STORMSHIELD

GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

INSTALLATION GUIDE

Version 2.3

Document last updated: September 08, 2022

Reference: ses-en-installation_guide-v2.3.1

Table of contents

In the documentation, Stormshield Endpoint Security Evolution is referred to in its short form: SES Evolution.

1. Getting started

Welcome to the Stormshield Endpoint Security Evolution installation guide version 2.3.

SES Evolution is a global security solution that offers comprehensive workstation protection in organizations of all sizes.

The SES Evolution agent runs on workstations and transparently protects them from known and unknown attacks and intrusions. Since the agent does not rely on signature databases, it can operate with the same level of security in the SES Evolution agent handlers' connected and disconnected modes.

The administration console makes it possible to organize, configure and monitor all agents in a pool. In addition, fully configurable security policies can be set, and agents can be segmented into groups for easier administration. With advanced tools that track logs and analyze attacks, administrators can monitor the status of their pools and trace the source of attacks detected and blocked by SES Evolution agents.

SES Evolution is also built into your other security solutions, and reports its events directly in your SIEM system.

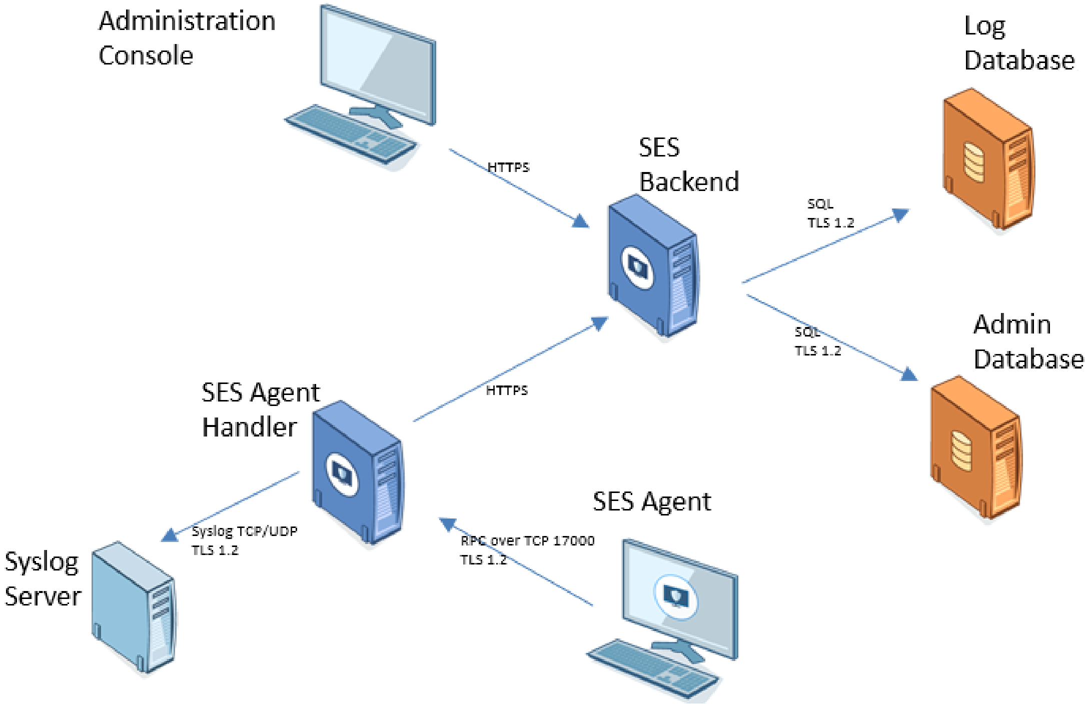
In the SES Evolution Installation Center, *SES_Evolution_Installation_Center.exe*, users can:

- Perform a new installation,
- Modify an existing installation,
- Update an existing installation,
- Uninstall databases.

The interface of the Installation Center appears in the language detected on the operating system.

SES Evolution runs on a set of components that communicate securely among themselves:

- Administration and log databases,
- One or several agent handlers, which receive data and logs directly from agents, and request updates for administration databases,
- One or several backend application servers, which centralize operations performed in the SES Evolution environment,
- One or several administration consoles,
- Agents deployed on workstations or servers.



For more information on how to protect network connections that use TLS, refer to the section Configuring TLS connections between components.

The administration console makes it possible to deploy SES Evolution agents on workstations. For further information, refer to Deploying agents on workstations in the *Administration Guide*.

Go to your MyStormshield client area, under the **Downloads** section, to obtain the SES Evolution Installation Center in the desired version.

2. System requirements for SES Evolution

To install and use Stormshield Endpoint Security Evolution version 2.3 in Microsoft Windows, you must meet these minimum requirements.

Some of the required components are in the *resources_x64* or *resources_x86* folders in the distribution package.

2.1 Backend

ℹ NOTES

- Virtual machines with a backend component installed cannot be cloned. This would make SES Evolution unstable, and it would then be impossible to uninstall the component.
- The backend component must not be installed on a domain controller.

Operating systems	• Windows Server 2012 R2*. On a newly installed Windows Server 2012 R2 operating system, Framework .NET 4.6.2 must be installed beforehand to enable the SES Evolution installation center to run. • Windows Server 2016* • Windows Server 2019* • Windows Server 2022* The Server Core version of these operating systems is also supported.
Processors for physical machines	At least a dual-core 2 GHz 64-bit processor or the equivalent. Itanium processors are not supported.
Processors for virtual machines	At least one virtual socket and two 2 GHz cores per socket. CPU reservation must be enabled on your hypervisor.
Physical memory	At least 2 GB or more if the operating system requires it.
Disk space	• At least 100 MB for installation • At least 1 GB for data storage. These are the disk space requirements for the NTFS file system. More space will be needed for updates and log storage.
Network configuration	• No static IP address requirements • Incoming communications: ◦ TCP 443 • Outgoing communications (SQL ports by default, but may depend on the settings of the SQL Server instance): ◦ TCP 1433 (SQL) ◦ TCP 1434 (SQL) ◦ UDP 1434 (SQL)
Software	• IIS server to install before SES Evolution. The IIS role must be enabled. • Framework .NET 4.6.2

Certificate	• *VeriSign Universal Root Certification Authority* certificate installed to verify the authenticity of SES Evolution updates. It must be installed in the Trusted root certification authorities or Third-party root certificate authorities certificate store.

2.2 Administration console

> **NOTE**
> Virtual machines with an SES Evolution administration console installed cannot be cloned. This would make SES Evolution unstable, and it would then be impossible to uninstall the component.

Operating systems	• Windows 7 (32 or 64 bits). Updates KB2533623, KB2922790 and KB3147071 are necessary. • Windows 8.1 update - August 2014 in 32 or 64 bits • Windows 10 Enterprise 2015 LTSB - 32/64 bits • Windows 10 Enterprise 2016 LTSB - 32/64 bits • Windows 10 Enterprise 2019 LTSC - 32 and 64 bits • Windows 10 20H2 – 32 and 64 bits • Windows 10 21H1 – 32 and 64 bits • Windows 10 21H2 – 32 and 64 bits • Windows 11 21H2 – 64 bits • Windows Server 2012 R2*. On a newly installed Windows Server 2012 R2 operating system, Framework .NET 4.6.2 must be installed beforehand to enable the SES Evolution installation center to run. • Windows Server 2016* • Windows Server 2019* • Windows Server 2022* * All versions supported by Microsoft except Server Core.
Processors for physical machines	• 32-bit processors: at least Intel Pentium 4 2 GHz or the equivalent, • 64-bit processors: at least Intel Pentium 4 2 GHz with x86-64 support or the equivalent. Itanium processors are not supported.
Processors for virtual machines	At least one virtual socket and a single 1 GHz core per socket. Stormshield recommends one virtual socket and two 2 GHz cores per socket. CPU reservation must be enabled on your hypervisor.
Physical memory	At least 1 GB. Stormshield recommends 2 GB.
Disk space	• At least 100 MB for installation • At least 100 MB for data storage These are the disk space requirements for the NTFS file system.
Network configuration	• Outgoing communication: ○ TCP 443 (HTTPS)
Software	Framework .NET 4.6.2

Certificate	• *VeriSign Universal Root Certification Authority* certificate installed to verify the authenticity of SES Evolution updates. It must be installed in the Trusted root certification authorities or Third-party root certificate authorities certificate store.

2.3 Agent handlers

> **NOTES**
>
> - Virtual machines with an agent handler installed cannot be cloned. This would make SES Evolution unstable, and it would then be impossible to uninstall the component.
> - The agent handler must not be installed on a domain controller.

Operating systems	• Windows 10 Enterprise 2015 LTSB – 64 bits • Windows 10 Enterprise 2016 LTSB – 64 bits • Windows 10 Enterprise 2019 LTSC – 64 bits • Windows 10 20H2 – 64 bits • Windows 10 21H1 – 64 bits • Windows 10 21H2 – 64 bits • Windows 11 21H2 – 64 bits • Windows Server 2008 R2. Update KB2533623 is necessary. The update KB3191566 is required in order to use the protection against WMI Persistence. • Windows Server 2012 R2*. On a newly installed Windows Server 2012 R2 operating system, Framework .NET 4.6.2 must be installed beforehand to enable the SES Evolution installation center to run. • Windows Server 2016* • Windows Server 2019* • Windows Server 2022* *Including the Server Core version.
Processors for physical machines	At least a dual-core 2 GHz 64-bit processor or the equivalent. Itanium processors are not supported.
Processors for virtual machines	At least one virtual socket and two 2 GHz cores per socket. CPU reservation must be enabled on your hypervisor.
Physical memory	At least 2 GB or more if the operating system requires it.
Disk space	• At least 100 MB for installation • At least 1 GB for data storage. These are the disk space requirements for the NTFS file system. More space will be needed for updates and log storage.

Network configuration	• No static IP address requirements • Incoming communications: ◦ TCP 17000 • Outgoing communication: ◦ TCP 443 (HTTPS) ◦ TCP port for Syslog ◦ UDP port for Syslog
Software	Framework .NET 4.6.2
Certificate	• *VeriSign Universal Root Certification Authority* certificate installed to verify the authenticity of SES Evolution updates. It must be installed in the Trusted root certification authorities or Third-party root certificate authorities certificate store.

2.4 SQL Server databases

Operating systems	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Processors	At least a 2 GHz 64-bit processor. Itanium processors are not supported. SQL Server runs more slowly on a virtual machine than in native mode due to the additional workload involved in virtualization.
Physical memory	SQL Server Express: at least 1 GB and a maximum of 1,41 GB SQL Server: at least 4 GB
Disk space	• At least 6 MB for installation. • The space required for data storage depends on the environment. Stormshield recommends NTFS (New Technology File System).
Network configuration	• No static IP address requirements. • Incoming communications (SQL ports by default, but may depend on the settings of the SQL Server instance): ◦ TCP 1433 (SQL) ◦ TCP 1434 (SQL) ◦ UDP 1434 (SQL)
Software	• SQL Server 2017 Cumulative Update 25 (14.0.3401.7) • SQL Server Express 2017 Cumulative Update 25 (14.0.3401.7) • SQL Server 2019 • SQL Server Express 2019 The SQL Server Express 2019 installation file and Cumulative Update 16 file can be found in your MyStormshield client area, under the **Downloads** section, in **Stormshield Endpoint Evolution** > **Resources**. Drop them in the same folder as the Installation Center if you want them to be installed when there is a new installation or when the solution is updated.

For more information about adapting the size and installing SQL Server, refer to *SQL Server Recommendations guide*.

2.5 Agents

2.5.1 Requirements

Operating systems	• Windows 7 in 32 and 64 bits. Updates KB2533623, KB2922790, KB3147071 KB4474419 and KB4490628 are necessary. The update KB3191566 is required in order to use the protection against WMI Persistence. Ensure that the Windows firewall service is running, otherwise the installation of the agent will fail. • Windows 8.1 update 3 (August 2014) - 32 or 64 bits • Windows 10 Enterprise 2015 LTSB - 32 and 64 bits • Windows 10 Enterprise 2016 LTSB - 32 and 64 bits • Windows 10 Enterprise 2019 LTSC - 32 and 64 bits • Windows 10 20H2 – 32 and 64 bits • Windows 10 21H1 – 32 and 64 bits • Windows 10 21H2 – 32 and 64 bits • Windows 11 21H2 – 64 bits • Windows Server 2008 R2. Update KB2533623 is necessary. The update KB3191566 is required in order to use the protection against WMI Persistence. • Windows Server 2012 R2* • Windows Server 2016* • Windows Server 2019* • Windows Server 2022* *Including the Server Core version.
Processors for physical machines	• 32-bit processors: at least Intel Pentium 4 2 GHz or the equivalent, • 64-bit processors: at least Intel Pentium 4 2 GHz with x86-64 support or the equivalent. Itanium processors are not supported.
Processors for virtual machines	At least one virtual socket and a single 1 GHz core per socket. Stormshield recommends one virtual socket and two 2 GHz cores per socket. CPU reservation must be enabled on your hypervisor.
Physical memory	At least 1 GB. Or more if the operating system requires it. Stormshield recommends 2 GB.
Disk space	• At least 100 MB for installation, • At least 200 MB for data storage. These are the disk space requirements for the NTFS file system. More space will be needed for updates and log storage.

Network configuration	• Outgoing communication: ○ TCP 17000 (RPC)
Software	Framework .NET 4.6.2 or higher.
Display	At least 1024X768.
Certificate	• *VeriSign Universal Root Certification Authority* certificate installed to verify the authenticity of SES Evolution updates. It must be installed in the Trusted root certification authorities or Third-party root certificate authorities certificate store.

2.5.2 Using agents on Microsoft Windows Server Core operating systems

SES Evolution agents can be installed on Windows Server Core 2012 R2, 2016, 2019 and 2022 operating systems.

As these operating systems do not have a traditional GUI, the agent's interface does not start automatically when a user session is opened (🛡 icon in the task bar on a standard operating system). To display the agent’s GUI:

- Use the command `EsGui.exe`.

In addition, if requests for user confirmation are configured in a security rule, the agent will not open any window, automatically assuming that the answer to the confirmation is "no". There is no way for the user to reply with a "yes".

2.6 Adapting the size of the SES Evolution server according to the number of agents

The table below gives an estimate of the lowest hardware requirements that your SES Evolution environment needs in relation to the number of agents installed. All server components can be installed on the same machine up to 5,000 agents. If you have more than 5,000 agents, you are advised to dispatch components on several machines.

Agent handlers can support up to 30,000 agents.

SSD hard disks are recommended in particular to optimize performance and response time.

> **IMPORTANT**
> RAM quota refers to the amount of memory that you must allocate to the SQL Server so that it does not use up all the memory on the server. This value can be configured in *SQL Server Management Studio* after the databases have been installed. Refer to the RAM column in the table below.

Number of agents	CPU	RAM	Disk
< 200 agents (1 server)	2 cores/2 threads - 3 GHz	4 GB SQL quota: 1.5 GB	170 GB for 1 year of log retention, 155 GB for 6 months, 150 GB for 3 months.

< 500 agents (1 server)	4 cores/4 threads - 3 GHz	6 GB SQL quota: 3 GB	250 GB for 1 year of log retention, 175 GB for 6 months, 150 GB for 3 months.
< 1000 agents (1 server)	4 cores/4 threads - 3 GHz	6 GB SQL quota: 3 GB	300 GB for 1 year of log retention, 250 GB for 6 months, 200 GB for 3 months.
< 2500 agents (1 server)	4 cores/4 threads - 3 GHz	8 GB SQL quota: 4 GB	600 GB for 1 year of log retention, 350 GB for 6 months, 250 GB for 3 months.
< 5000 agents (1 server)	6 cores/6 threads - 3 GHz	12 GB SQL quota: 6 GB	1 TB for 1 year of log retention, 600 GB for 6 months, 350 GB for 3 months.
< 10000 agents (2 servers)	**Database**: 2 cores/2 threads - 3 GHz **Backend + Agent handler:** 4 cores/4 threads - 3 GHz	**Database**: 8 GB **Backend + Agent handler:** 8 GB	**Database**: 2 TB for 1 year of log retention, 1 TB for 6 months, 600 GB for 3 months. **Backend + Agent handler:** 50 GB
< 30000 agents (3 servers)	**Database**: 4 cores/4 threads - 3 GHz **Backend + Agent handler:** 4 cores/4 threads - 3 GHz **Additional agent handler**: 4 cores/4 threads - 3 GHz	**Database**: 16 GB **Backend + Agent handler:** 16 GB **Additional agent handler**: 16 GB	**Database**: 8 TB for 1 year of log retention, 4 TB for 6 months, 2 TB for 3 months. **Backend + Agent handler:** 100 GB **Additional agent handler**: 100 GB
< 60000 agents (4 servers)	**Database**: 4 cores/4 threads - 3 GHz **Backend + Agent handler:** 4 cores/4 threads - 3 GHz **2 additional agent handler**s: 4 cores/4 threads - 3 GHz	**Database**: 16 GB **Backend + Agent handler:** 16 GB **2 additional agent handler**s: 16 GB	**Database**: 12 TB for 1 year of log retention, 6 TB for 6 months, 5 TB for 3 months. **Backend + Agent handler:** 100 GB **2 additional agent handler**s: 100 GB
< 90000 agents (5 servers)	**Database**: 4 cores/4 threads - 3 GHz **Backend + Agent handler:** 4 cores/4 threads - 3 GHz **3 additional agent handler**s: 4 cores/4 threads - 3 GHz	**Database**: 16 GB **Backend + Agent handler:** 16 GB **3 additional agent handler**s: 16 GB	**Database**: 16 TB for 1 year of log retention, 8 TB for 6 months, 5 TB for 3 months. **Backend + Agent handler:** 100 GB **3 additional agent handler**s: 100 GB
< 120000 agents (6 servers)	**Database**: 4 cores/4 threads - 3 GHz **Backend + Agent handler:** 4 cores/4 threads - 3 GHz **4 additional agent handler**s: 4 cores/4 threads - 3 GHz	**Database**: 16 GB **Backend + Agent handler:** 16 GB **4 additional agent handler**s: 16 GB	**Database**: 16 TB for 1 year of log retention, 8 TB for 6 months, 5 TB for 3 months. **Backend + Agent handler:** 100 GB **4 additional agent handler**s: 100 GB
< 150000 agents (7 servers)	**Database**: 4 cores/4 threads - 3 GHz **Backend + Agent handler:** 4 cores/4 threads - 3 GHz **5 additional agent handler**s: 4 cores/4 threads - 3 GHz	**Database**: 16 GB **Backend + Agent handler:** 16 GB **5 additional agent handler**s: 16 GB	**Database**: 24 TB for 1 year of log retention, 12 TB for 6 months, 6 TB for 3 months. **Backend + Agent handler:** 100 GB **5 additional agent handler**s: 100 GB

3. Getting the SES Evolution license

You need to get your license from your MyStormshield client area and register it when installing the solution.

Licenses determine the number of active SES Evolution agents that you can manage with the solution, and have an expiry date. Several licenses can be combined for the same environment. However, each license is valid for the installation of a single SES Evolution environment. An additional license is needed to install another environment.

To get your license:

1. Make sure you have the Stormshield PDF delivery document and log in to your MyStormshield client area.
2. In the menu on the left, select **Products** > **Register a product** > **Register SES software**, and accept the terms of use.
3. Enter the following information:
   - **Associated company**: name of the company under which you are registered at Stormshield.
   - **License key**: character string located in the Serial number column of the delivery document.
   - **Reseller**: name of your SES Evolution reseller.
4. Click **Register**.
5. On your personal area dashboard, from the **List of products** table, click on your serial number.
6. Click on **Download all licenses** and unzip the downloaded file.

4. Installing SES Evolution

The SES Evolution Installation Center takes you through the various steps in a standard or demo installation.

The solution's components can either be installed on the same machine or on separate machines.

Read the following recommendations before installing SES Evolution:

- The console, backend component and databases must be installed on hosts that belong to the same Active Directory domain, or on two domains that have a relationship of trust.
- The SQL Server is needed to install databases.
- You are advised to install the backend component and databases in a trusted zone.
- Do not install the backend component or agent handler on a domain controller.
- Administrator privileges are required to install the solution.
- Before installing a full server or the backend component, it is recommended to disable Windows update and to enable it again afterwards.
- On a backend component or an agent handler, the "%PROGRAMDATA%\SES Evolution" folder should be excluded from the antivirus scan on the workstation in order to optimize performance. SES Evolution indeed uses many compressed *cab* files, which trigger the antivirus analysis.
- An SES Evolution agent can be installed on a backend component or an agent handler; an appropriate security policy is provided by default to protect them.

If you encounter issues while installing SES Evolution, look up the log files located in the administrator's *AppData/Local/Temp* folder.

4.1 Demo installations

In demo installations, all the components of the solution are installed on the same machine with a simplified password and access account configuration.

> **WARNING**
> Additional components cannot be added in demonstration installations.
> Such installations are recommended only for test or demonstration purposes. Do not install a demo in a production environment.
> In addition, a demonstration installation cannot be migrated to a standard installation. The solution would need to be fully uninstalled before you can proceed with a standard installation.

To install SES Evolution:

1. Log in to the machine using a Windows account with the following characteristics:
   - If the machine belongs to a domain, the Windows account must be a domain account,
   - It must hold administration privileges on the local machine,
   - If the database already existed before the installation, the account must have access to the database instance with the "sysadmin" server role.
2. Double-click on the *SES_Evolution_Installation_Center.exe* file.
3. Click on **New installation**.

4. Select **Demo installation**.
5. Installation options in the **Databases** section are automatically selected based on your configuration:
   - If there are no SQL Server instances installed on the workstation, SES Evolution will suggest installing SQL Server Express. The first option will then be automatically selected. The Installation Center automatically detects the SQL Server Express installation file, and the SQL Server Express update file (if there is one), if they are in the same folder as the Installation Center. Fill in the information required to connect to the SQL Server Express instance.
   - If there is already a SQL Server instance on the workstation, the second option will be automatically selected. The SQL Server instance must not contain any data. The name of the database instance appears automatically.
   - The “sysadmin" role is required for the creation of databases, regardless of whether a Windows or SQL Server account is selected.
6. Configure **Log database storage.** The parameters differ depending on whether you have SQL Server Enterprise or SQL Server Express.
   - **Log storage path**: Use the default SQL Server storage path or a custom path. This field is available only on SQL Server Enterprise.
   - **Agent event retention** and **System log retention**: SES Evolution logs are kept by default for 12 months before they are automatically deleted, and only for two months if you are using SQL Server Express. Enter a retention period higher than or equal to 1 month. The maximum duration allowed on SQL Server Express is 12 months.
     Logs can be kept indefinitely on SQL Server Enterprise. As such, ensure that you always have enough disk space to contain all logs.
     Retention values can be modified later through the administration console. For more information, refer to the section in the *Administration Guide*.
7. In the **General single password** section, set a password which will be used later to encrypt certification authorities and the backend component's connections to databases. Choose a password that meets the requirements of the database instance.
   The super administrator account is the domain account with which you have logged in. It must belong to the same Active Directory domain as the SQL server, the various SES Evolution database instances and the administration console. If this is not the case, then a relationship of trust must be established between the domains.
8. Register your license file. To get your license, refer to the section Getting the SES Evolution license.
9. Click **Install**.
10. In the next step, move your mouse randomly to produce random numbers. The certificates needed to run SES Evolution and guarantee its security are generated from these numbers.
11. Quit the Installation Center once the installation is complete. The solution is now ready.

You are advised to back up the administration database and log database regularly.

4.1.1 Troubleshooting

Installation failed. The network path was not found

Situation: During a demo installation, the Installation center displays this error:
Installation failed. The network path was not found.

Cause: The host is linked to an Active Directory but you have run the Installation center with a local account.

Solution: Log in as an Active Directory account to install SES Evolution.

4.2 Standard installations

Standard installations make it possible to use SES Evolution in a production environment. You can either install all the components on the same machine or spread them out over several machines.

During the initial installation of SES Evolution on the first machine, databases and certificates must be installed and the super administrator must be created; these options cannot be unselected. Other components can be added to this machine.

To add one or several backend components, administration consoles and agent handlers later on other machines, you need to run the Installation Center on each machine and modify an existing installation. The machines on which consoles and agent handlers are installed must be able to communicate with the backend. The backend must also be able to communicate with the databases.

4.2.1 Preparing a standard installation

Follow the recommendations below for a standard installation of your SES Evolution environment:

- Active Directory, DNS and network configurations must be prepared in advance, before installing SES Evolution.
- The backend component and agent handlers can be installed on machines that belong to different Active Directory domains. For further information, refer to **Installing SES Evolution servers on different Active Directory domains**.
- If you have more than 50,000 agents, we recommend that you set up Windows NLB on machines that host backend servers to form a cluster that will guarantee redundancy and load balancing.
- We recommend that you run the Installation Center on machines in the following sequence:
  - Servers that host administration and log databases,
  - Servers that host the backend component,
  - Servers that host the agent handler,
  - Servers or workstations that host the administration console.
- You are advised to back up the administration database and log database regularly.

4.2.2 Performing a standard installation

For an initial installation of SES Evolution:

1. Log in to the machine using a Windows account with the following characteristics:
   - If the machine belongs to a domain, the Windows account must be a domain account,
   - It must hold administration privileges on the local machine,
   - If the database already existed before the installation, the account must have access to the database instance with the “sysadmin” server role.
2. Double-click on the *SES_Evolution_Installation_Center.exe* file.
3. Click on **New installation**.
4. Select **Standard installation**.

5. Enter the addresses of the administration and log database instances. Both databases can be located on the same instance. Regardless of which authentication type is selected, the “sysadmin" role is required for the creation of databases.

> **NOTE**
> Database instances must not contain data and the operating system from which the Installation Center is run must be able to access the instances.

6. Configure **Log database storage.** The parameters differ depending on whether you have SQL Server Enterprise or SQL Server Express.
    - **Log storage path**: Use the default SQL Server storage path or a custom path. This field is available only on SQL Server Enterprise.
    - **Agent event retention** and **System log retention**: SES Evolution logs are kept by default for 12 months before they are automatically deleted, and only for two months if you are using SQL Server Express. Enter a retention period higher than or equal to 1 month. The maximum duration allowed on SQL Server Express is 12 months.
      Logs can be kept indefinitely on SQL Server Enterprise. As such, ensure that you always have enough disk space to contain all logs.
      Retention values can be modified later through the administration console. For more information, refer to the section in the *Administration Guide*.
7. Enter the passwords that encrypt private keys for root and intermediate certificate authorities.
8. The domain account with which you have logged in is pre-entered as the super administrator account. The super administrator is the user of the console that makes it possible to create other users. It must belong to the same Active Directory domain as the SQL server, the various SES Evolution database instances and the administration console. If this is not the case, then a relationship of trust must be established between the domains.

> **NOTE:**
> If you rename the domain account which is SES Evolution super administrator, make sure you have created before a user with the new name in the SES Evolution administration console. Otherwise you will not be able to log in to the console. For more information, refer to the *Administration Guide*.

9. Select **Backend** if you wish to install a backend component on this machine. The backend centralizes all the operations performed in the environment, and is the core of the installation. Specify the following parameters:
   - The DNS name of the host that will be used to access the backend in HTTPS. The name of the machine from which you have logged in and the domain are pre-entered. This name cannot be changed later.
   - The cluster host name is mandatory. If you want to implement load balancing or redundancy (NLB feature) on several backends (recommended for more than 50,000 agents), this is the address that agent handlers and the console will use to connect to the backend. The DNS name must be different from the first host name. This information will be known only after the initial installation of the backend. Both of these DNS names cannot be changed later.
     If you do not wish to set up a backend cluster, a DNS entry (CNAME) must still be declared with a specific name (e.g., SESBACKCLUSTER.SES.local). Its IP address will point to the address of the machine on which the backend is installed. SES Evolution components will not need to be reinstalled later if an architecture with an NLB cluster is implemented. The DNS alias will need to be changed so as it points to the virtual IP address of the NLB cluster.
   - Select the type of account that will be used as the identity for the worker processes of the IIS server:

Domain account	Account on the domain, ideally created only for use as the identity of SES Evolution services and programs, with a password that never expires. The service that updates the backend, installed on every backend server, also uses this domain account.
Local account	Local account on the machine. This option can be used to install SES Evolution outside a Windows domain that uses several different machines. This requires the creation of local accounts with the same login and password on every machine. The service that updates the backend, installed on every backend server, also uses this domain account.
Predefined IIS account	Virtual account valid only on the local machine, and to be used only for local installations of a backend on the same machine as the database. In this case, the update service on the backend is installed as SYSTEM.

   - Enter the name and password of the account.
10. Next, select **Stormshield Endpoint Security Evolution Agent handlers** and **Administration console** if you wish to install them on this machine. Enter the contact address of the agent handler, that agents will use to contact it.
11. Register your license file. To get your license, refer to the section Getting the SES Evolution license.
12. Click **Install**.
13. In the next step, move your mouse randomly to produce random numbers. The certificates needed to run SES Evolution are generated from these numbers.
    If the IIS role is not enabled, the Installation Center will enable it automatically when the backend component is installed. This operation may take a while to complete.
14. Quit the Installation Center once the installation is complete.

To install the other components on other machines, run the Installation Center on each machine and select **Modify an existing installation**. For further information, refer to Adding a console, backend component or agent handler.

You are advised to back up the administration database and log database regularly.

4.3 Installing SES Evolution servers on different Active Directory domains

If there are several Active Directory domains in your infrastructure, you can install agent handlers on machines that belong to domains other than the one on which the backend component is located. Communications between the backend communication and agent handlers are secured using certificate-based mutual authentication.

The various Active Directory domains must therefore be able to communicate with one another.

Follow the steps below to install an agent handler on a domain other than the one on which the backend component is located:

1. Using a server that belongs to the Active Directory domain 1, perform an **advanced installation** in the Installation Center and select the installation of the backend component.
2. Using a server that belongs to Active Directory domain 2, click on **Modify an existing installation** in the Installation Center and click on **Stormshield Endpoint Security Evolution Agent handlers**.
3. Enter the values of the parameters and click on **Install**.

If you are installing several agent handlers, repeat the operation on each machine that hosts agent handlers.

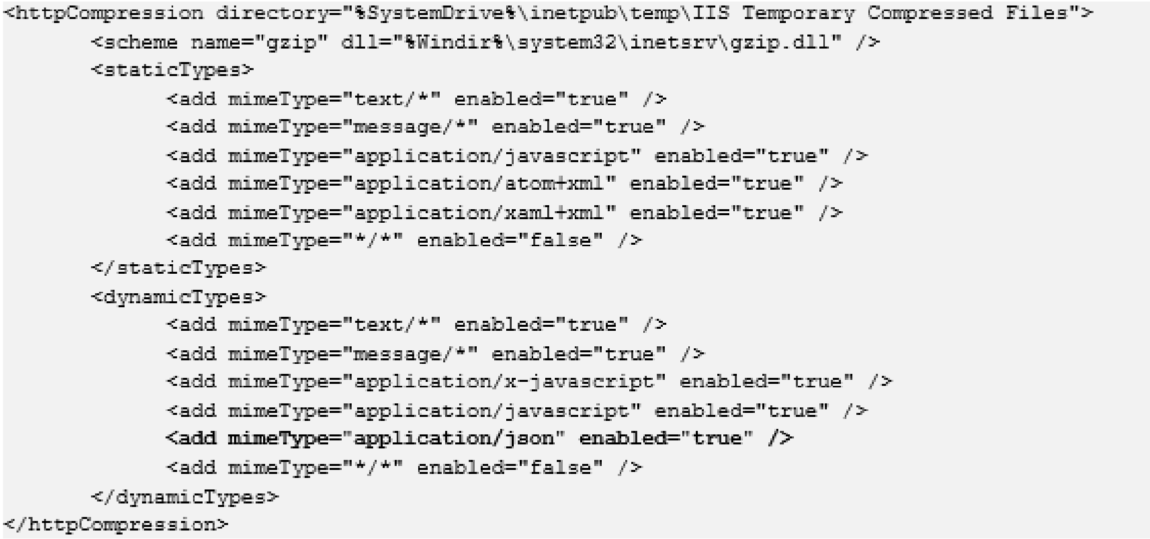
4.4 Windows Server 2012: Enabling HTTP compression

> **NOTE**
> This process applies only to Windows Server 2012 operating systems. Compression is automatic in Windows Server 2016 and 2019.

On machines that host the backend component in Windows Server 2012, HTTP compression must be manually enabled for traffic sent from the backend component to agent handlers and administration consoles.

To enable compression:

- Add the line `<add mimeType="application/json" enabled="true" />` to the section `<dynamicTypes>` in the file `%windir%\System32\inetsrv\config\ApplicationHost.config`.



```
<httpCompression directory="%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files">
       <scheme name="gzip" dll="%Windir%\system32\inetsrv\gzip.dll" />
       <staticTypes>
             <add mimeType="text/*" enabled="true" />
             <add mimeType="message/*" enabled="true" />
             <add mimeType="application/javascript" enabled="true" />
             <add mimeType="application/atom+xml" enabled="true" />
             <add mimeType="application/xaml+xml" enabled="true" />
             <add mimeType="*/*" enabled="false" />
       </staticTypes>
       <dynamicTypes>
             <add mimeType="text/*" enabled="true" />
             <add mimeType="message/*" enabled="true" />
             <add mimeType="application/x-javascript" enabled="true" />
             <add mimeType="application/javascript" enabled="true" />
             <add mimeType="application/json" enabled="true" />
             <add mimeType="*/*" enabled="false" />
       </dynamicTypes>
</httpCompression>
```

5. Adding a console, backend component or agent handler

In the Installation Center, the **Add a new component to an existing installation** menu offers the possibility of installing consoles, backend servers or agent handlers on machines other than the one on which you performed the first installation. Components cannot be added if you have performed a demo installation.

Agent handlers can be installed on machines that belong to Active Directory domains other than the one on which the backend component is located. For further information, refer to Installing SES Evolution servers on different Active Directory domains.

No additional license is needed to add these components to the same environment.

To add a console, backend component or agent handler, perform the following operations:

1. Log in to the machine using a Windows account with the following characteristics:
   - If the machine belongs to a domain, the Windows account must be a domain account,
   - The account must hold administration privileges and permissions to open interactive sessions on the local machine,
   - Only for the backend component, the account must have access to the database instance with the “sysadmin” server role.
2. Run the file *SES_Evolution_Installation_Center.exe*.
3. Click on **Add a new component to an existing installation.**
4. Select the component to install.
5. If you are adding a backend component, enter the address of the administration database instance and the login credentials of the super administrator account on the database. If you are adding a console or agent handler, enter the address of the backend component.
6. Define the various parameters. For more information on parameters, refer to Standard installations. With regard to the intermediate certification authority of the backend component or agent handler, its password cannot be viewed during the initial installation since the password is already entered in the **Certificates** section of the standard installation.
7. Apply these changes to complete the process.

6. Updating SES Evolution

To update the components of SES Evolution, obtain an Installation Center in the desired version from your MyStormshield client area, under the **Downloads** section and run it from a host on which a component of the solution has been installed. All components will be automatically updated.

1. Log in to the machine using your domain account.
2. Double-click on the *SES_Evolution_Installation_Center.exe* file.
3. Click on **Update an existing installation**.
4. Enter the address of the administration database instance and the login credentials of the super administrator account on the database.
5. In the next window, the Installation Center automatically detects the components that need to be updated. Click on **Start update**.
   If the administration console requires an update, the Installation Center shows the list of users connected to the console, and the names of their workstations. A red banner appears on all open consoles, asking users to save their changes and quit the console. The update starts when all consoles are closed.
6. If there are still consoles that remain open:
   a. Click on **Force update** to shut down the consoles remotely and proceed with the update. Use this option only if you are sure that there are no changes to be saved, for example if the console user is absent.
   b. Click on **Cancel update** if you prefer to postpone the update.

Refer to the section Updating agents in the Administration Guide for more details on how to update agents.

6.1 Troubleshooting

6.1.1 Failed to extract files from patch (0xa0050005)

Situation: During an update, the Installation center displays this error:
Failed to extract files from patch (0xa0050005).

Cause: The certificate required to verify the authenticity of the SES Evolution update could not be found on the machine.

Solution: Add the **VeriSign Universal Root Certification Authority** certificate to the *Trusted root certification authorities* or *Third-party root certificate authorities* certificate store.

- or -
Link up the machine to the Internet so that the certificate can be downloaded automatically.

7. Uninstalling SES Evolution

To fully uninstall SES Evolution, the various SES Evolution components must be uninstalled in the following order:

1. SES Evolution agents,
   For further information, refer to Uninstalling agents in the *Administration Guide*.
2. Administration consoles,
3. Agent handlers,
4. Backend servers,
5. Databases,

Administrator privileges are required.

7.1 Uninstalling consoles, agent handlers and backend servers

1. Log in to the computer that hosts the SES Evolution component using your domain account.
2. In **Programs and Features** in the Windows control panel, select the desired component and click on **Uninstall**.
3. Enter the requested information in the SES Evolution uninstaller which opens: **Backend host name** for the console and agent handler, and **Database instance** for the backend server
4. Click on **Uninstall**.
5. Restart the computer once the components are uninstalled.

7.2 Uninstalling databases

1. Log in to the host using your domain account.
2. Double-click on the *SES_Evolution_Installation_Center.exe* file.
3. Click on **Uninstall database**.
4. Fill in the information required to connect to the database instance and click on **Connect**.
5. In the following screen, click on **Uninstall database**.
6. Quit the Installation Center once the databases are uninstalled.

For further information on uninstalling agents, refer to Uninstalling agents in the *Administration Guide*.

8. Configuring TLS connections between components

Network connections between the components of the SES Evolution solution are protected by TLS. To configure connections that use TLS, components rely on the configuration of the operating system on backend servers and agent handlers.

For more secure TLS connections, we recommend disabling the weakest encryption algorithms.

You can choose either of the following methods to configure such connections.

> **NOTE**
> If any of the other applications installed on the server also use TLS, changes made to the configuration will affect them.

8.1 Configuring TLS connections through group policy objects (GPO)

1. Open the group policy editor (*gpedit.msc*),
2. Select **Computer configuration** > **Policies** > **Administrative templates > Network > SSL configuration settings**,
3. In the panel on the right, double-click on **SSL cipher suite order**,
4. The **SSL cipher suite order** window opens. Select the **Enabled** option.
5. In the **SSL cipher suites** field, paste the following value on a single line without spaces:
   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384
6. Deploy this configuration on the servers hosting the backend and SES Evolution agent handlers.

8.2 Configuring TLS connections via PowerShell script

1. Run the following PowerShell script on the servers hosting the backend and SES Evolution agent handlers with administrator privileges:

```
$AllowedSuites = `
'TLS_DHE_RSA_WITH_AES_128_GCM_SHA256', `
'TLS_DHE_RSA_WITH_AES_256_GCM_SHA384', `
'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256', `
'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256', `
'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384', `
'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384', `
'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256', `
'TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256', `
'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384', `
'TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384', `
'TLS_RSA_WITH_AES_128_CBC_SHA256', `
'TLS_RSA_WITH_AES_128_GCM_SHA256', `
'TLS_RSA_WITH_AES_256_CBC_SHA256', `
'TLS_RSA_WITH_AES_256_GCM_SHA384'

Get-TlsCipherSuite | foreach { $_.Name } | where { $AllowedSuites -notcontains $_ } | Disable-TlsCipherSuite
```

2. Restart the servers to apply the new configuration.

9. Further reading

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

STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.