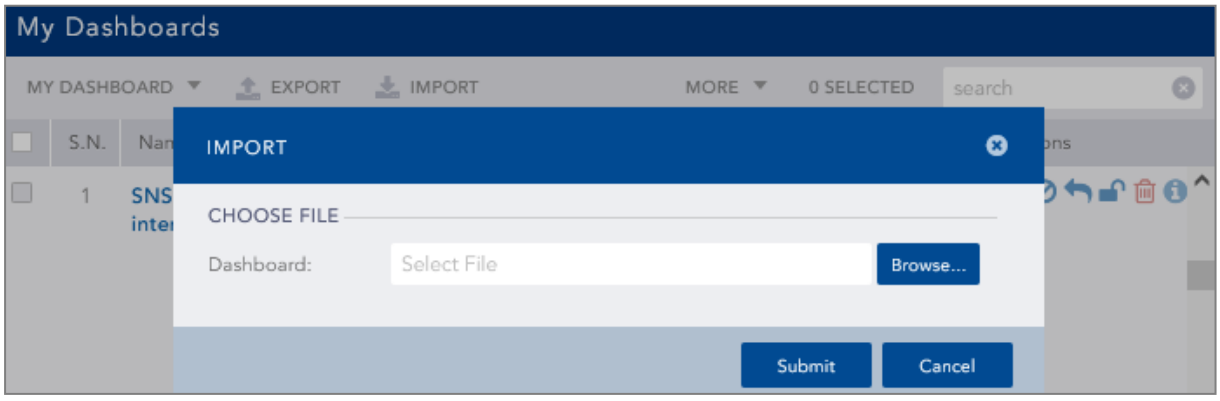
Configuring a TCP/TLS connection on the Agent handler

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.

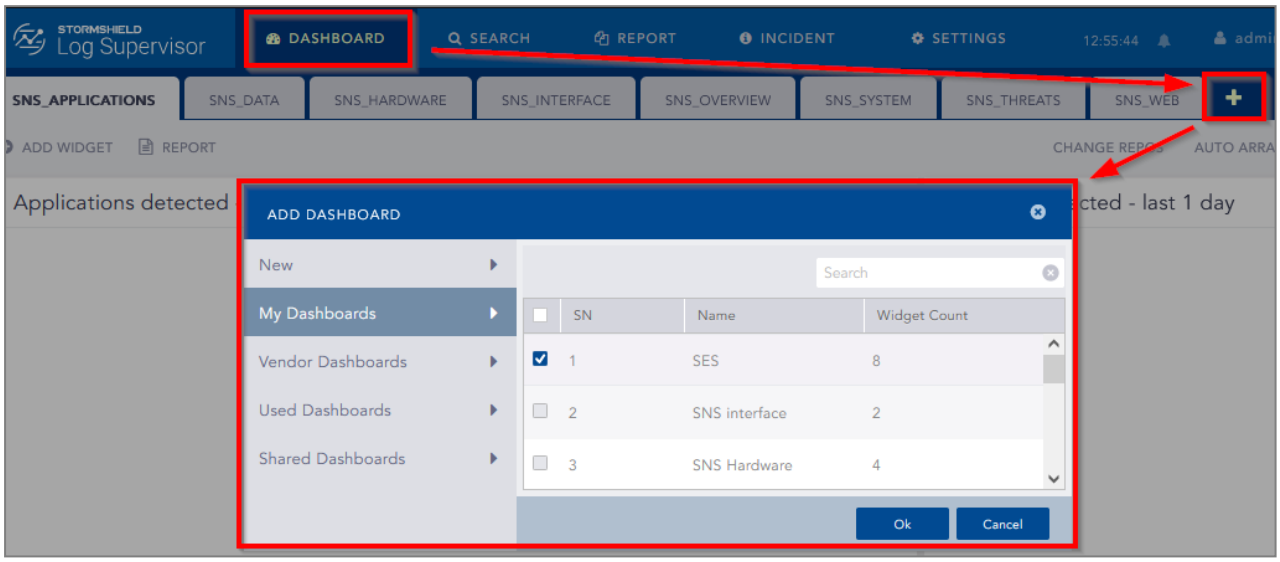


6.4 Configuring SES dashboards on SLS

1. Download the SES dashboards (*.pak* file) from your MyStormshield personal area, in **Downloads > Downloads > Stormshield Log Supervisor > Resources**.
2. On SLS, go to *Dashboard >> Quick Links >> My Dashboard* and click **Import**.
3. Browse to the *.pak* file and click **Submit**.



4. Go to *Dashboard* and click the + icon.
5. Click **My Dashboards**.
6. Select **SES**.
7. Click **Ok**.



7. 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