GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

MIGRATION GUIDE
Version 2.7.1

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 version 2.7.1 migration guide.

This document contains all the information needed to migrate your environment from SES Evolution versions 2.6.x to versions 2.7.x.

You need to follow the step-by-step procedures described in this guide to ensure that you have a working SES Evolution solution after migration.

2. Requirements

To migrate to SES Evolution 2.7.1, you must meet at least the following prerequisites:

- SES Evolution 2.6.x must be installed on all backoffice components: agent handlers, backends and administration consoles.
- The following Runtimes in the latest version 8.0.x must be installed on machines hosting agent handlers. Use the links below to download version 8.0.11:
  - ASP.NET Core 8.0.x
  - Desktop Runtime .NET 8.0.x
- If you are using a firewall, its configuration must be updated to reflect the communication port changes made in version 2.7.1. For more information, see Configuring the firewall.
- You must have carefully read the SES Evolution 2.7.1 release notes

3. Configuring the firewall

SES Evolution 2.7.1 now uses the standard HTTPS port (443) between agents and agent handlers to facilitate deployment. You must prepare your new firewall configuration before installing SES Evolution 2.7.1.

3.1 Warning

You must maintain both the old and the new firewall configuration throughout the backoffice migration phase.
Only permanently delete the old firewall configuration once the migration is complete on all backoffice components: agent managers, backends, and administration consoles.

3.2 Updating the firewall configuration

SES Evolution version 2.7.1 brings the following changes to the communication ports:

- Port 443 is now used for agent communication with agent handlers,
- Port 8443 is now used by backends to communicate with administration consoles and agent handlers.

You should thus change your firewall rules using the table below. It details the ports used by components and the differences between SES Evolution versions 2.6 and 2.7.1. New features are shown in bold.

If you only have Windows Defender Firewall, some port changes are applied automatically by SES Evolution. For further information, see the Case of Windows Defender Firewall section.

SES EVOLUTION - MIGRATION GUIDE - V 2.7.1
3. CONFIGURING THE FIREWALL

Component	Direction	Port 2.6	Port 2.7 if backend and agent handler are installed on the same machine	Port 2.7 if backend and agent handler are installed on different machines	Purpose
Backend	incoming	TCP 443	**TCP 8443**	**TCP 443**	Communication with the administration console and the agent handler.
	incoming	TCP 10443	TCP 10443	TCP 10443	Public API.
	outgoing	TCP 443	TCP 443	TCP 443	Access to the Stormshield public policy update server
	outgoing	TCP 1433 (SQL) TCP 1434 (SQL) UDP 1434 (SQL)	TCP 1433 (SQL) TCP 1434 (SQL) UDP 1434 (SQL)	TCP 1433 (SQL) TCP 1434 (SQL) UDP 1434 (SQL)	Communication with the SQL Server database. These are the default ports, they can be modified when creating the instance.
Administration console	outgoing	TCP 443	**TCP 8443**	**TCP 443**	Communication with the backend.
Agent handler	outgoing	TCP 443	**TCP 8443**	**TCP 443**	Communication with the backend.
	outgoing	TCP 1468 UDP 514 TCP 5614	TCP 1468 UDP 514 TCP 5614	TCP 1468 UDP 514 TCP 5614	Communication with the Syslog server The ports used depend on the configuration of the agent handler groups in the administration console.
	incoming	TCP 17000	TCP 17000	TCP 17000	Communication with agents whose version is **lower than 2.7.1** over MSRPC.
	incoming	N/A	**TCP 443**	**TCP 443**	Communication with agents whose version is **2.7.1 or higher** over HTTPS.
Agent lower than 2.7.1	outgoing	TCP 17000	TCP 17000	17000	Communication with agent handlers
Agent greater than or equal to 2.7.1	outgoing	N/A	**TCP 443**	**TCP 443**	Communication with agent handlers

3.3 Case of Windows Defender Firewall

When installing backoffice components, SES Evolution automatically creates Windows Defender Firewall rules, regardless of whether it is enabled or not.

The rules created for version 2.7.1 are as follows:

3.3.1 If backend and agent handler are installed on different machines

Incoming rules

- On the machine hosting the agent handler:
  - *Stormshield Endpoint Security Evolution Agent Handler (TCP-In)* on port 17000 for communication with agents with a version **lower than 2.7.1** via EsServer over MSRPC.
  - *Stormshield Endpoint Security EvolutionAgent Handler (TCP-In)* on port 443 for communication with agents with version **2.7.1 or higher** via EsServer over HTTPS.

- On the machine hosting the backend:
  - *Stormshield Endpoint Security EvolutionBackend (TCP-In)* on port 443 for communication with consoles, and agent handlers as *system* users.
  - *Stormshield Endpoint Security EvolutionPublic API (TCP-In)* on port 10443 for communication with SIEM/SOAR as *system* user.

Outgoing rules

Installing SES Evolution does not create any outgoing Windows Defender Firewall rules.

If you filter outgoing connections, you must change your rules manually so that admin consoles and agent handlers can connect to backends on TCP port 8443.

3.3.2 If backend and agent handler are installed on the same machine

Incoming rules

- On the machine hosting the agent handler:
  - *Stormshield Endpoint Security Evolution Agent Handler (TCP-In)* on port 17000 for communication with agents with a version **lower than 2.7.1** via EsServer over MSRPC.
  - *Stormshield Endpoint Security EvolutionAgent Handler (TCP-In)* on port 443 for communication with agents with version **2.7.1 or higher** via EsServer over HTTPS.

- On the machine hosting the backend:
  - *Stormshield Endpoint Security EvolutionBackend (TCP-In)* on port 8443 for communication with consoles, and agent handlers as *system* users.
  - *Stormshield Endpoint Security EvolutionPublic API (TCP-In)* on port 10443 for communication with SIEM/SOAR as *system* user.

Outgoing rules

Installing SES Evolution does not create any outgoing Windows Defender Firewall rules.

If you filter outgoing connections, you must change your rules manually so that admin consoles and agent handlers can connect to backends on TCP port 8443.

4. Update SES Evolution backoffice to 2.7.1

1. Update the SES Evolutionbackoffice as described in the Update SES Evolution section of the SES Evolution installation guide.

2. Open the administration console. It automatically updates to 2.7.1 when it is started.
   The new 2.7.1 console has the following features:
   - A yellow banner indicates that the security policies no longer use the latest versions of the Stormshield rule sets.
   - A deployment request is pending in the **Security > Deployment** panel.

3. Click the **Deploy** button to update the environment.

4. In the **Backoffice > System** logs menu, check that there are no errors related to the migration.

5. In the **Environment > Agent logs** menu, check that there are no errors related to the migration.

6. Update the default security policies. This step can be performed immediately or later at your convenience. Be sure to:
   - Carefully read the Default Security Policy Release Notes *2506a* for changes to Stormshield security policies and rule sets.
   - Carefully read the SES Evolution 2.7.1 Release Notes, in particular the section Recommendations.

7. Click the **Deploy** button to update existing agents.
   The yellow banner is no longer displayed.

8. Once you have performed the migration of the backoffice and all agents to version 2.7.1, close port 17000 on agent handlers and agents.

5. Updating agents to 2.7.1

1. Update agents as described in the Update SES Evolution section of the SES Evolution installation guide.

2. Restart the machines when required by the procedure.

3. Once you have performed the migration of the backoffice and all agents to version 2.7.1, close port 17000 on agent handlers and agents.

6. Further reading

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

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