GUIDE

STORMSHIELD LOG SUPERVISOR

HYPER-V VHD DEPLOYMENT GUIDE

Version 2

Document last updated: July 4, 2024

Reference: sls-en-deployment_guide_hyperv

Table of contents

Change log

Date	Description
July 4, 2024	New document

Getting started

Welcome to the Stormshield Log Supervisor Hyper-V VHD version 2 Deployment Guide.

This guide discusses the steps and considerations for deploying the SLS Hyper-V VHD on the Microsoft Hyper-V Server.

With the SLS Hyper-V VHD, you can benefit from the following unique features of Microsoft Hyper-V Server:

- **Expandable private cloud environment** provides flexible, on-demand IT services allowing you to make adjustments on resources as per change in requirements.
- **Efficient hardware usage** consolidates the servers dividing the workloads equally and uses powerful physical computers decreasing the power consumption and physical space.
- **Improve business continuity** minimizes the impact of both scheduled and unscheduled downtime of your workloads.
- **Expandable virtual desktop infrastructure (VDI)** who uses a centralized desktop strategy to increase business agility and data security, as well as simplify regulatory compliance and manage applications.

For a better assessment of this guide, we expect you to have a basic understanding of the Microsoft Hyper-V Server and its 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.
- You can launch one SLS instance from one VHD. To launch multiple SLS instances, make the required number of copies from the original VHD, and launch SLS from each one of them.
- SLS records all the changes and configurations made in its VHD. Therefore, we recommend that you save the downloaded VHD in its original state and launch a SLS instance only on its copy.
- The Stormshield Log Supervisor Hyper-V VHD file is a dynamically expanding VHD file; the disk storage is allocated only on demand. For the fixed sized VHD file, the disk storage is allocated immediately during the VHD file creation. You can convert the VHD to a fixed sized VHD file by using the **Edit Disk utility** of the HyperV Manager application.

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.

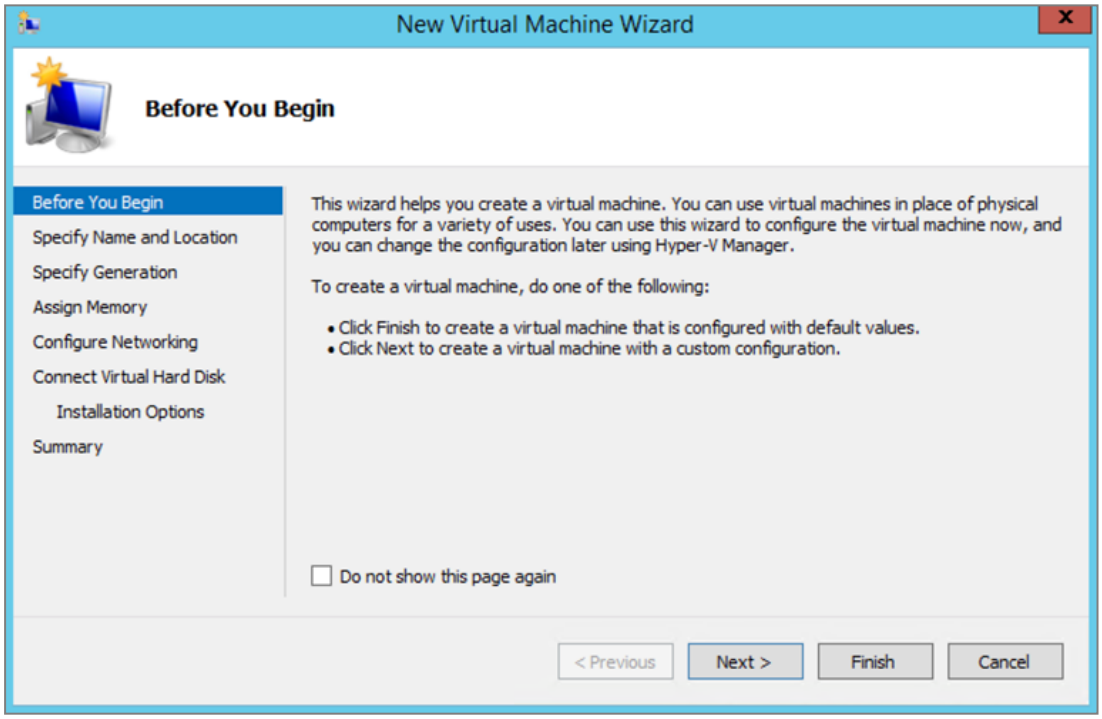
Deploying SLS Hyper-V VHD

You can deploy the SLS Hyper-V VHD using Hyper-V Manager from another Windows machine or using Windows PowerShell from the Hyper-V server itself.

Deploying SLS from another Windows machine using Hyper-V Manager

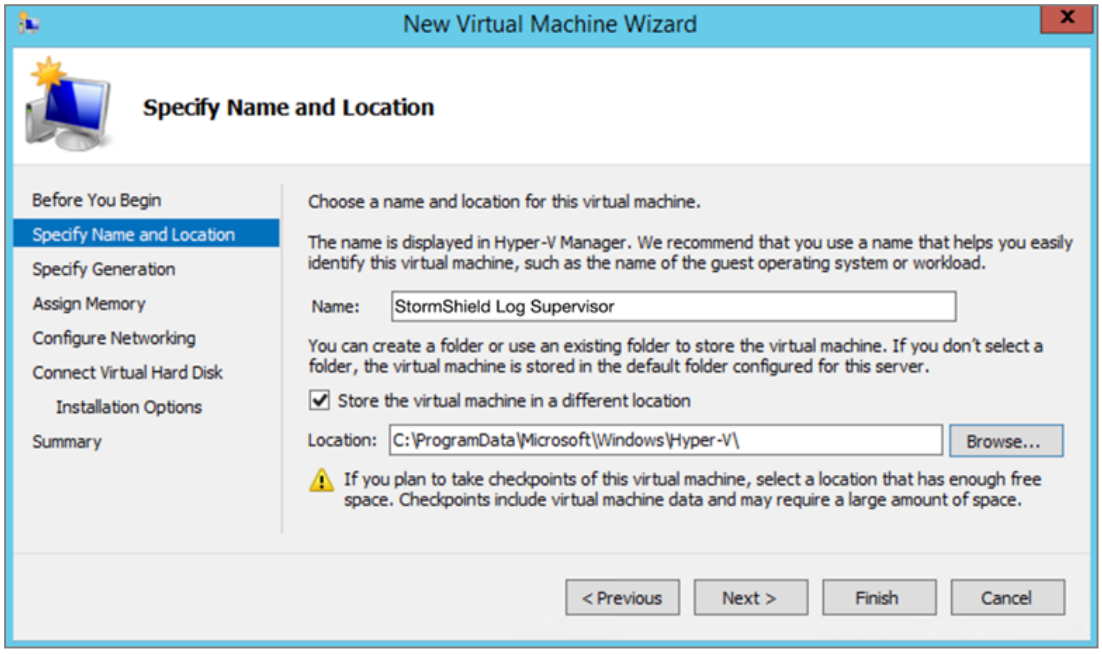
Selecting the Hyper-V Server

1. Download the provided SLS *.vhd* file from your MyStormshield personal area, in **Downloads > Downloads > Stormshield Log Supervisor > Firmware**.
2. Open the **Hyper-V Manager** console and select the Hyper-V server where you want to launch the SLS.
3. In the *Actions* tab of the console, click **New** and select **Virtual Machine**.
4. Read the details on the *Before You Begin* tab and click **Next**.



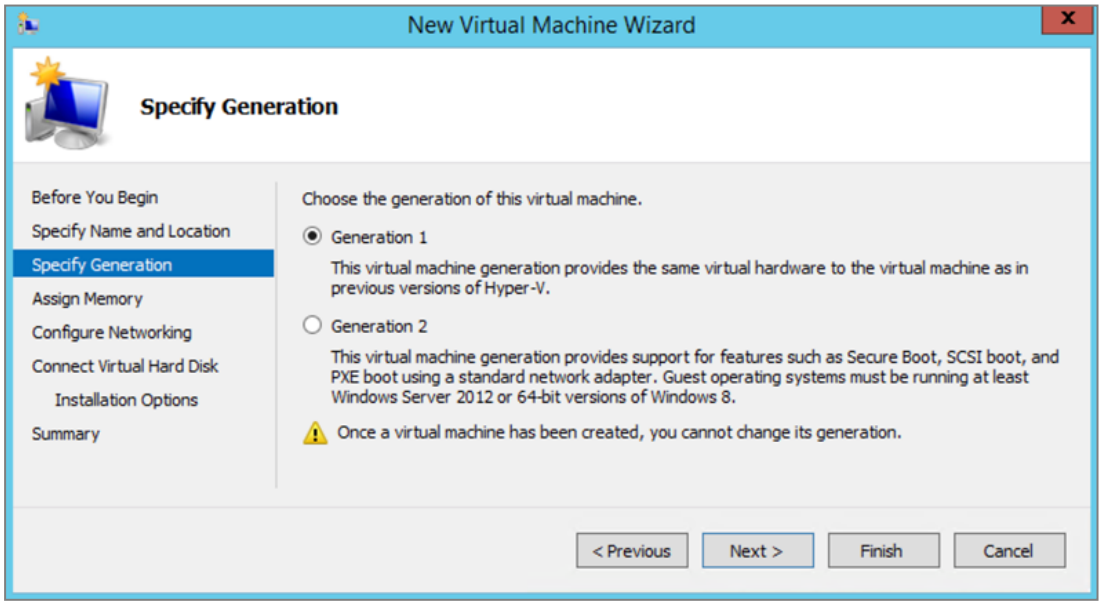
Specifying a Name and Location

1. Enter a **Name** for the virtual machine.
2. Select a **Location** to store the virtual machine and click **Next**.
   We recommend that you create a separate folder to store the SLS virtual machine. Make sure the folder has enough space to store the files of the SLS virtual machine.



Specifying the Generation

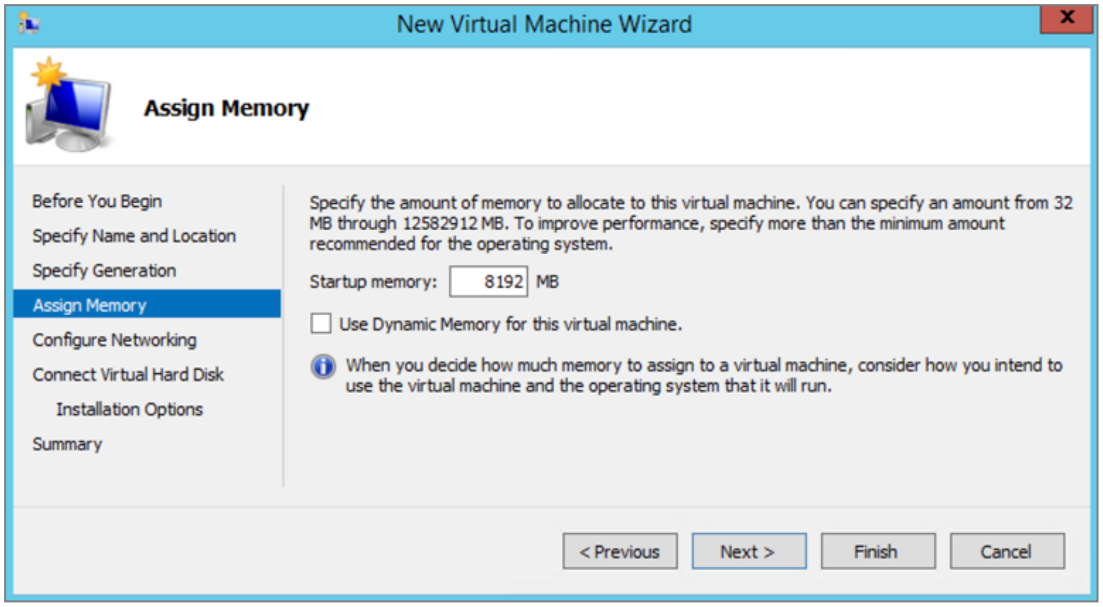
1. Choose **Generation 1** and click **Next**.



Assigning Memory

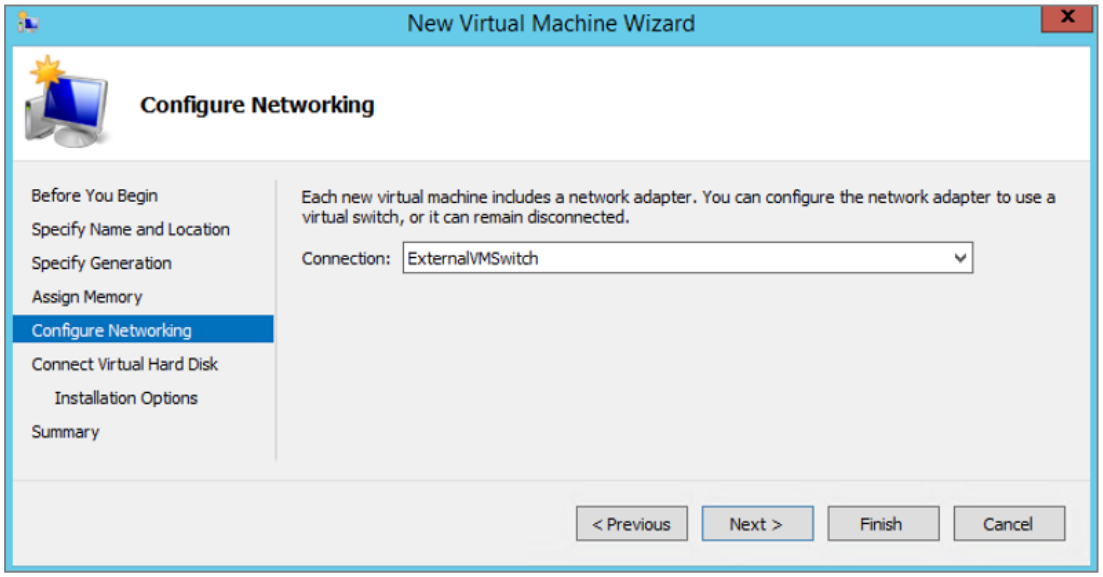
1. Specify the **Startup memory** for the virtual machine. For SLS, the minimum memory requirement is 7GB.

2. Enable **Dynamic Memory** to use on-demand memory allocation and click **Next**.



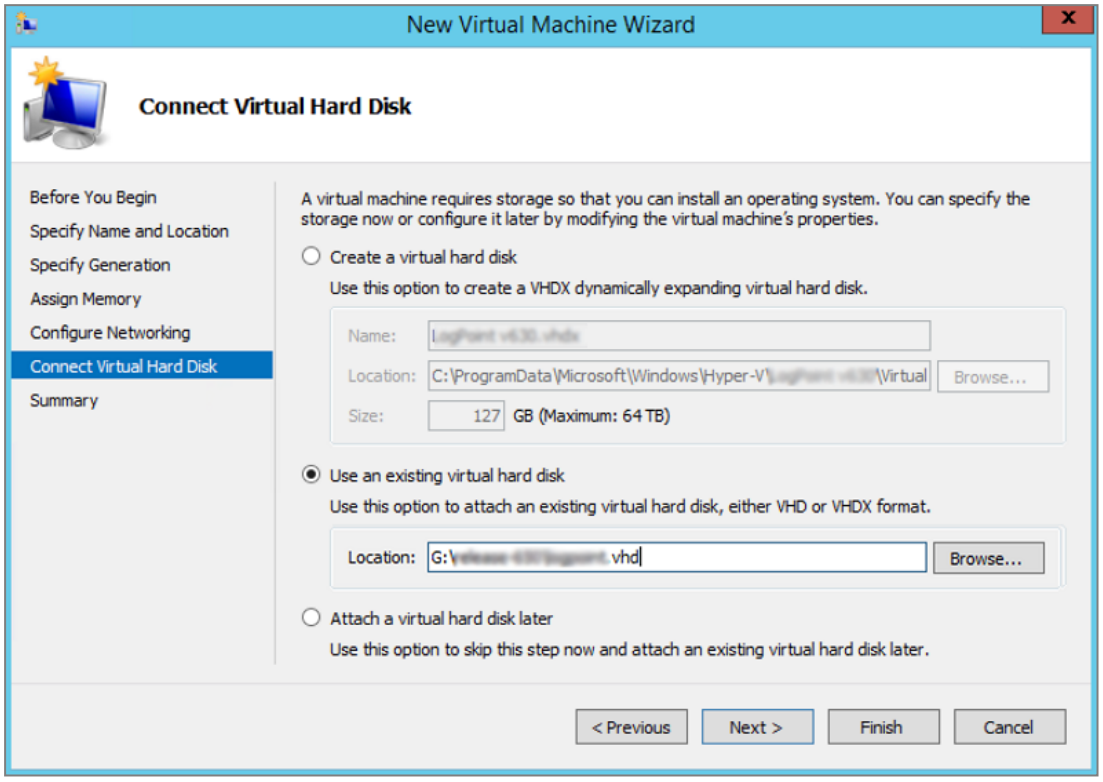
Configuring Networking Connection

1. Select the switch as per your networking requirement and click **Next**.
In the screenshot below, we have selected an already created ExternalVMSwitch. For more information about the Hyper-V virtual switches, refer to Microsoft's Create and configure a virtual switch with Hyper-V page.



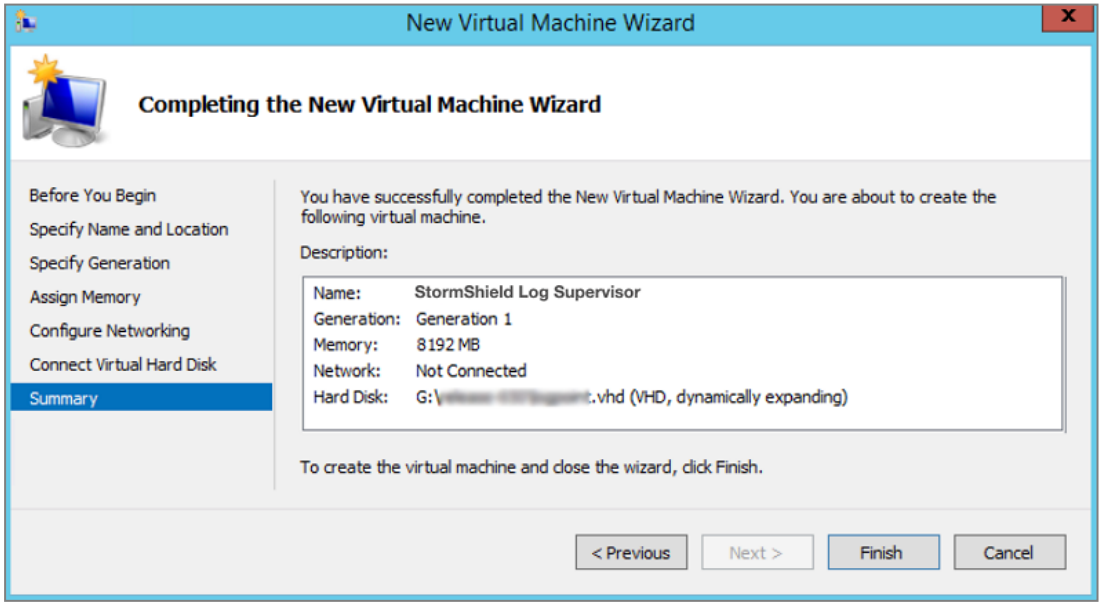
Connecting the Virtual Hard Disk

1. Select **Use an existing virtual hard disk**, browse to the *.vhd* file, then click **Next**.



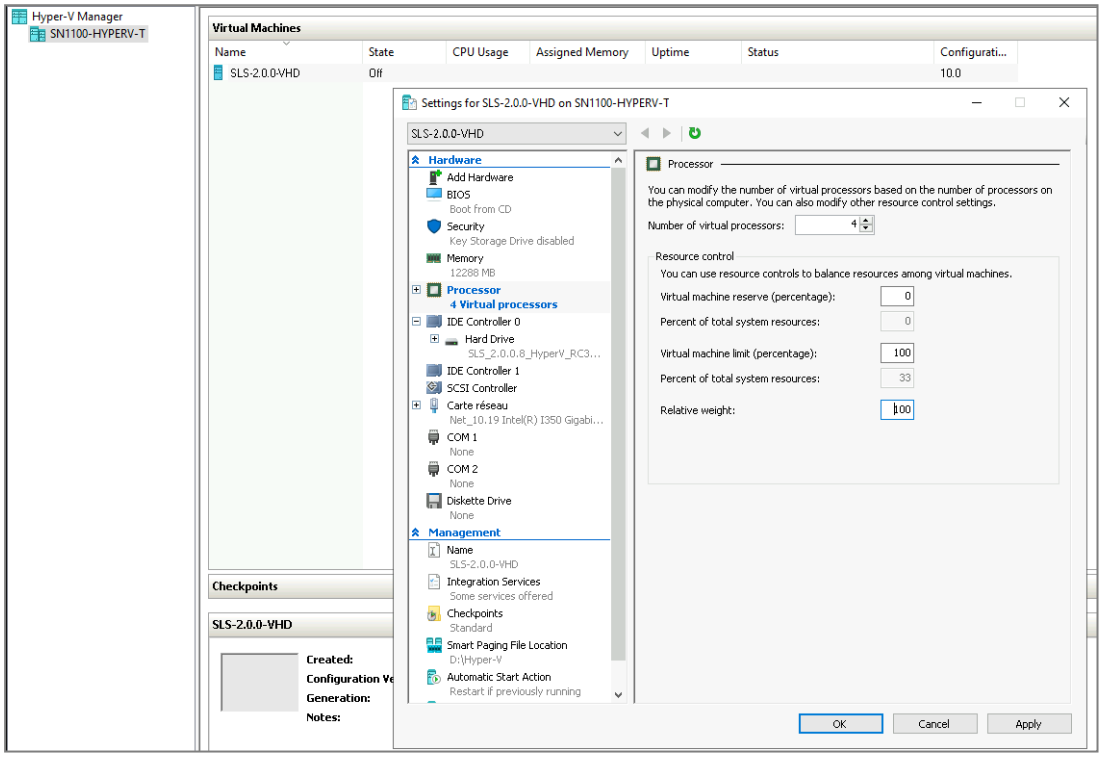
Completing the New Virtual Machine Wizard

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



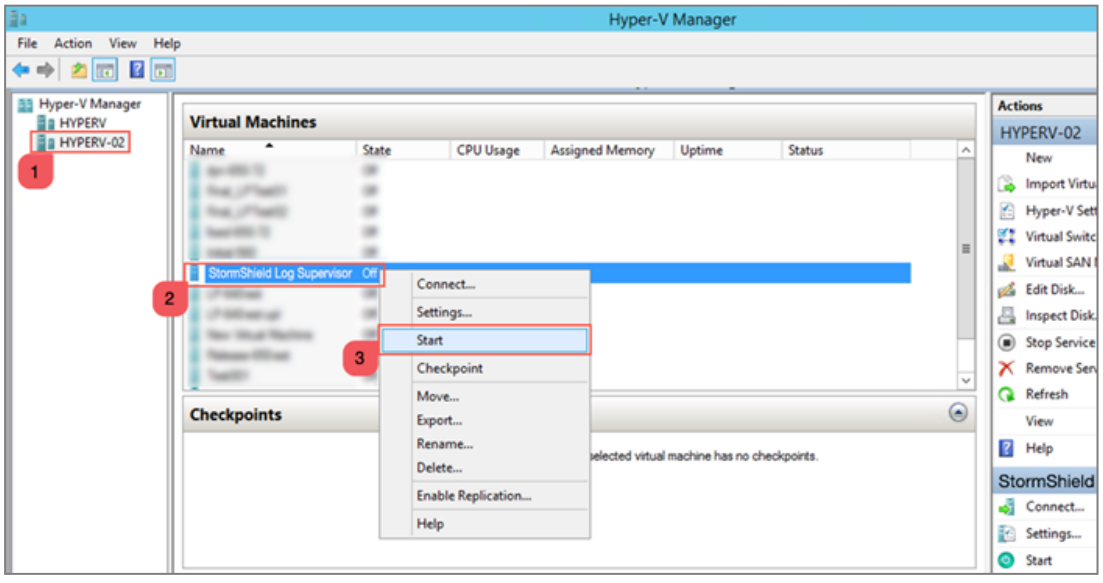
Assigning Processors

1. In the *Hyper-V Manager* application, select the required **Hyper-V server**.
2. Select the required **Virtual Machine**, right-click on it, then click **Settings...**.
3. Select **Processor** and specify the **Number of virtual processors** for the virtual machine. For SLS, the minimum requirement is a *Quad-core* processor.
4. Click **Apply**.



Starting the Virtual Machine

1. In the *Hyper-V Manager* application, select the required **Hyper-V Server**.
2. Select the required **Virtual Machine**, right-click on it, then click **Start**.



Deploying SLS from the Hyper-V server itself using Windows PowerShell

Download the provided SLS *.vhd* file from your MyStormshield personal area, in **Downloads > Downloads > Stormshield Log Supervisor > Firmware**.

On the Hyper-V server, open **Windows PowerShell** as an administrator and run the command:

```
New-VM -Name <VM_Name> -MemoryStartupBytes 7GB -BootDevice VHD -
VHDPath"<the_StormshieldLogSupervisor_VHD_path>" -Path <"<destination_
path_for_the_VM>"> -Generation 1 -Switch <virtual_switch_name>
```

Then run the following commands:

```
Set-VM -Name <VM_Name> -ProcessorCount 4
```

```
Start-VM -Name <VM_Name>
```

Activating SLS

Accessing the SLS user interface

1. In the *Hyper-V Manager* application, select the required **Hyper-V Server**, select the required **Virtual Machine**, then click **Connect** on the *Actions* tab.
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).

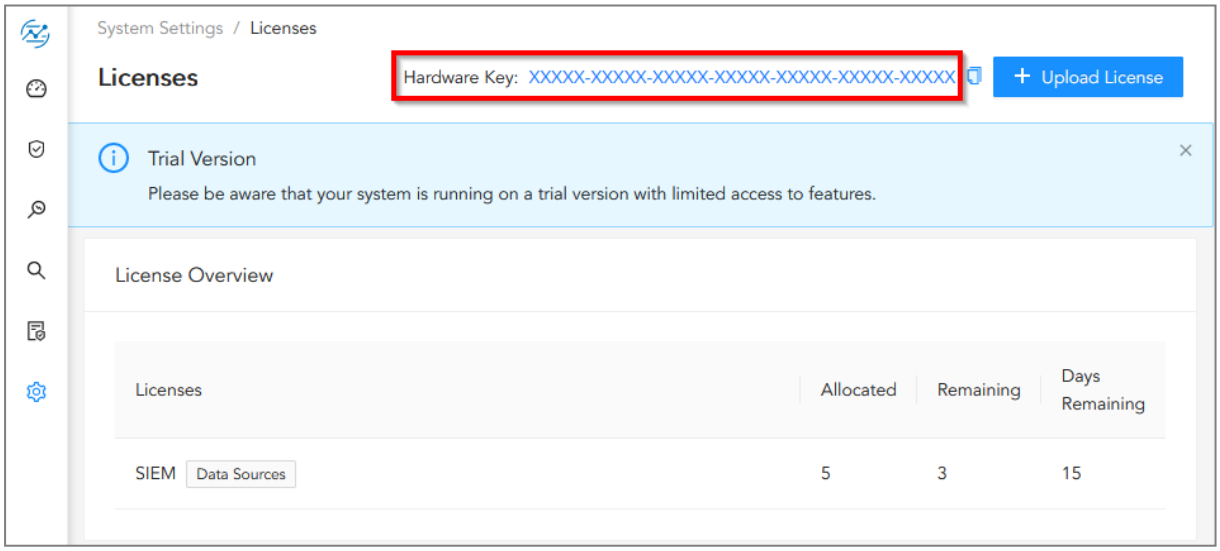
If you need to get or set the IP address of the SLS instance:

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

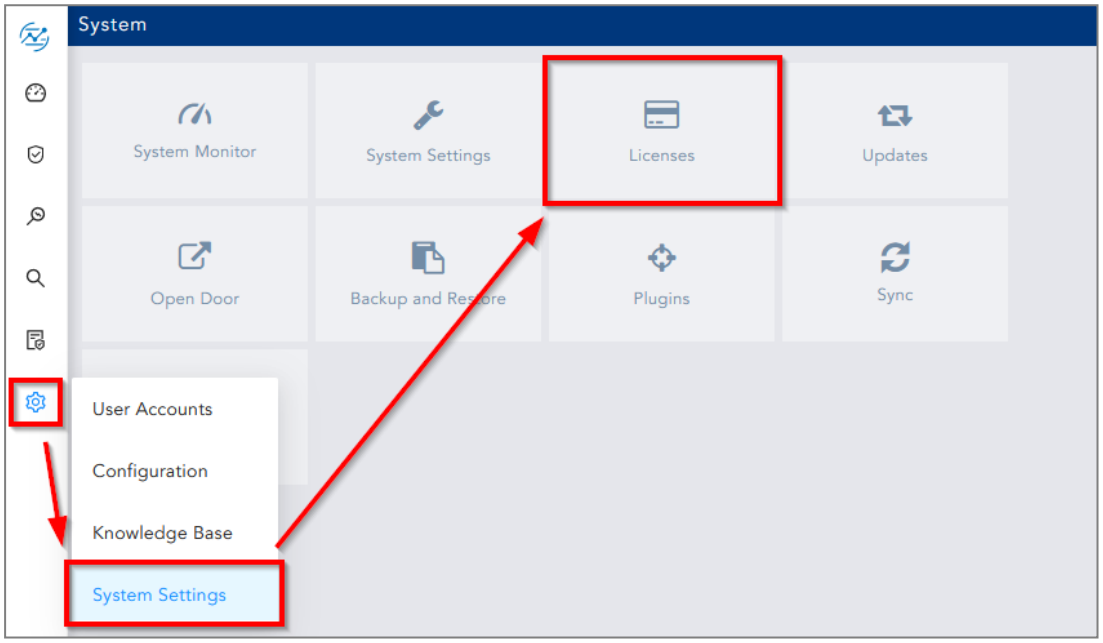
You must contact your Stormshield reseller or partner to obtain an SLS product. Then, register it in your MyStormshield personal area. You will be prompted to enter your SLS Hardware Key and SLS Serial Number. For more information, refer to the Registering products guide.

Downloading the SLS license (*.pak* file)

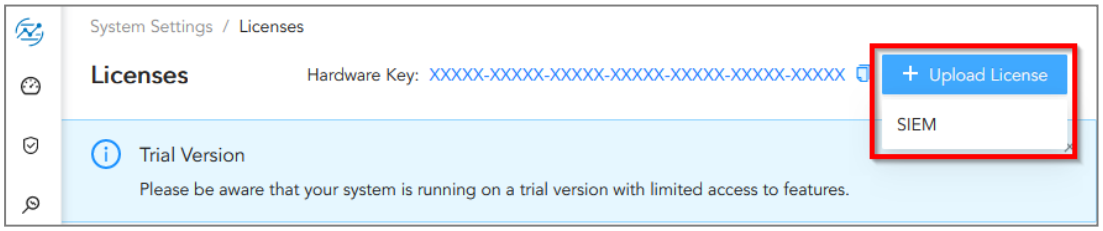
Download the license (*.pak* file) from your MyStormshield personal area. For more information, refer to the Downloading a product's license file page.

Installing the License

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

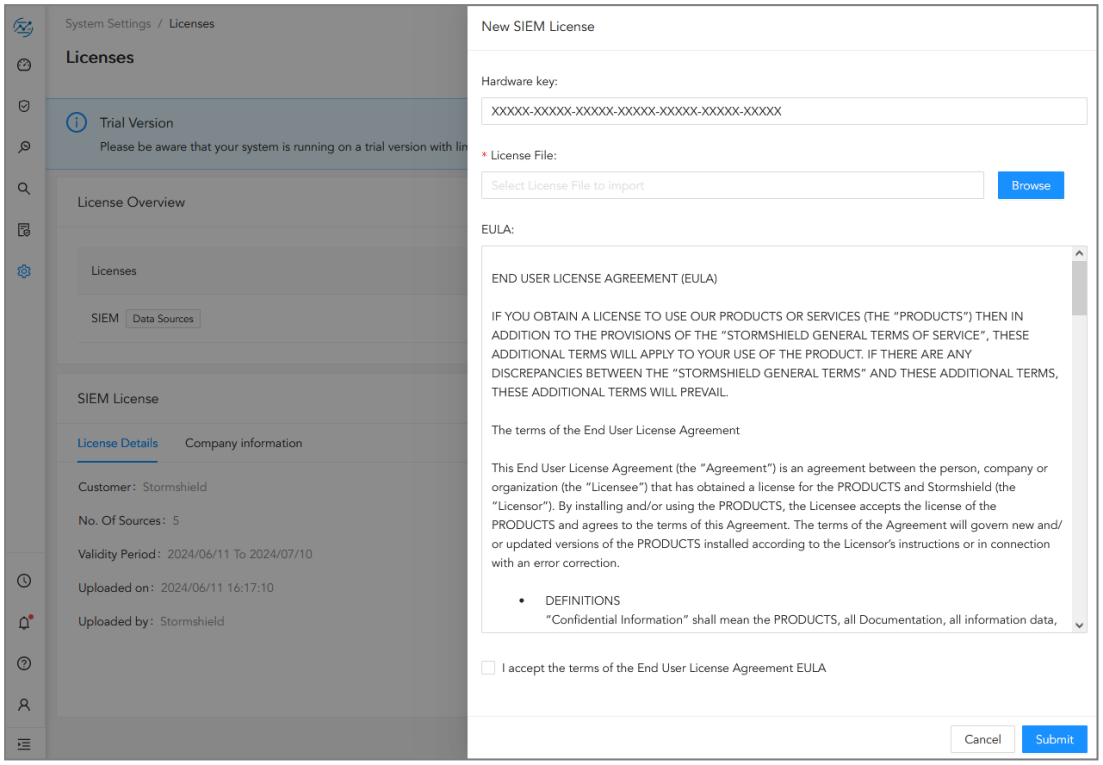


2. Click **Upload License > SIEM**.



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

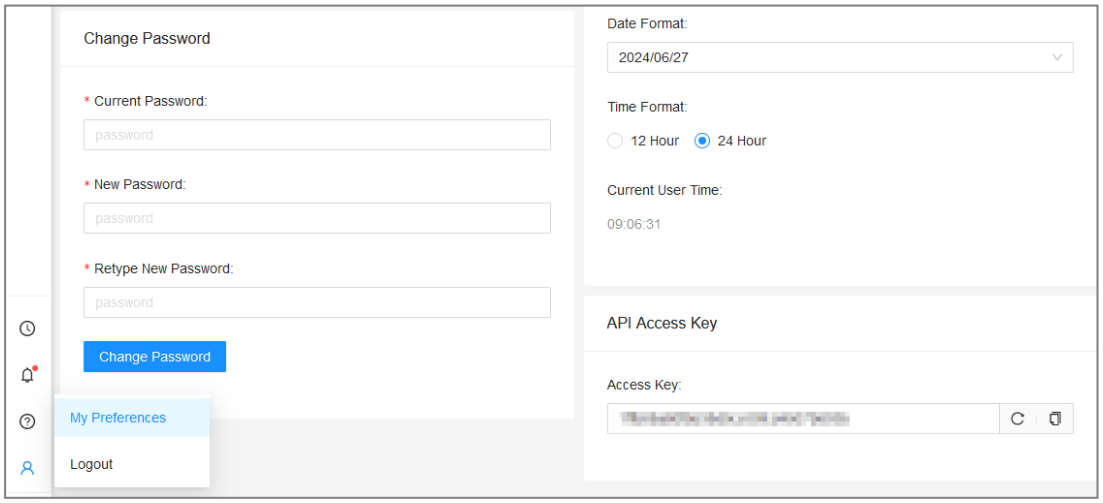
5. Click **Submit** if you agree with the terms and conditions of the EULA.



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

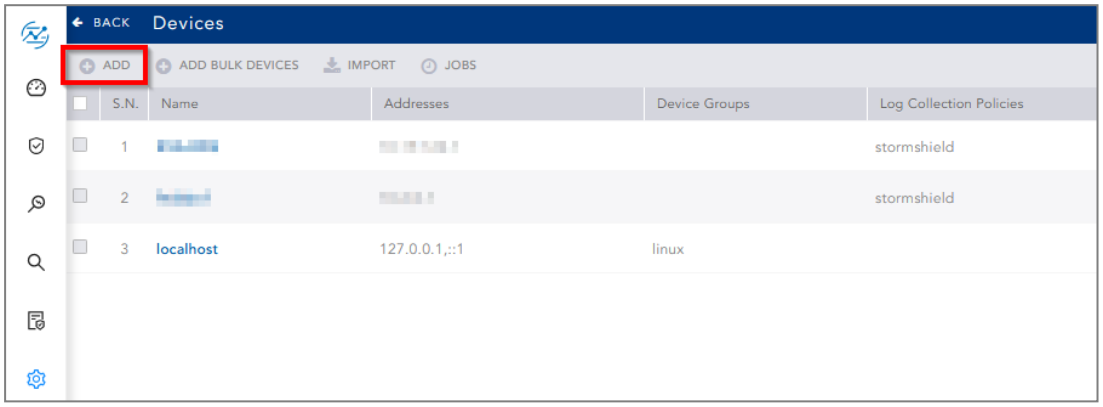
1. Identify the current SLS version installed. On SLS, click on ⓘ **Help** > **About SLS** in the navigation bar on the left and look for the version number.

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.

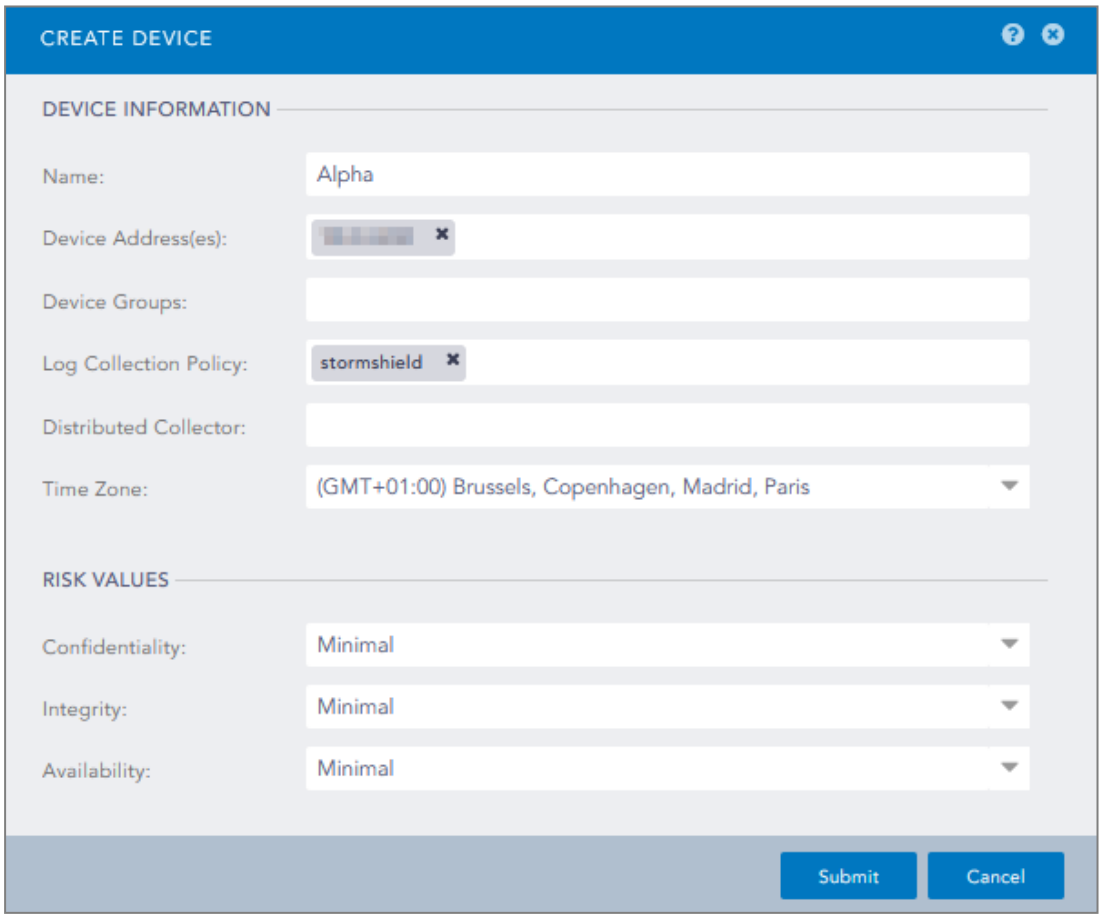
Getting the logs from an SNS firewall

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**.



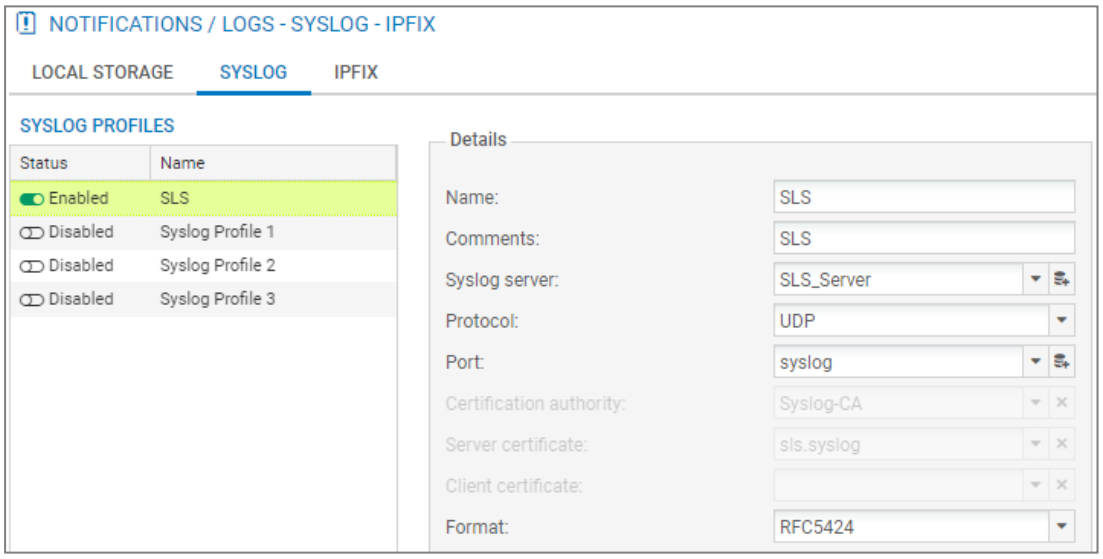
Configuring logs retrieval

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.

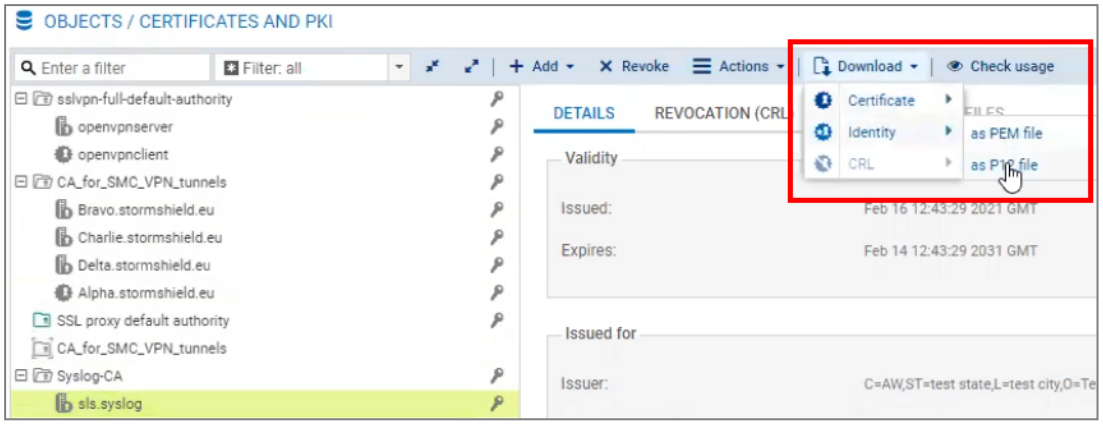


Getting the logs through Syslog-TLS

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.

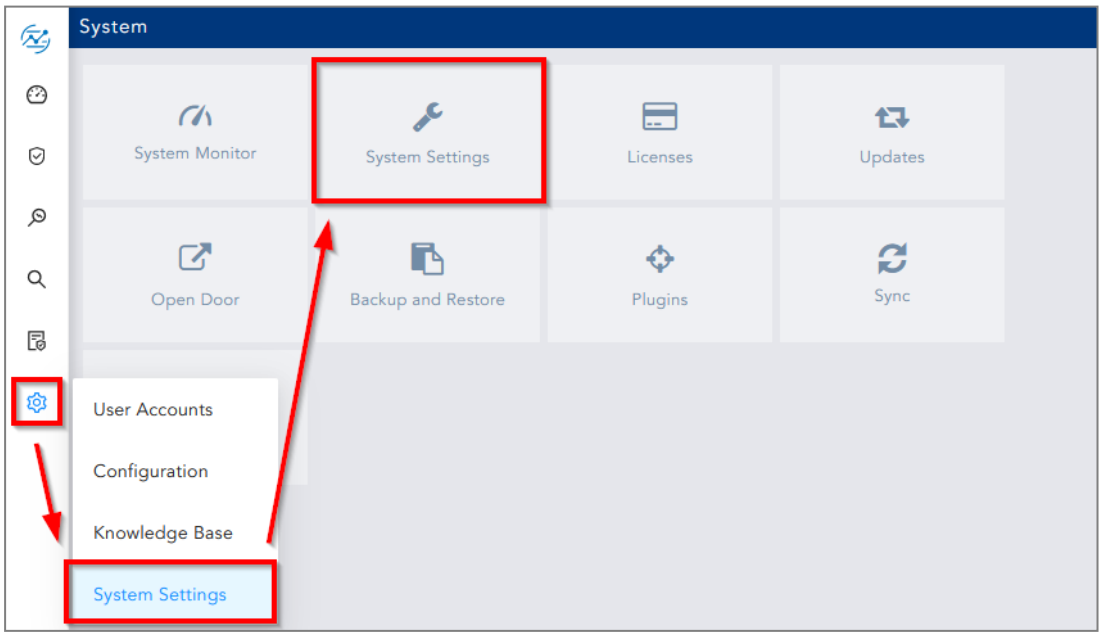
```
~/ SYSLOG-TLS ]$ openssl pkcs12 -in syslog2.sls.local.p12 -out
syslog2.sls.local.key -nocerts
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

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

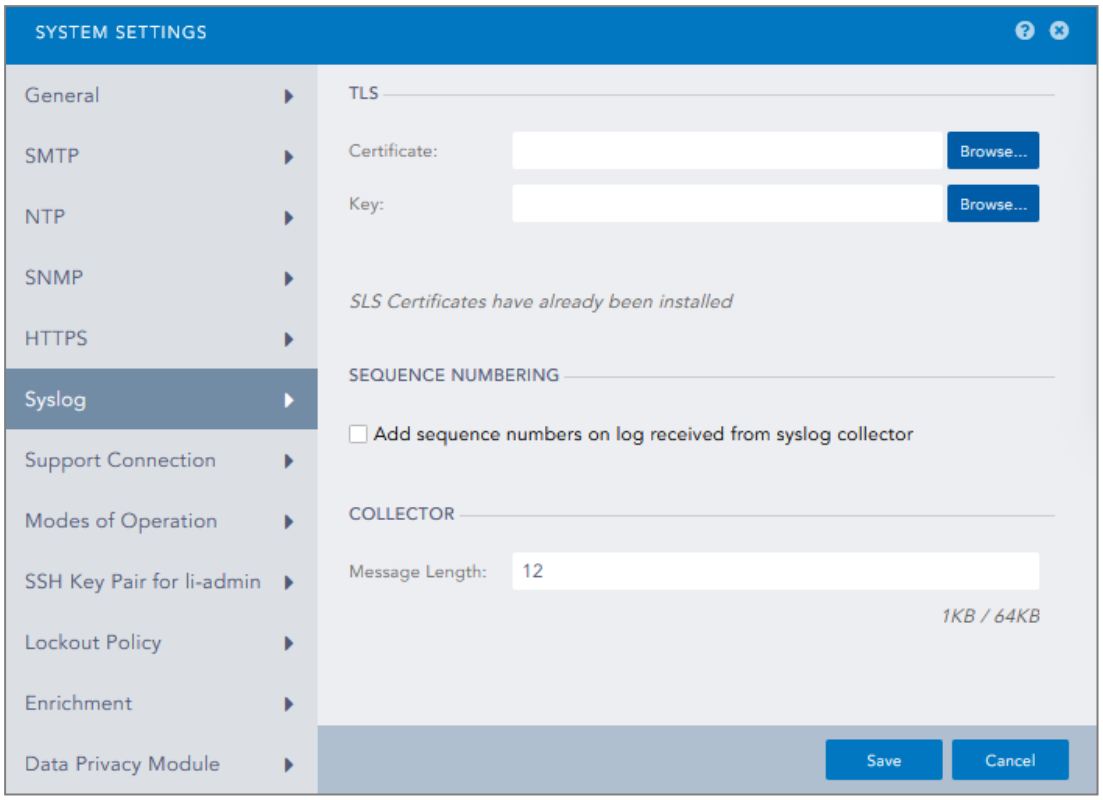
```
~/SYSLOG-TLS ]$ openssl rsa -in syslog2.sls.local.key -out syslog2.sls.local-
unprotected.key
Enter pass phrase for syslog2.sls.local.key:
writing RSA key
```

Importing the SNS Certificate Identity on SLS

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

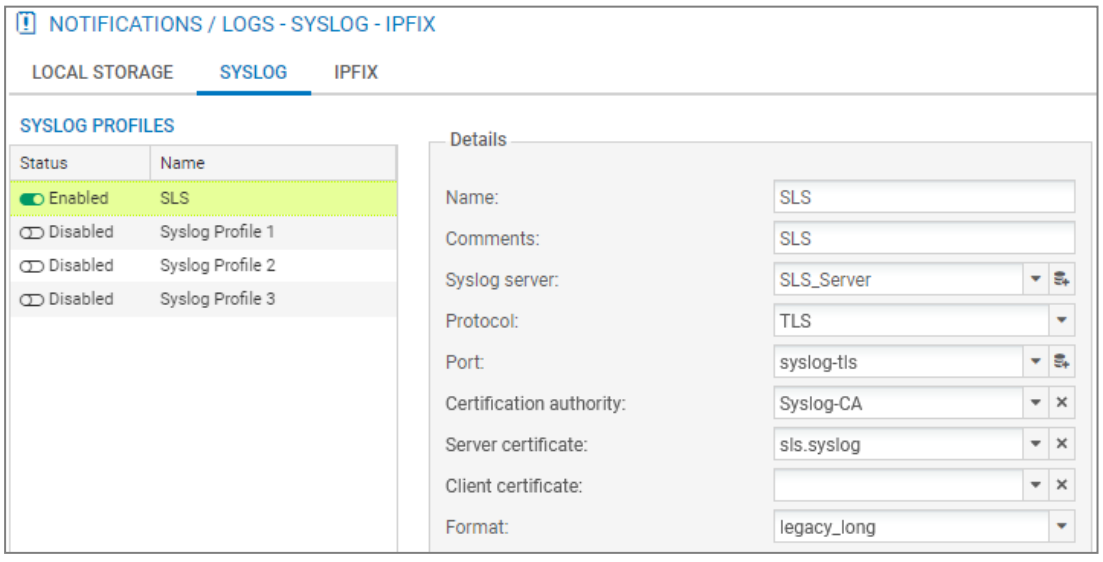


2. On the **Syslog** tab, import the **Certificate** (*.crt* file) and the **Key** (*.key* file).
3. **Save**.



Configuring a Syslog-TLS connection on the SNS firewall

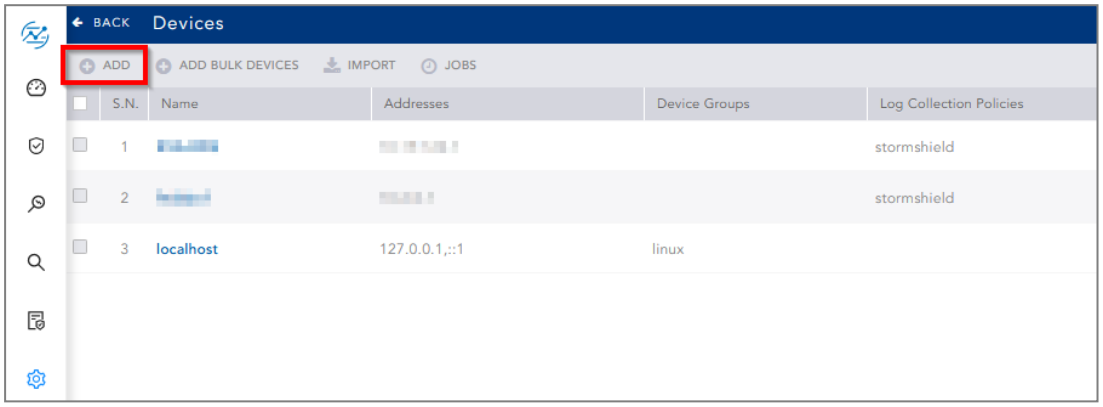
1. On SNS, go to **Configuration > Notifications > Logs – Syslog – IPFIX > Syslog**.
2. Select the object representing the IP address of the SLS instance or create a new object if one has not been created yet.
3. Choose *TLS* Protocol.
4. Fill in the certificate information.
5. Select *legacy_long* format.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



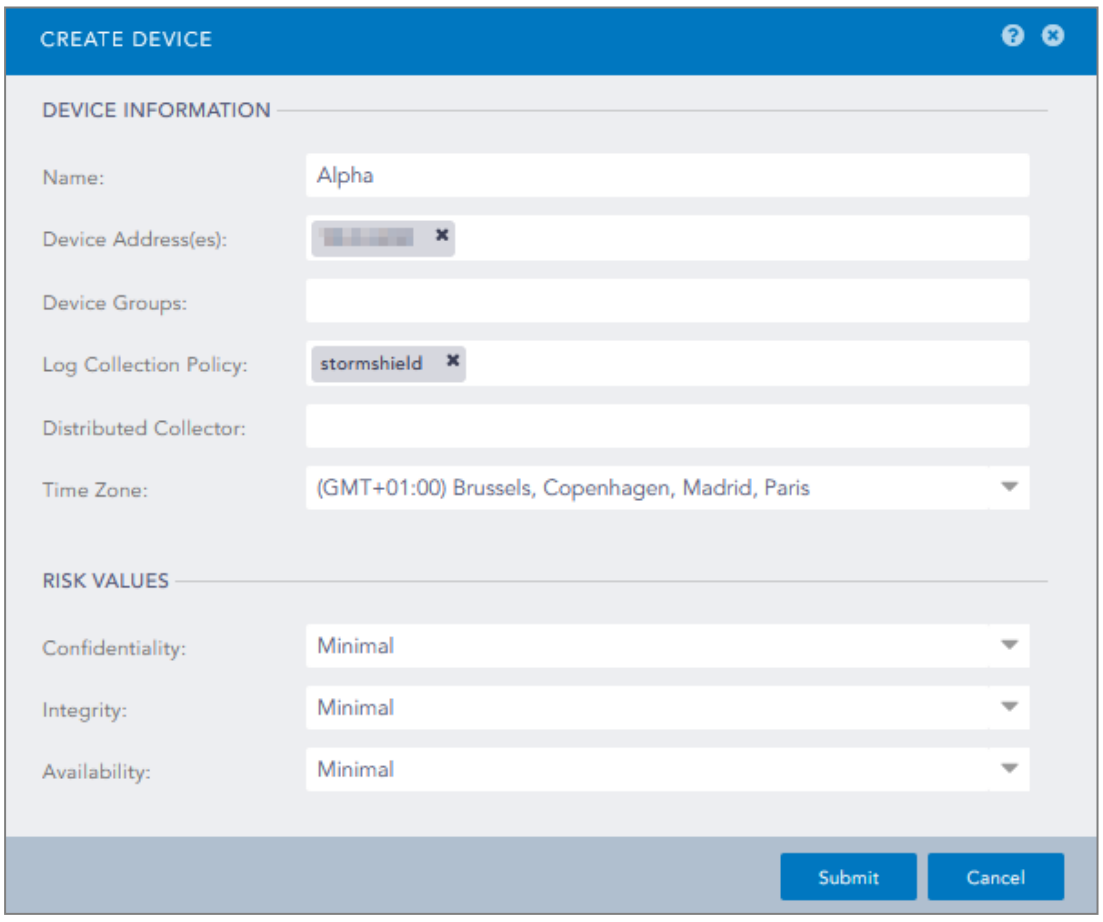
Getting the logs from SES Evolution

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**.



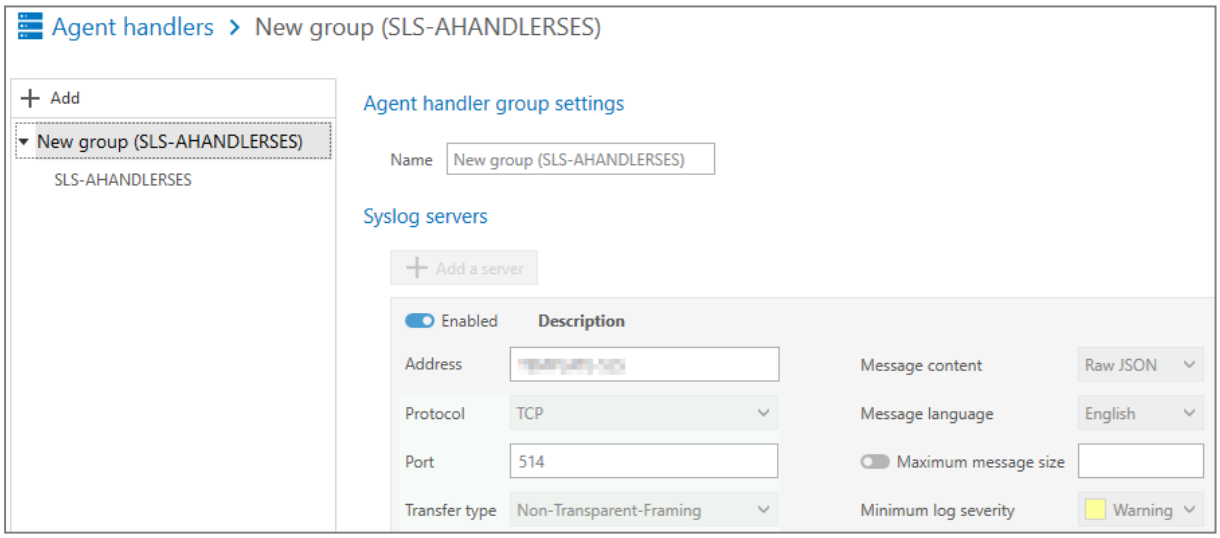
Configuring logs retrieval

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

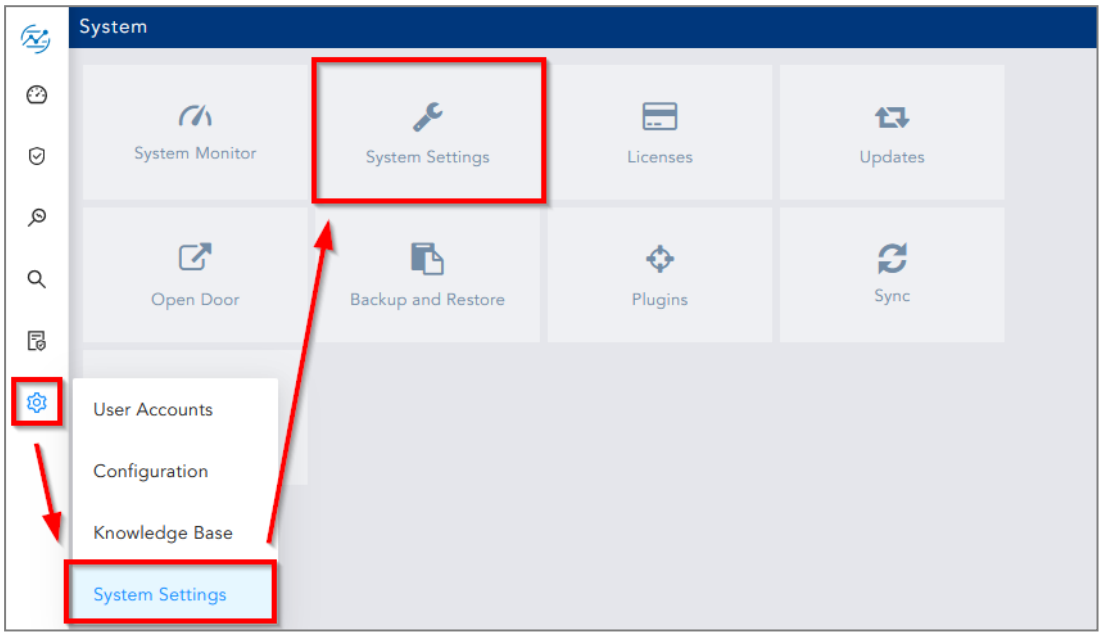
1. On the SES Evolution administration console, go to the **Agent handlers** menu and click the + icon.
2. Enter the **Name** of the Agent handler group.
3. In the **Address** field, enter the IP address of the SLS instance.
4. Select the appropriate **Protocol** (TCP or UDP).
5. Enter the **Port** number. 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.



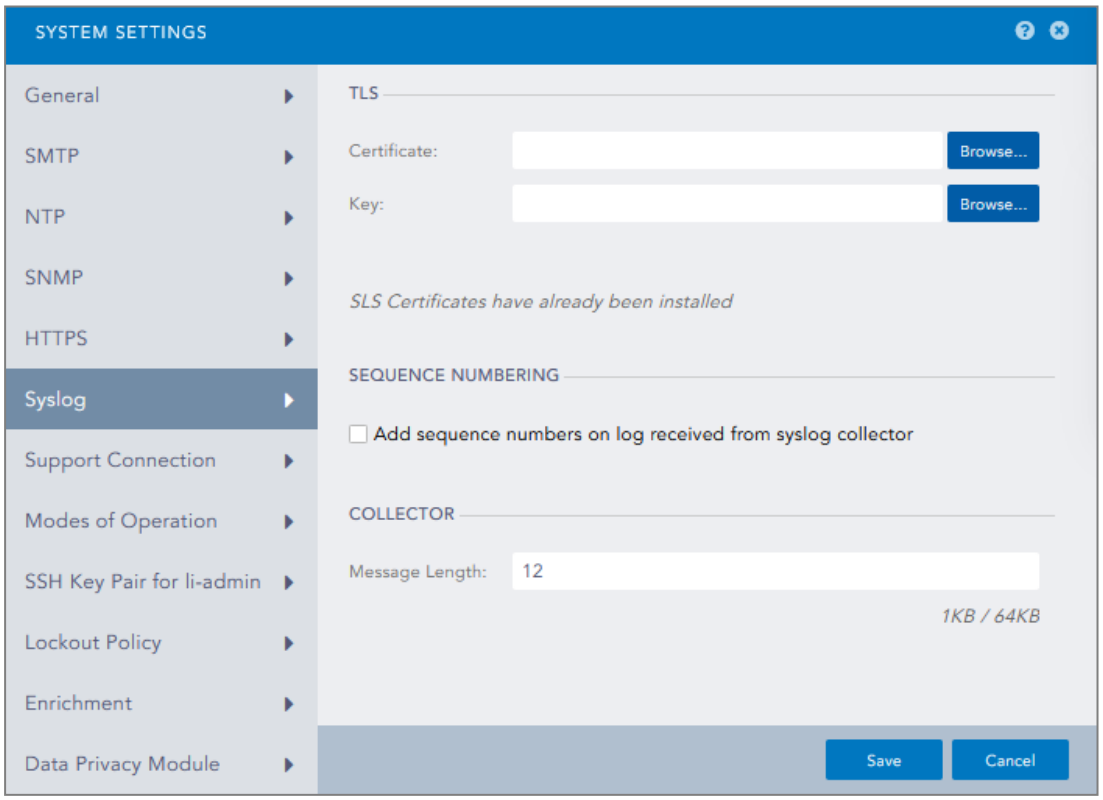
Getting the logs through Syslog-TLS

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**.

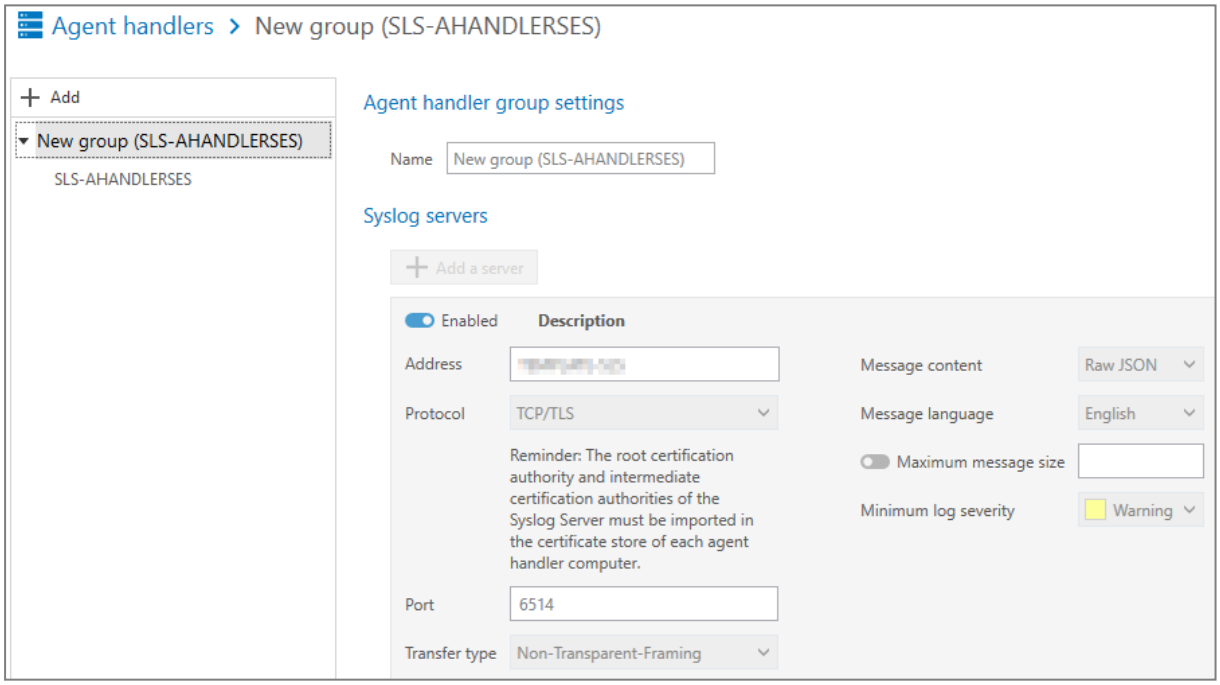


Importing the Root Certificate Authority

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