GUIDE
STORMSHIELD ENDPOINT SECURITY

ADMINISTRATION GUIDE
Version 7.2

Table of contents

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

Preface

Thanks!

Dear Client,

Thank you for choosing **Stormshield Endpoint Security** from Stormshield.

Our proven, award-winning Security Suite provides consistent, powerful, 360-degree protection, via a single agent installed on user workstations and managed from a central console.

With just a single agent, Stormshield Endpoint Security allows companies to protect their entire population of desktop and mobile workstations from known or unknown attacks, and theft of critical data, without disrupting user activity.

What is the target audience?

This documentation is intended for **System Administrators** who will deploy and manage the Stormshield Endpoint Security solution.

It contains all of the technical information necessary to install and operate the product on your system and network environment.

This technical documentation comes with Release Notes for the version of Stormshield Endpoint Security that you are using.

Contact

Should you need further information on our products or professional services, do not hesitate to:

- call us at +33 9 69 32 96 29

- send us an e-mail through our website http://www.stormshield.eu/.

1. Use environment

To use Stormshield Endpoint Security under the conditions of the Common Criteria evaluation and of the french qualification at standard level, it is essential to observe the following guidelines.

1.1 Recommendations on security watch

1. Regularly check the Stormshield products security advisories provided on https://advisories.stormshield.eu.
2. Always apply a software update if it contains a security breach correction. These updates are available on MyStormshield website.

1.2 Recommendations on keys and certificates

1. RSA keys of workstations and certification authorities must be a minimum size of 2048 bits, with a public exponent strictly greater than 65536, for a use not exceeding the year 2020.
2. For a use beyond the year 2020, the minimum size of an RSA key is 4096 bits.

1.3 Recommendations on algorithms

1. Stormshield Endpoint Security recommends using AES 256.

1.4 Recommendations on administrators

1. The security administrator responsible for defining the security policy of Stormshield Endpoint Security is considered as trusted.
2. The system administrator is also considered as trusted. He/She is responsible for the installation and maintenance of the application and workstation (operating system, protection software, desktop and engineering software, etc.). He/She applies the security policy defined by the security administrator.
3. The product user must respect the security policy in force in the company.

1.5 Recommendations on workstations

1. The workstation on which the SES agent is installed must be healthy. There must be an information system security policy whose requirements are met on the workstations. This policy shall verify the installed software is regularly updated and the system is protected against viruses and spyware or malware (firewall properly configured, antivirus updates, etc.).
2. At the installation of the agent, the SES server must be available so that the agent be able to download the security policy defined by the administrator. The installation shall take place on a trusted network environment such as a local network properly set up and protected by a firewall.
3. Access to administrative functions of the workstation system is restricted to system administrators only.

4. The operating system must manage the event logs generated by the product in accordance with the security policy of the company. It must for example restrict read access to these logs to only those explicitly permitted.

5. The local folder in which the SES agent is installed must not be shared with writing access on the network.

6. The user must ensure that a potential attacker can not see or access the workstation when it is started.

7. The user must ensure that the access to the workstation is not possible after shutdown during a few seconds.

1.6 Recommendations on administration workstations

The workstations on which the SES console and server and the database are installed must meet the following requirements:

1. These workstations are protected against virus and spyware.

2. Access to these workstations is restricted to administrators only (system administrator or database administrator).

3. Software installation and update must be supervised by the administrator.

4. Installed software is updated on a regular basis.

1.7 Certification and qualification environment

The features evaluated in the context of the EAL 3+ Common Criteria Certification and of the qualification of Stormshield Endpoint Security are:

1. Full disk encryption.

2. Encryption keys and recovery passwords drawing.

3. Security policy download from the SES server and the application of this policy.

4. Events logging and uploading to the SES server.

5. Disk recovery which allows modifying the password or decrypting an encrypted disk thanks to a support (CD, USB drive) created from the management console.

However the management console is beyond the evaluation scope.

2. Stormshield Endpoint Security Overview

In an ever more interconnected world, IT organizations have to introduce ever more complex security measures to face threats.

At present, there are few really satisfactory security solutions implemented on workstations. Security service providers mostly offer specialized solutions (hard disk encryption, antivirus, personal firewall).

Let us consider the examples of a firewall and an antivirus software which prove to be highly efficient against external threats. Their value, though, is limited when you install them on laptops located outside of your company's defense perimeter.
Security flaws can also be exploited when network analysis and filtering fail to identify or counter threats.

In order to protect and ease workstation security management, Stormshield Endpoint Security can rely on the workstation organization of your company's Active Directory if it has one.

ℹ NOTE
Stormshield Endpoint Security only reads the Active Directory's data. It does not modify them.

2.1 Concepts

Stormshield Endpoint Security's approach encompasses seven basic main concepts.

2.1.1 Concept 1: Integrated security

The Stormshield Endpoint Security solution provides, all through a **single** agent, consistent security policies that encompass:

- Users.
- System-level security.
- Data protection.
- Network connectivity.

2.1.2 Concept 2: Proactive protection

This concept provides security policies relying on intelligent behavior-based (**unknown** threats) and signature-based (**known** threats) technologies. This eliminates the need for IT teams to periodically check and update PCs for compliance and remove unauthorized applications.

Unfortunately, new types of attacks are launched every day. Security measures based on signatures which must know what the threat is before its identification and prevention, no longer provide sufficient protection against new variants of viruses or against the spread of new malicious software.

Besides, antivirus software is unable to block an attack targeted at a specific organization. These programmed stealth attacks never lead to a signature being issued since antivirus solution vendors remain unaware of them.

Should a virus succeed in installing itself on a workstation, its operation will be neutralized by Stormshield Endpoint Security until the time when an antivirus signature becomes available to completely clean the workstation.

2.1.3 Concept 3: Adaptive control

This concept offers security and user control policies that change dynamically depending on the level of risk associated with the use of the endpoint (workstation, laptop, PDA, etc.) or the **environment** (WiFi).

For example, applications installed directly by users for personal use may present both a security threat and a source of lost productivity. Stormshield Endpoint Security provides the tools to apply different levels of control over how any individual or group may use their workstations.

2.1.4 Concept 4: Flexible policy control

This concept gives IT the ability to secure endpoints through both quickly deployed **automatic protections** built into the security suite and fine-grained, customizable **configurations** that address your organization's specific security and policy requirements.

2.1.5 Concept 5: Application of policies based on the organization's directory

To ease configuration and administration of workstation security, Stormshield Endpoint Security relies on the existing organization's Active Directory or on an internal directory. Policies defined in Stormshield Endpoint Security are applied to Active Directory objects or to agents groups of the internal directory. Active Directory objects can be organizational units, computer groups, or single computers.

2.1.6 Concept 6: Information feedback

Stormshield Endpoint Security provides a wide range of information on dangerous or suspect operations affecting the client workstation. This information forms an essential complement to the data from the network monitoring systems in the context of overall IT system protection.

2.1.7 Concept 7: Data encryption

To help you protect your systems and data, Stormshield Endpoint Security provides a combination of **full-disk** encryption before booting and **file** encryption after booting.
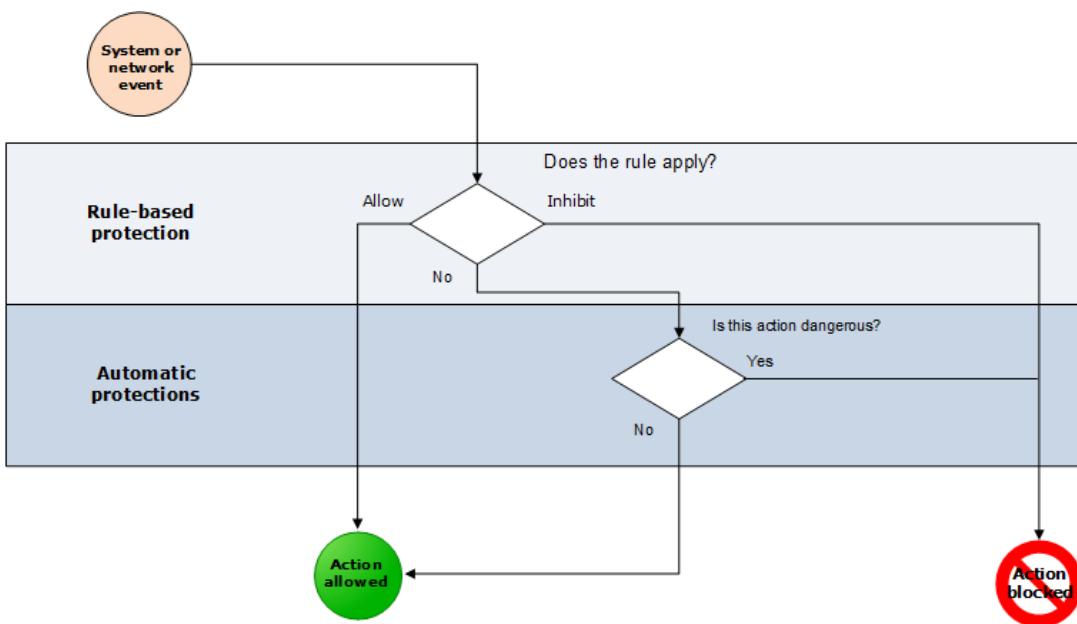
Your data is protected at all time, regardless of the workstation user. The encryption policy which is managed from a centralized console, can be applied to:

- Any user.
- Any workstation.
- The whole hard disk.
- Removable devices.
- Specific files/folders.

2.2 Protection mechanisms

Stormshield Endpoint Security includes two protection mechanisms to provide the highest possible level of workstation security:

- Rule-based protection.
- Automatic protections.

2.2.1 Rule-based protection

Rule-based protection is used to define and ensure the application of a security policy on points which are considered sensitive by the client. A security policy contains the formal rules set out to allow or ban access to the following:

- Application execution.
- Firewall network rules.
- Resource usage rules (network, files, register base) for each application.
- Usage rights on file types (depending on their extensions).
- Usage rights on mass storage devices.
- Trusted applications (which can override part or all of Stormshield Endpoint Security restrictions).

An explicit security policy can be applied to different workstation groups.

Stormshield Endpoint Security is supplied with predefined rules so that policies can be applied immediately by the administrator. These default rules may be modified at any time to adapt policies to company's requirements.

2.2.2 Automatic protections

Automatic protections are designed to detect and block **known** and **unknown** malicious codes using attack pattern identification instead of code identification.

Automatic protections do not require any configuring by the administrator. The administrator can, however, adjust these mechanisms to specify the level of how Stormshield Endpoint Security reacts to different events. For more information, see Configuring automatic protections.

Two major categories of automatic protection mechanisms are built into Stormshield Endpoint Security:

- The first category covers application and system activities.
  This serves to protect the workstation against attempts to corrupt executable files and access sensitive system services or data.

- The second category comprises an Intrusion Detection System (IDS) so that the workstation can protect itself from attacks from the network.
The mechanisms applied for detecting system or network attacks by the automatic protection system remain active on a permanent basis. Stormshield Endpoint Security's treatment of these events can be controlled by the administrator. Depending on the type of event that occurs, the system will send an alert or apply automatic counter measures as defined by the administrator.

2.3 Architecture

Stormshield Endpoint Security is a distributed protection system that covers all of the workstations belonging to an organization.

Its architecture is based on a multi-tier model and on deployment techniques that allow it to be quickly integrated into the organization's Active Directory if the company uses one.

2.3.1 Concepts

Inter-component communication

Communications between all components are authenticated and encrypted using TLS v1 and X509 v3 certificates. Mutual authentication is used between every component to reinforce solution security.

Workstation protection

Each workstation is protected by a software module called *Stormshield Endpoint Security Agent*.

The agent communicates with the deployment server, whose role is to distribute security policies to each agent and collect data concerning workstation security from them.

This data is stored by the server in a dedicated database which can also be accessed by the Stormshield Endpoint Security management console (management console).

Scalability and high availability

Stormshield Endpoint Security responds to the scalability and high availability requirements of the most demanding business environments.
High availability is based on load balancing and failover mechanisms, distributed over a number of deployment servers.
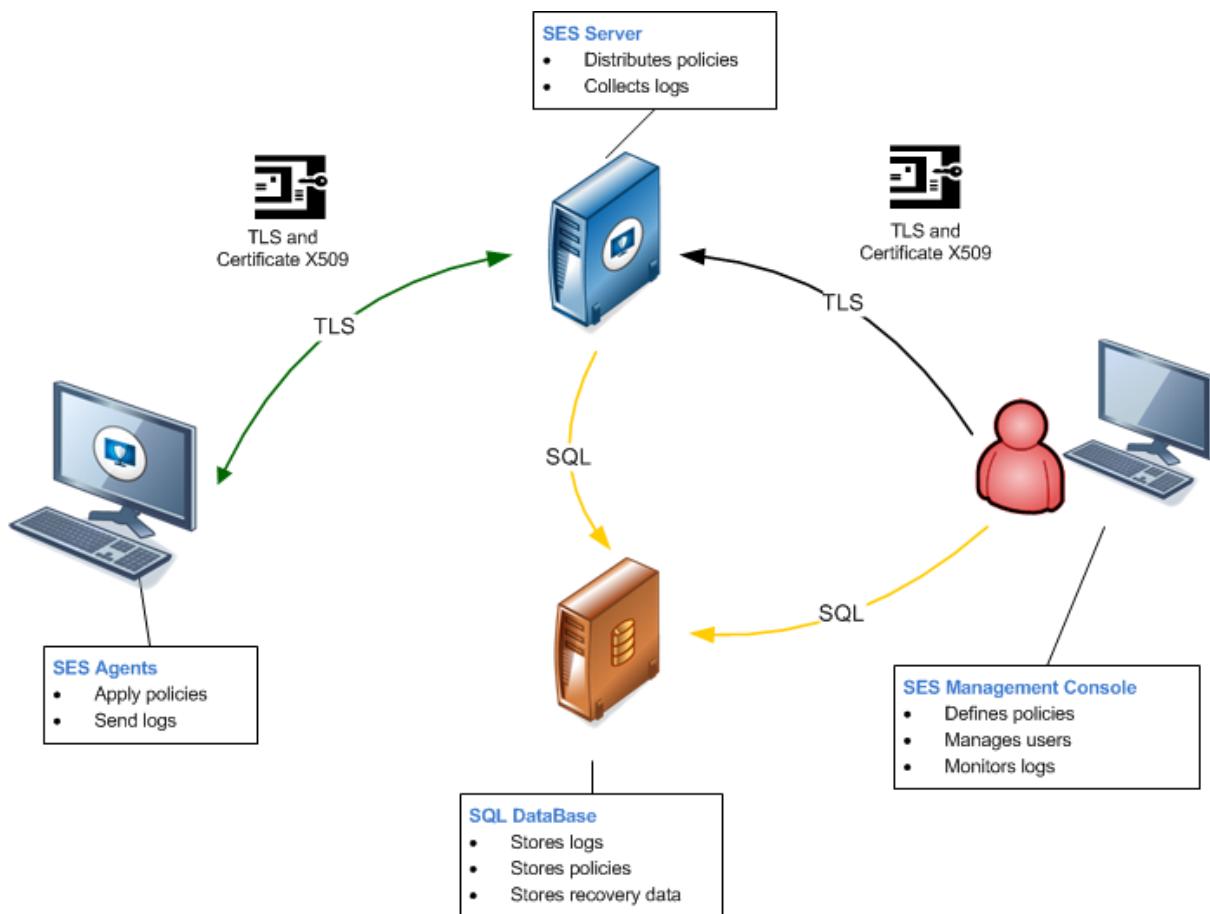
For more information, see section .

2.3.2 Stormshield Endpoint Security components

Stormshield Endpoint Security is made up of the following components:

- The Stormshield Endpoint Security server.
- SQL databases.
- The management console.
- The Stormshield Endpoint Security agents.

Stormshield Endpoint Security Server

The server is used to distribute security policies and collect logs.

Any Stormshield Endpoint Security agent deployment requires at least one deployment server. There must be at least one server at each geographical site.

After being installed, additional servers can be added from the **Servers** panel. They can be used as failover backups and for load distribution.

Policies and configurations information and their application to the Active Directory are shared by all servers.

In the case of an environment based on an internal directory, policies and configurations information and their application to the agents groups are only shared by servers assigned to one internal directory.

The management console communicates with all available servers. The console sends configurations to the servers only if they are not up-to-date. It also detects certificates inconsistencies between servers of an environment.

If a server is down when the console sends information, it will not be updated. It will be updated during the next application of changes to the environment performed from the console, if the connection is restored between the console and the server primary IP address.
The **Servers** panel displays information about the servers update statuses.

Several IP addresses can be defined for one server. The console updates the server via the main IP address defined in the console. Communication between the agents and the server is performed via the other IP addresses defined in the console. This mechanism presents a
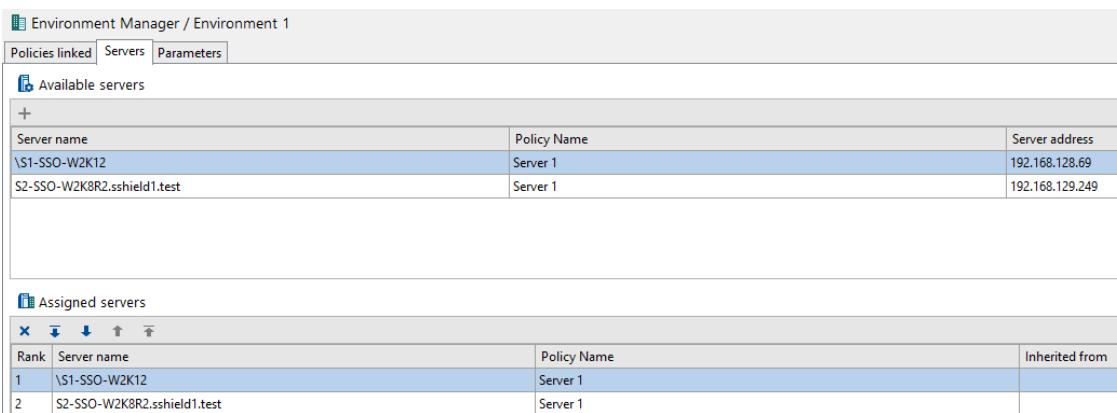
specific interest if the workstations on which the agent is installed are out of the company network.

Server load balancing

In the *Server* tab of each organizational unit (OU) or agents group, you can define a list of servers to share the load.

Each time a configuration is deployed, agents receive IP addresses of servers which they can access. When an agent tries to connect to a server to check whether new configurations are available and to upload the latest logs, by default it connects to the most recent server it connected to. If the server is overloaded or does not answer, a message is sent to the agent to request that it connects to another server defined on the hierarchically closest OU or in the agents group.

A server is regarded as overloaded when the number of assigned agents has reached the maximum. A global server must always be defined. It is the server assigned to the first rank of each main node of the directory (domain root for an Active Directory or default group for an internal directory). By default, the global server is the first server installed.

Environment Manager / Environment 1		
Policies linked Servers Parameters		
Available servers		
+		
Server name	Policy Name	Server address
\S1-SSO-W2K12	Server 1	192.168.128.69
S2-SSO-W2K8R2.sshield1.test	Server 1	192.168.129.249

Assigned servers		
× ⤓ ↓ ↑ ⤒		
Rank	Server name	Policy Name	Inherited from
1	\S1-SSO-W2K12	Server 1	
2	S2-SSO-W2K8R2.sshield1.test	Server 1	

Failover to another server

The agent tries to connect to the first server in the list of assigned servers. If the server does not answer, it tries to connect to the following server in the list and so on, until it finds a responding server. The agent thus communicates with the first available server. If no server is available, it connects to the global server.

SQL databases

Databases allow storing different elements:

- The "srkey" database stores all encryption information, which can be related to full-disk or file encryption, or to exchanges between modules.
- The "stormshield" database stores logs collected by agents.
- The "stormshield3" database stores the management console configuration, including policies, scripts and files to be dispatched to agents.
- The "urd" database stores all data related to agents status monitoring.

In case of backup and restore, the Stormshield Endpoint Security environment only needs the "srkey" and "stormshield3" databases content to work properly.

A single database server can be assigned to several Stormshield Endpoint Security consoles (if necessary).

Management console

The management console is used to:

- Define policies and configurations.
- Monitor logs sent by Stormshield Endpoint Security agents.
- Manage console users.

The **features** of the management console depend on the license of your organization.
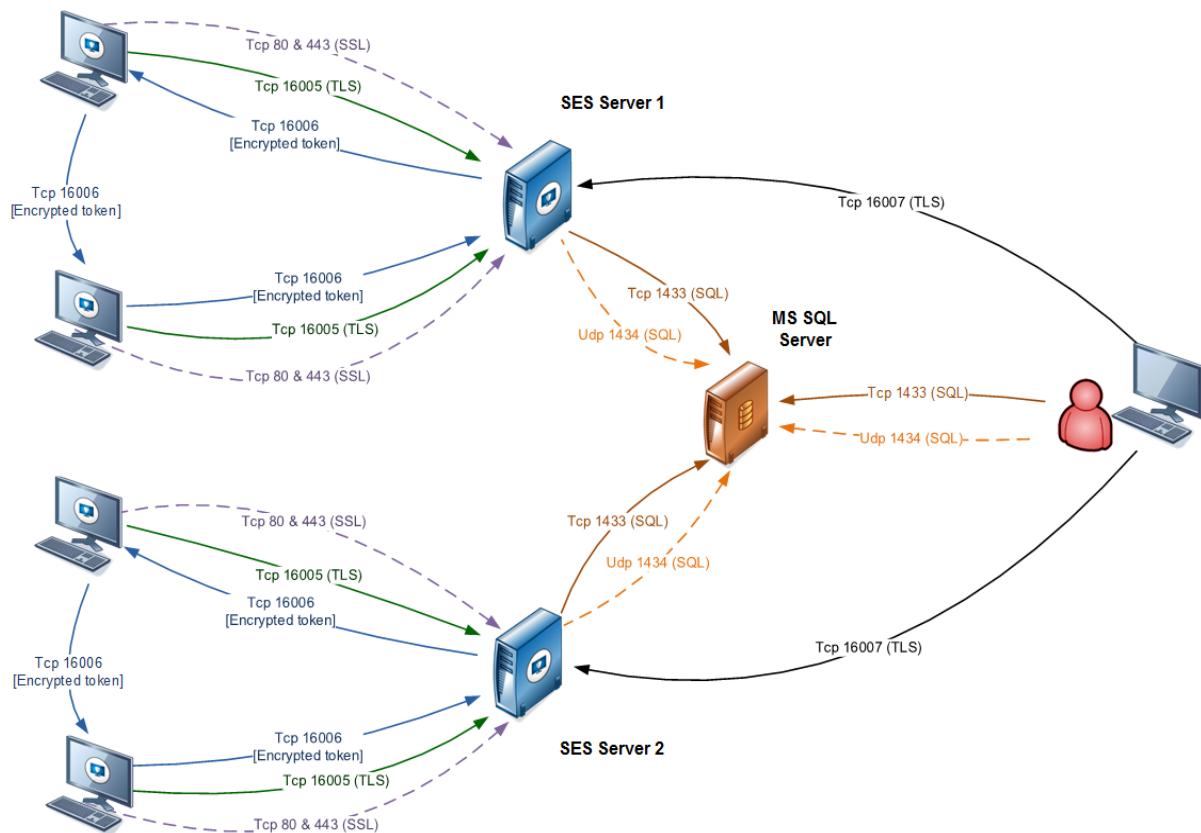
For more information, see the section Packages and licenses.

Stormshield Endpoint Security Agent

The agents installed on your workstations are used to apply security policies and send logs to the Stormshield Endpoint Security server.

Communication ports between components

The following diagram shows communications ports used between the various components of Stormshield Endpoint Security:

Note: if SES servers have been previously referenced and if the required flows have been authorized, each agent will then be able to communicate with both servers.

2.4 Packages and licenses

2.4.1 Packages

Stormshield Endpoint Security is available in **three packages,** each offering features adapted to your needs:

- Stormshield Endpoint Security Professional Edition.
- Stormshield Endpoint Security Secure Edition.
- Stormshield Endpoint Security Server-Side Edition.

Stormshield Endpoint Security packages exist in the following versions:

Stormshield Endpoint Security packages	32-bit version	64-bit version
Professional Edition	✓	✓
Secure Edition	✓	✓
Server-Side Edition	✓	✓

Each package requires a license. This license applies to a specific environment.

The following table describes the Stormshield Endpoint Security features offered in each package.

Stormshield Endpoint Security features	Professional Edition (32 bits)	Professional Edition (64 bits)	Secure Edition (32 bits)	Secure Edition (64 bits)	Server-Side Edition
Security Policies					
System Behavior	✓	✓	✓	✓	✓
Kernel Components	✓	✗	✓	✗	✗
Device Control	✓	✓	✓	✓	✓
Removable Devices	✓	✓	✓	✓	✓
Network Security Control	✓	✓	✓	✓	✓
Network Firewall	✓	✓	✓	✓	✓
WiFi Access Points	✓	✓	✓	✓	✓
Application Rules	✓	✓	✓	✓	✓
Extensions	✓	✓	✓	✓	✓
Trusted applications	✓	✓	✓	✓	✓
Agent Configurations					
Agent Configuration	✓	✓	✓	✓	✓
Temporary web access	✓	✓	✓	✓	✓
Challenges	✓	✓	✓	✓	✓
Scripts					
Scripts	✓	✓	✓	✓	✓
Script Resources					
Tests	✓	✓	✓	✓	✓
Actions	✓	✓	✓	✓	✓
Encryption Policies					
Full disk encryption	✗	✗	✓	✓	✗

Stormshield Endpoint Security features	Professional Edition (32 bits)	Professional Edition (64 bits)	Secure Edition (32 bits)	Secure Edition (64 bits)	Server-Side Edition
File encryption	✗	✗	✓	✓	✗

Stormshield Endpoint SecurityProfessional Edition

The Stormshield Endpoint Security Professional Edition package includes three features:

- Security policies.
- Configurations.
- Scripts.

"Security policies" feature

This feature enables the administrator to apply specific controls to the Stormshield Endpoint Security agents (via the server).

"Configurations" feature

This feature enables the administrator to apply policies and configurations that change dynamically.

"Scripts" and "Script resources" feature

This feature enables the administrator to write customized scripts in order to define conditions under which policies and configurations are applied.

Stormshield Endpoint Security Secure Edition

The Stormshield Endpoint Security Secure Edition package includes the three Stormshield Endpoint Security Professional Edition features as well as the "Encryption Policies" feature.

"Encryption policies" feature

This additional feature enables the administrator to create encryption policies for local hard disks and files.

Stormshield Endpoint Security Server-Side Edition

The Stormshield Endpoint Security Server-Side Edition package is meant for servers running on these operation systems:

- Windows Server 2003 SP2 32 bits.
- Windows Server 2003 R2 SP2 32 bits.
- Windows Server 2008 R2 64 bits
- Windows Server 2012 R2 64 bits

> 🛑 WARNING
> The Stormshield Endpoint Security server and the Stormshield Endpoint Security agent must not be installed on the same workstation.

The Stormshield Endpoint Security Server-Side Edition package includes the 64-bit Stormshield Endpoint Security Professional Edition's features.

⚠️ **WARNING**

The Stormshield Endpoint SecurityServer-Side Edition package is not compatible with the **Server Core** installation option in Windows Server 2008 R2.

For more information, refer to the table Stormshield Endpoint Security features.

2.4.2 Licenses

Updating your licenses
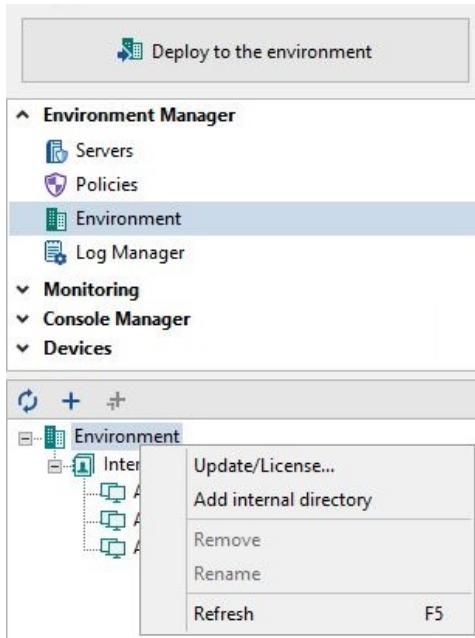
A license is dedicated to a specific environment. It can only be applied to this environment.

The new license file shows the total number of licenses.

Applying a license to an environment

To update and apply a license to an environment, follow the steps below:
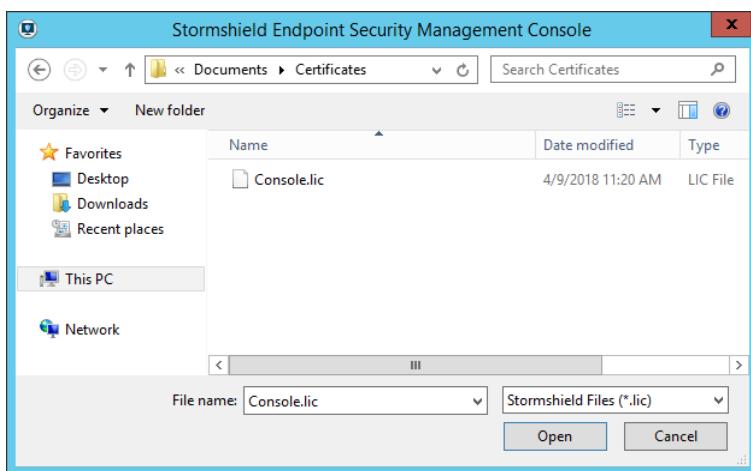
1. Right-click the environment and select **Update/License** from the menu.

2. To update the Stormshield Endpoint Security license, select **Update**.

3. Select the Stormshield Endpoint Security license and click **Open**.

ℹ️ **NOTE**
If the updated license **lacks features** supported by the old license, Stormshield Endpoint Security will warn you that you may lose information.
If you click **Yes**, information will indeed be lost.
Example: Applying a license that loses the encryption feature.

ℹ️ **NOTE**
If you have a **limited license for evaluation purposes**, you will have a demo version of the management console. An expiry date is displayed on the **License information** window available by right-clicking the environment and selecting **Update/License**.

The following window is displayed.

4. Click **OK** to complete the update.

Information on licenses

To obtain information on your licenses, follow the steps below:
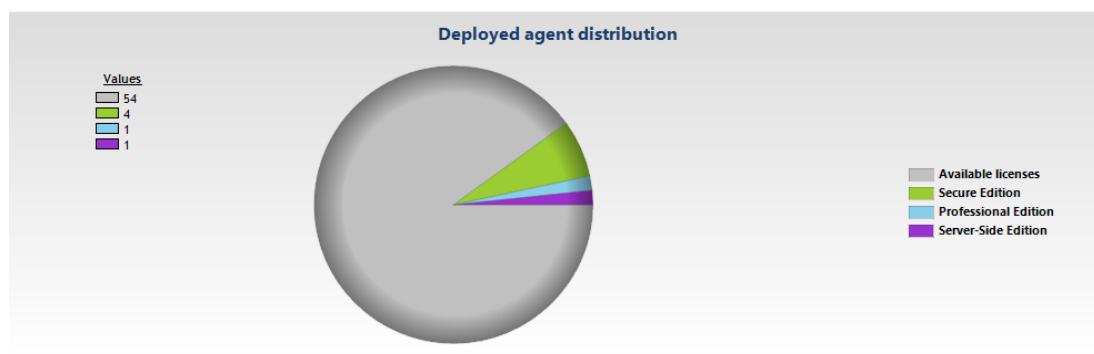
1. Click **Reports** in the **Monitoring** section.

2. Select **Licenses** in the **Reports** drop-down menu.

   A report is displayed showing:
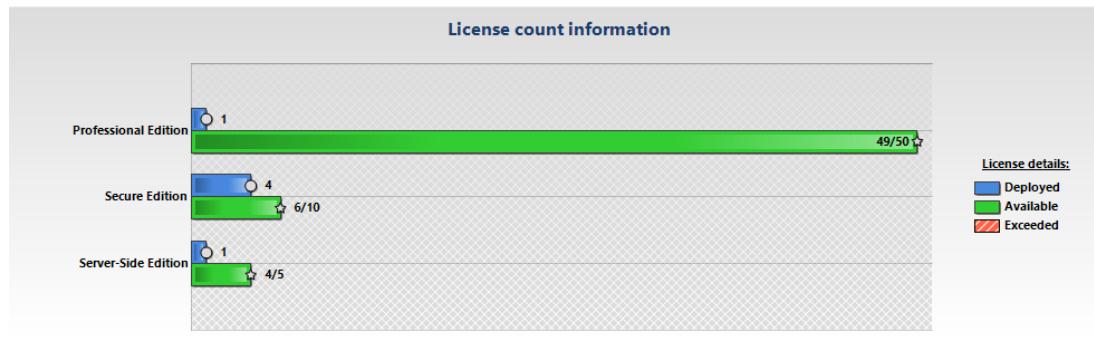
   ◦ The **Date** of the license report.

   ◦ The **Deployed agent distribution** and the number of licenses which are still available.

   ◦ **License count information**:

      - Deployed.

      - Available.

      - Exceeded.

If you have exceeded the number of deployed agents, a warning window pops up. You will have to wait a few seconds before using it. To sort this situation out, you must remove some (obsolete) agents in the **Agents** menu. You can also contact your sales representative to extend the current license. For more information on removing obsolete agents, refer to Agent monitoring.

3. If you want to save the license report, click the icon ⬆ Save Report .

   The report is saved to the location specified, in the `.png` format.

3. Stormshield Endpoint Security Installation and Uninstallation

3.1 Downloading the Stormshield Endpoint Security software

3.1.1 Downloading from the client area

Stormshield products are distributed via our MyStormshield client area.

In this area, you will be able to look up and download:

- the product's various software versions and patches,
- associated documentation (User guides and Release notes),
- hashes of installation packages in order to verify their authenticity,
- your *.lic* license file,
- security alerts,
- frequently asked questions.

Once you have placed your order for Stormshield, you will receive via e-mail a bill of delivery containing the serial number of your software license.

If you do not already have an account in the client area, you will need to create one:

1. In your browser, go to MyStormshield.
2. Click on **Create a new profile**.
3. Fill out the various fields.
4. Under the section **Register your first product**, enter the serial number indicated in the bill of delivery.

If you already have an account, log on to this account and register the serial number.

Once you have registered the serial number, you will be able to download the associated *.lic* license file needed for installing the product.

3.1.2 Checking software authenticity

Stormshield Endpoint Security is available in the form of an archive. In order to verify the authenticity of this package:

1. Calculate its SHA-256 hash using a tool of your choice.
2. Check that this hash is indeed the same as the one indicated in the client area.

Executable files can also be checked using their digital signatures:

1. In the explorer, right-click on the *.exe* file and select **Properties.**
2. Click on **Digital signatures** and select the "Stormshield" row.
3. Click on **Details**.

3.2 System prerequisites for Stormshield Endpoint Security under Windows

3.2.1 Active Directory prerequisites

To use the Active Directory option, you must meet the following requirements:

- All Stormshield Endpoint Security agents must be installed on workstations belonging to the same Active Directory forest. Stormshield Endpoint Security servers may not necessarily belong to the same forest of the Active Directory.
- Stormshield Endpoint Security 7.2 supports Active Directory on MS Server 2008 R2 and MS Server 2012 R2.
- Workstations must belong to an Organizational Unit (OU). Sub-domains are not supported, i.e. domains must all be at the same level.
- Stormshield Endpoint Security 7.2 runs with LDAP SASL, which communicates with TCP port 3268 and TCP/UDP port 389. It is not compatible with LDAP SSL/TLS.

3.2.2 Stormshield Endpoint Security server prerequisites

To install and use Stormshield Endpoint SecurityVersion 7.2 under Windows, you must at least satisfy the following **Server** environment prerequisites:

- Dual-core processor: 2 GHz.
- Memory: 2 GB minimum.
- Hard disk space: 1 GB minimum.
- Operating systems:
  - Windows Server 2008 R2 64 bits, with updates KB4474419 and KB4490628
  - Windows Server 2012 R2 64 bits
  - Windows Server 2016 (64 bits)
  - Windows Server 2019 (64 bits)
  - Windows Server 2022 (64 bits)
- Static IP address of the machine where the server is installed.
- Incoming communication (Stormshield Endpoint Security server):
  - TCP port 16004.
  - TCP port 16005.
  - TCP port 16006.
  - TCP port 16007.
- Outgoing communication (Stormshield Endpoint Security server):
  - TCP port 80.
  - TCP port 1433 (customizable).
  - UDP port 1434 (customizable).
- Incoming communication (Web server):
  - TCP port 80 (customizable).
  - TCP port 443 (customizable).

  You will have to choose other ports if they are already used by a Web server installed on the server machine.

TCP ports 80 and 443 will be used by the Web server to deploy the agents installed with the server.

Prerequisites for a system managing a large number of agents

- Operating systems: Windows 2008 R2 64 bits, Windows 2012 R2 64 bits, Windows Server 2016 and Windows Server 2019.
- RAM: 16 GB.
- Between 8 and 16 cores at 3 GHz or more.
- One 1 Gb/s Ethernet network adapter for links with agents.
- One 1 Gb/s Ethernet network adapter for links with the logs SQL server.
- The SQL server and Stormshield Endpoint Security must be close to each other (bandwidth of 1 Gb/s and ping time lower than 2 ms).

SQL servers and Stormshield Endpoint Security can be executed on the same machine. In this case, we recommend applying the more effective configuration for each prerequisite.

Number of agents per server according to the quantity of logs

The number of agents a server can support strongly depends on three criteria:

- The connection time of agents to the server.
- The amount of logs an agent will send. This amount depends on the policies applied to agents.
- The type of network. The LAN network is a 1 Gb/s Ethernet network. The WAN network is a broadband network (fiber or similar) for the server side and standard ADSL for the agents side. Agents are located on several sites.

The following table is a summary of our recommendations:

Number of logs per agent	Connection time	Type of network	Number of connected agents per server
5 GB/year	5 min	LAN	600
5 GB/year	10 min	LAN	700
5 GB/year	5 to 10 min	WAN	500
1.5 GB/year	5 min	LAN/WAN	2500
1.5 GB/year	10 min	LAN/WAN	2700
100 MB/year	10 to 30 min	LAN/WAN	7500
2 MB/year	10 min	LAN	15000
2 MB/year	10 min	WAN	9000
2 MB/year	1 h	LAN	50000
2 MB/year	1 h	WAN	45000
0.3 MB/year	10 min	LAN	15000
0.3 MB/year	10 min	WAN	8000
0.3 MB/year	1 h	LAN	75000
0.3 MB/year	1 h	WAN	50000

3.2.3 Stormshield Endpoint Security database prerequisites

To install and use Stormshield Endpoint Security Version 7.2 under Microsoft Windows, you must satisfy the following **Database environment** prerequisites:

- Operating system: any Windows release compatible with MS SQL Server 2012, MS SQL Server 2014, MS SQL Server 2016, MS SQL Server 2017, MS SQL Server 2019 and MS SQL Server 2022.

- Communication with the Stormshield Endpoint Security server and the console:

  - **TCP port 1433**

  - **TCP dynamic port** defined in:

    ```
    SQL Server Network Configuration > Protocols for [instance de la
    base de données] > TCP/IP > Propriétés > IP Addresses > IPAll >
    TCP Dynamic Port.
    ```

    For more information, refer to Changing the TCP port for MS SQL Server 2012 2014, 2016, 2017, 2019 or 2022.

  - **UDP port** 1434.

- **RAM**: 2 GB minimum.

  A 64-bit operating system (Windows 2008 R2, Windows 2012 R2, Windows Server 2016 or Windows Server 2019) is recommended for a server managing a large number of agents.

- **Hard disk space**: ~ 10 MB for the initialized Stormshield Endpoint Security database (excluding the SQL engine), and an additional space to be determined depending on the security policies.

  Additional hard disk space is required for the following:

  - Log database: 100 MB per agent for one year.

  - Identification database: 1 MB per agent.

  - Encryption key database: 1 MB per agent.

    ⓘ NOTE
    Use information only as an estimate for disk space requirements. Disk space requirements strongly depend on the security policies implemented and log settings. The average log policies usually generate from 1 MB per year and per agent to 5 GB per year and per agent. Disk space required also depends on the log retention period.

MS SQL Server 2012 Express Edition is supplied with Stormshield Endpoint Securityand can be installed directly using the Stormshield Endpoint Security installation tools. This version of the server requires the following minimal configuration:

- Windows Server 2008 R2.

- 64-bit systems.

- A workstation with a processor Intel or compatible at 1 GHz or more (2 GHz recommended as a minimum).

- RAM: Minimum 512 MB (4 GB recommended as a minimum).

- Available disk space: 6 GB.

- Microsoft .NET Framework n.n.n (installed during the installation procedure of MS SQL Server 2012 Express Edition if necessary).

🛈 NOTE

When installing the database, use the **Mixed Mode** authentication mode.

⚠ WARNING

You must use **Case-Insensitive** collations in MS SQL Server 2012, 2014, 2016, 2017 or 2019 otherwise the scripts necessary to install the Stormshield Endpoint Security database will not be supported.

⚠ WARNING

MS SQL Server 2012 Express Edition provided with Stormshield Endpoint Security is limited to 4 GB of data per database, which corresponds to 9 million logs.

If manually installing the SQL server:

- you need to enable the automatic start of the SQL Server Browser service. This service must be started when installing SES to allow the administrator to complete the step of connection to the database.

- you need to install the SES database with a Windows account with sysadmin rights or with an MSSQL account with the sysadmin rights on the SQL instance on which SES will be installed.

Prerequisites for a system managing a large number of agents

- Operating systems: Windows 2008 R2 64 bits, Windows 2012 R2 64 bits, Windows Server 2016, Windows Server 2019 and Windows Server 2022.

- SQL 2012 64-bit version, SQL 2014 64-bit version, SQL 2016, SQL 2017, SQL 2019 or SQL 2022 (standard or enterprise).

- RAM: 16 to 32 GB.

- Between 8 and 16 cores at 3 GHz or more.

- One 1 Gb/s Ethernet network adapter for links with the Stormshield Endpoint Securityserver.

- The SQL server and Stormshield Endpoint Security must be close to each other (bandwidth of 1 Gb/s and ping time lower than 2 ms).

- SSD disks can be useful but need to be properly set up (refer to the Microsoft documentation about using SQL Server on SSD disks).

- The SQL Server license must match the number of cores of the workstation.

Stormshield Endpoint Security makes the most out of the features in SQL Server 2012 and higher to optimize performance. Configurations based on a previous version or express edition of MS SQL Server are less optimized.
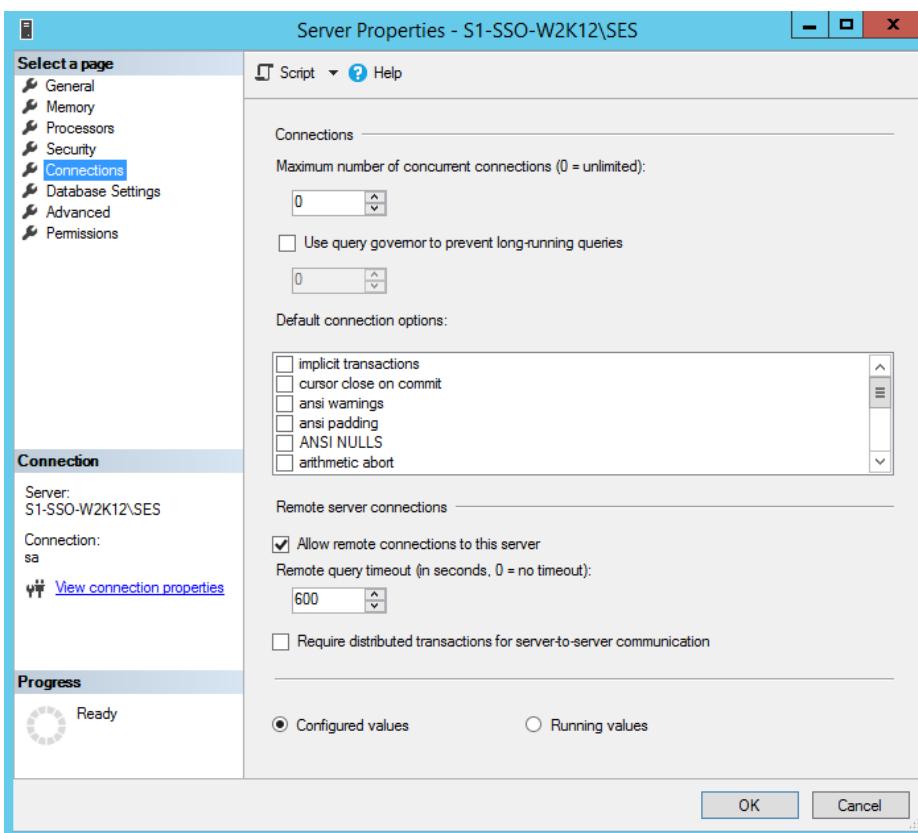
Each time it starts, the Stormshield Endpoint Security server detects the configuration of the SQL server. If you change the configuration of the SQL server (connection to a new base or hardware modification), we recommend that you restart the Stormshield Endpoint Securityserver.

Using an existing database

A mixed (NT and SQL) authentication mode and TCP connectivity are required.

Changing connection parameters to MS SQL Server 2012, 2014, 2016, 2017, 2019 or 2022
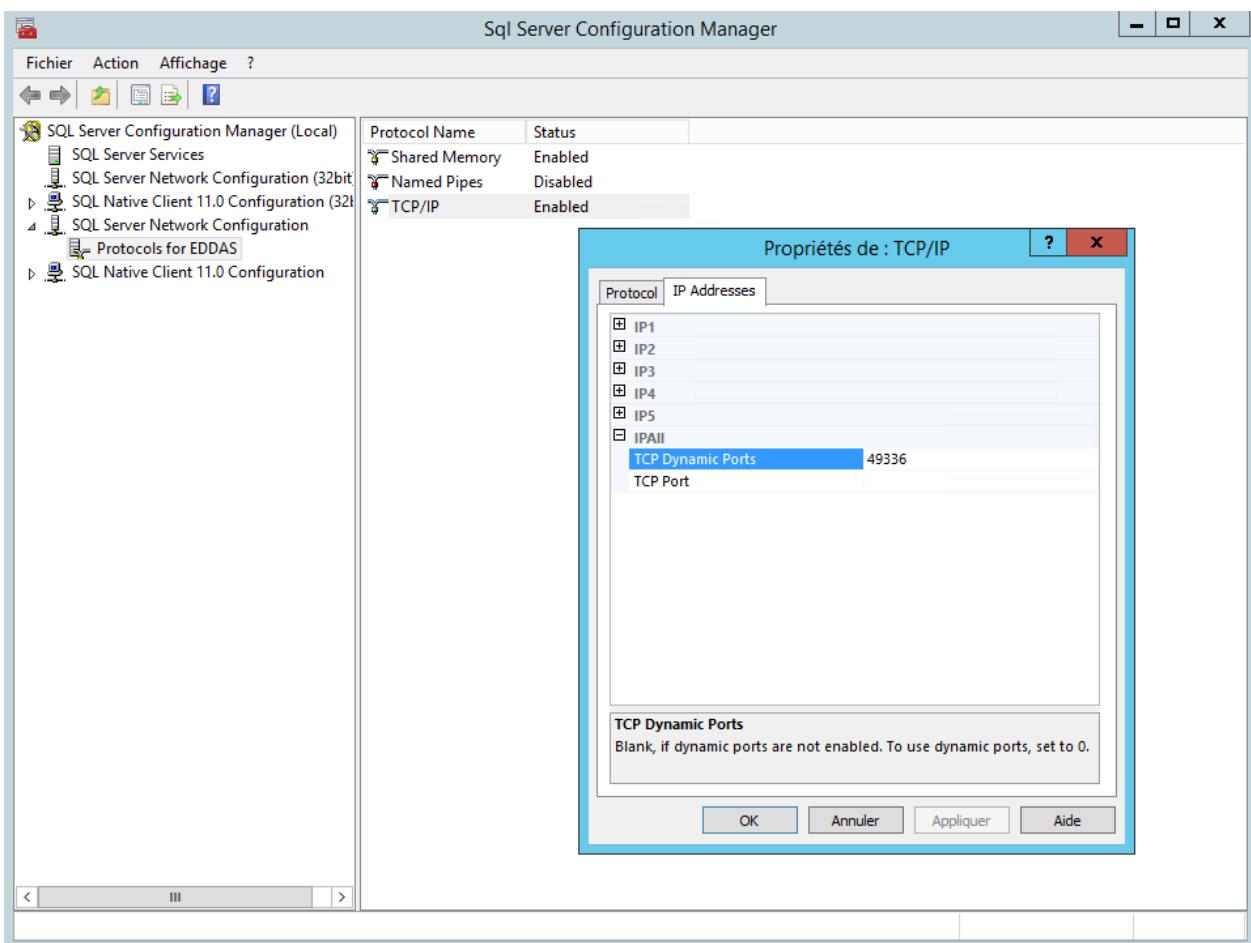
To change connection parameters (local or remote access) to MS SQL Server, use **Microsoft SQL Server Management Studio**.

Changing the TCP port for MS SQL Server 2012 2014, 2016, 2017, 2019 or 2022

To change the TCP port number assigned to the database instance, use **SQL Server Configuration Manager** in:

```
SQL Server Network Configuration > Protocols for [instance de la
base de données] > TCP/IP > Propriétés > IP Addresses > IPAll > TCP
Dynamic Ports
```

Using the embedded database

Check on the target machine that there is no database instance having the same name than the database to be installed (SES). For this purpose, make sure that the list of services in the control panel does not include the **SQL SERVER (SES)** service.

If a "SES" SQL Server instance already exists, the installation of MS SQL Server 2012 will not be proposed.

3.2.4 Management console prerequisites

To use the management console, you must satisfy the following prerequisites:

- Single-core processor: 2 GHz minimum.
- RAM: 512 MB.
- Hard disk space: 75 MB.
- Operating systems:

Operating system	32-bit version	64-bit version
Windows 7 SP1, with updates KB4474419 and KB4490628	✓	✓
Windows 8.1 Update 1	✓	✓
Windows 10	✓	✓

Operating system	32-bit version	64-bit version
Windows Server 2008 R2, with updates KB4474419 and KB4490628	N/A	✓
Windows Server 2012 R2	N/A	✓
Windows Server 2016	N/A	✓
Windows Server 2019	N/A	✓
Windows Server 2022	N/A	✓

.NET Framework n.n.n, installed during the installation procedure of the Stormshield Endpoint Security management console.

> ⓘ **WARNING**
> Make sure you always have the latest update of the .NET Framework.

- Microsoft Visual C++ 2008 Redistributable.
- Static IP address of the machine where the first server is installed.
- IP address or name of the machine where the database is installed.
- Outgoing communication:
  - TCP port 16007.
  - UDP port 1434.
  - TCP port 1433.
- Password of the database system administrator account.

3.2.5 Stormshield Endpoint Security agent prerequisites

To use the Stormshield Endpoint Security agent, you must satisfy the following prerequisites:

- Single-core processor: 2 GHz.
- RAM: 512 MB (minimum), 1 GB (recommended).
- Hard disk space: 30 MB (100 MB with agent logs).
- Operating systems:

Windows version	Professional Edition	Secure Edition	Server-Side Edition
Windows XP SP3- 32 bits	✓	✓	-
Windows 7 SP1 - 32/64 bits, with updates KB4474419 and KB4490628	✓	✓	-
Windows Embedded Standard - 32 bits	✓	✓	-
Windows 8.1 Update 1- 32/64 bits	✓	✓	-
Windows 10 Enterprise 2015 LTSB - 32/64 bits	✓	✓	-
Windows 10 Enterprise 2016 LTSB - 32/64 bits	✓	✓	-

Windows version	Professional Edition	Secure Edition	Server-Side Edition
Windows 10 2019 LTSC - 32/64 bits	✓	✓	
Windows 10 20H2- 32/64 bits	✓	✓	-
Windows 10 21H1- 32/64 bits	✓	✓	
Windows 10 21H2- 32/ 64 bits	✓	✓	
Windows 10 22H2 - 32/64 bits	✓	✓	
Windows Server 2003 SP2 - 32 bits	-	-	✓
Windows Server 2003 R2 SP2- 32 bits	-	-	✓
Windows Server 2008 R2 - 64 bits, with updates KB4474419 and KB4490628	-	-	✓
Windows Server 2012 R2 - 64 bits	-	-	✓

- Secure Boot:
  Stormshield Endpoint Security is not compatible with Secure Boot under Windows 8.1. If you have a UEFI compatible system, you should disable Secure Boot. Options such as Device Guard and Credential Guard, which need Secure Boot as a prerequisite, cannot be used with Stormshield Endpoint Security.
  Under Windows 10, Stormshield Endpoint Security is compatible with Secure Boot as well as with Device Guard and Credential Guard, except the option Hypervisor Code Integrity (HVCI).

- GINA (*Graphical Identification and Authentication*) :
  If your company uses a strong authentication system based on a `gina` DLL, you must install the authentication product before installing Stormshield Endpoint Security. When you need to uninstall the authentication product, you must first uninstall Stormshield Endpoint Security. Stormshield Endpoint Securitysaves the existing `gina.dll` location upon installation, and will restore it upon uninstallation.

  ### 🛈 NOTE
  The remark on the `gina` DLL only applies to **Windows XP** environments.

- Outgoing communications between the Stormshield Endpoint Security agent and server:
  - TCP port 16004.
  - TCP port 16005.
  - TCP port 16006.
  - TCP port 443 (customizable).
  - TCP port 80 (customizable).
  - TCP port 7080.

  ### 🛈 NOTE
  TCP ports 16004, 16005 and 16006 are reserved for the Stormshield Endpoint Security agent. When testing agent/server communication, the agent will block any communication software from using these ports (example: telnet).

- Outgoing communications between the agent and the Active Directory server:
  - TCP 88.
  - TCP 389.
  - UDP 389.
  - UDP 53.
  - TCP 3268.
- Local loop:
  - TCP port 16010.
  - TCP port 16011.
  - TCP port 16012.

> ⚠ **WARNING**
> If a firewall is enabled on the workstation (the Windows Firewall for example), you need to set rules to authorize the above network flows.

3.3 Stormshield Endpoint Security installation

3.3.1 Prerequisites

Before installing Stormshield Endpoint Security, check that the following files/folders are present:

- The `resources_x64` (64-bit version) folder including the following files:
  - `dotnetfx40_Full_x86_x64.exe` (Microsoft .NET Framework n.n.n)
  - `MSXML6.msi` (Microsoft MSXML 6.0 Parser).
  - `SQLEXPR_x64_ENU.exe` (Microsoft SQL Server 2012 Express Edition).
  - `vcredist.exe` (Microsoft Visual C++ 2008 SP1 Redistributable).
  - `WindowsInstaller.exe` (Microsoft Windows Installer 4.5).
  - `wic_x64_enu.exe` (Windows Imaging Component).
- The `setup.exe` file (Stormshield Endpoint Security).

3.3.2 Procedure

Stormshield Endpoint Security is installed in **four** stages using the following wizards on the main server:

1. Installation WizardStormshield Endpoint Security
2. Database setup wizard
3. Environment configuration wizard.
4. Agent deployment wizard.

Additional servers are installed using the server installation wizard. See section Installing additional servers.
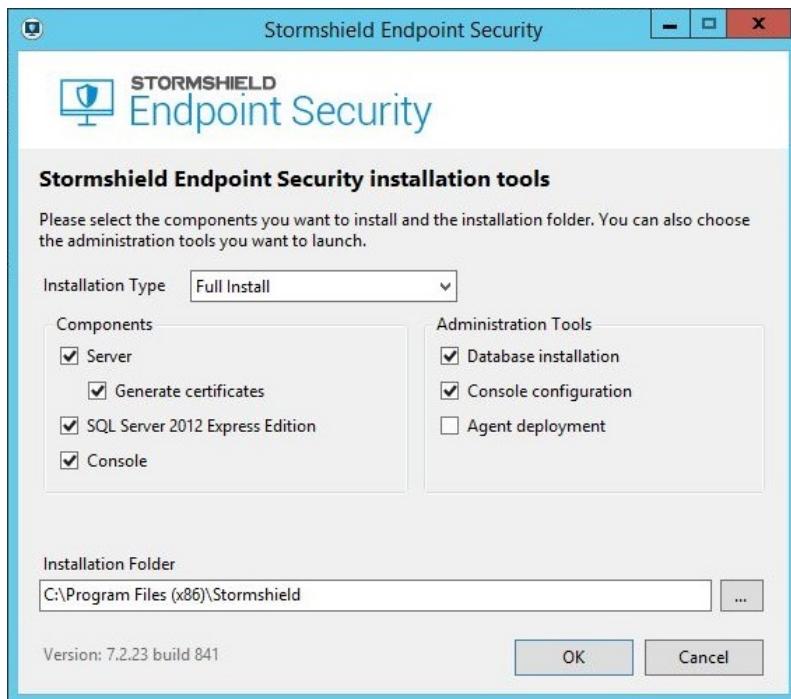
Agents can also be directly installed from the client workstation. See section Installing the agent from the client workstation.

Installing the management console, the server(s) and databases in a trusted zone is recommended.

Installation WizardStormshield Endpoint Security

To install Stormshield Endpoint Security, follow the steps below:

1. Double-click `setup.exe`.

2. Select a language.

3. Define your settings:

- ° The **Installation Type** that you wish to launch:

  - Full Install (automatic installation and configuration of all components using wizards).

    ### 🛈 NOTE
    Agent deployment is not selected by default, even in Full Install mode. If you wish to launch the agent deployment wizard after the installation, select this option.

  - Simple Install (component installation only).

  - Server Only (additional servers).

  - Console Only (installation of additional consoles).

  - Custom Install.

- ° The Stormshield Endpoint Security**Components** that you wish to install (if you choose an installation type other than **Full Install**):

  - The Stormshield Endpoint Security server (and its certificate).

  - The SQL server database.

  - SkyRecon management console.

- ° The **Administration Tools** that you wish to use to configure Stormshield Endpoint Security:

  - Database installation (Database setup wizard).

- Console configuration (Environment configuration wizard).

- Agent deployment (Agent deployment wizard).

◦ The Stormshield Endpoint Security **Installation folder**.

Click **OK** to validate your settings.

> **NOTE**
> If you wish to install the agent and the console on the same workstation, install the agent first and then the console.

4. To launch the full installation of Stormshield Endpoint Security, select **Full Install** and click **Next** in the installation wizard.

5. In the **Server** step, enter the IP address of the Stormshield Endpoint Security server and click **Next**.

For a first installation, the default backup directory for certificates generation is **[ProgramData]\Stormshield Endpoint Security Certificates**. It is only for the console certificate.

If you change the backup directory, it only applies to the console certificate.

By default the server certificates are in the following directory: **[Program Files]\Stormshield\Stormshield Endpoint Security Server**.

6. In the **Certificates** step, enter the new console certificate password.

Click on **Next**.

> **NOTE**
> If you have selected **Server** and **Generate certificates** in the **Components** section (See **Define your settings:**), the **Generate certificates** settings in the window above will be grayed out and cannot be used.

7. In the **Random numbers** step, move the mouse in order to increase random for the generation of encryption keys for full disk encryption. The **Next** button displays after the mouse has been moved enough.

8. In the **SQL Server 2012** step, select Windows authentication or authentication via the SA MSSQL (super-administrator) account.

> **WARNING**
> According to Microsoft guidelines, choose Windows authentication to limit exposure to security vulnerabilities.
> The SA account is then renamed, deactivated and has a random password assigned.

9. If you choose the SA MSSQL account, enter and confirm the new password.

> **NOTE**
> The password must observe the complexity criteria defined on the machine and/or domain.

Click on **Next**.

10. The following window displays. It summarizes the settings that you have just defined.

Click on **Next**.

11. Wait until the installation procedure is completed.

12. The window below shows that the components have been properly installed. Click **Finish**.

Database setup wizard

In the case of a full installation, the database setup wizard launches automatically after server installation.

In the case of a simple installation, relaunch `setup.exe` and tick the database setup wizard to configure the database.

To configure the Stormshield Endpoint Security database, follow the steps below:

1. The database setup wizard window is displayed.

   Click on **Next**.

2. In the **Super Admin** step, select Windows authentication or authentication via the SA MSSQL account. You must use an account with the sysadmin rights on the SQL instance on which SES will be installed.

3. If you select authentication via SA MSSQL, enter:

   ◦ The database administrator login.

   ◦ The database administrator password.

   ### 🛈 NOTE
   If you subsequently need to add the Windows account you used for the installation of the database as a user of the console, this user will then have Administrator rights on the Stormshield Endpoint Security database. For more information, see section "Monitoring" section.

4. The SQL server instance.

   Click on **Next**.

NOTE
To declare the SQL server instance, two methods are available:

   Method 1:

   If the SQL server uses a fixed port (example: 1433), declare the SQL port in the instance field in either way:

   - SqlServeur,1433

   - 192.168.1.1,1433

   • **Method 2**:

If the SQL server uses a dynamic port, declare the SQL instance in either of the following ways:

- SqlServeur\SES

- 192.168.1.1\SES

Method 2 also applies when the SQL server uses a fixed port.

5. In the **Database** step, to create an Administrator account dedicated to the Stormshield Endpoint Security main database:

   ◦ Check **Install Main Database**.

   ◦ Enter the password.

   ◦ Confirm password

   ◦ Click on **Next**.

6. In the **Alert Database** step, to enable reporting alerts to the Stormshield Endpoint Security server:

   ◦ Check **Install Alert Database**.

   ◦ Enter the password.

   ◦ Confirm password

   ◦ Click on **Next**.

7. In the **Key Database** step, to activate the database account:

   ◦ Check **Install Key Database**.

   ◦ Check **Use same password as for the alert database account**.

   ◦ Click on **Next**.

   ### ⓘ NOTE
   If needed, you can select a different password for the key database. If so, uncheck **Use same password as for the alert database account**.

8. In the **Automatic backup** step, to automatically save the main database on the server, follow the steps below:

   ◦ Check **Automatic Database Backup**.

   ◦ Enter the backup file path.

   ◦ Select the backup frequency.

   ◦ Click on **Next**.

ⓘ NOTE
This feature is available only if you have access to the **SQL SERVER AGENT [SES]** service.
This feature is not available with MS SQL Express Edition.

⚠ WARNING
To enable automatic backup, it is necessary to start the **SQL SERVER AGENT** service
before finishing this step.

ⓘ NOTE
To back up your database in a directory other than the default directory (example:
`.\Mssql\Backup`), assign Read/Write rights to the security group
`SQLServer2005MSSQLUser$ServerName$SQLInstance`.

9. The following window displays. It summarizes the settings that you have just defined.

   Click **Next** to validate your settings.

10. Wait until the installation procedure is completed.

11. Complete the configuration by clicking **Finish**.

Environment configuration wizard

In the case of a full installation, the environment configuration wizard automatically launches
after database configuration.

In the case of a simple installation, relaunch `setup.exe` and select the environment
configuration wizard.

In this step, you must choose between an environment based on an Active Directory or an
environment based on an internal directory.

To configure the management console and create a first operational environment connected to
a server, follow the steps below:

1. The environment configuration wizard window is displayed.

   Click on **Next**.

2. In the **Directory type** step, to define the directory type matching your environment, you
   must select between:

   ° an internal directory. Agents will belong to groups created from NetBIOS names or IP
     addresses.

- an environment based on an Active Directory. All workstations on which you will install an agent belong to this directory.

> ⚠️ **WARNING**
> You cannot modify the choice you have made once the configuration of the environment is done.
> You will be able to add internal directories afterwards if the environment is based on an Active Directory.

> ℹ️ **NOTE**
> If your environment is based on an Active Directory, note that the "Computers" container is not an organizational unit.

3. In the **Directory configuration** step, to define the domain or forest of the directory corresponding to the console environment, follow the steps below and click **Next**:
   - Enter the type of directory you wish to include in your environment:
     - Current Domain: domain to which the Windows user belongs.
     - Current Forest: forest to which the Windows user belongs.
     - Other Domain: specify the domain name in Active Directory Server.
     - Other Forest: specify the forest name in Active Directory Server.
   - Select the authentication type on the directory server:
     - Anonymous.
     - Windows session: uses the Windows user login.
     - Specific account: enter the login and password you wish to use.
   - Check the directory connection by clicking the **Test connection** button.

   > ℹ️ **NOTE**
   > This button checks the connection to the directory. The directory must be accessible to go to the next step.

4. In the **Environment** step, follow the steps below to define the console environment and click **Next**:
   - Enter the environment name.
   - Select the license file using ⋯.
   - Enter the Stormshield Endpoint Securityserver configuration policy name.
   - Enter the IP address of the Stormshield Endpoint Security server on which the server configuration policy will be applied.
   - Select the output directory for console certificates using ⋯.
   - Enter the passphrase associated with the console certificates generated when installing Stormshield Endpoint Security.

5. In the **Database settings** step, to configure the connection between the database and the console, enter the database passwords defined when installing Stormshield Endpoint Security:
   - Alert database.
   - Key database

   Click on **Next**.

6. The following window displays. It summarizes the settings that you have just defined.

Click **Next** to validate your settings. The window below shows that the configuration is in progress.

7. The window below shows that your environment has been properly configured. Click **Finish** to exit the environment configuration wizard.

> **ⓘ NOTE**
> The **Launch the console when finished** box is checked by default. You can uncheck it if needed.

8. The management console is displayed if the **Launch the console when finished** box is checked.

> **ⓘ NOTE**
> The agent deployment wizard launches behind the management console window. Minimize the window to proceed with the installation.

> **⚠ WARNING**
> Before installing an agent or continuing the agent installation procedure, you need to apply changes to the server: from the console, click **Deploy to the environment**.

Agent deployment wizard
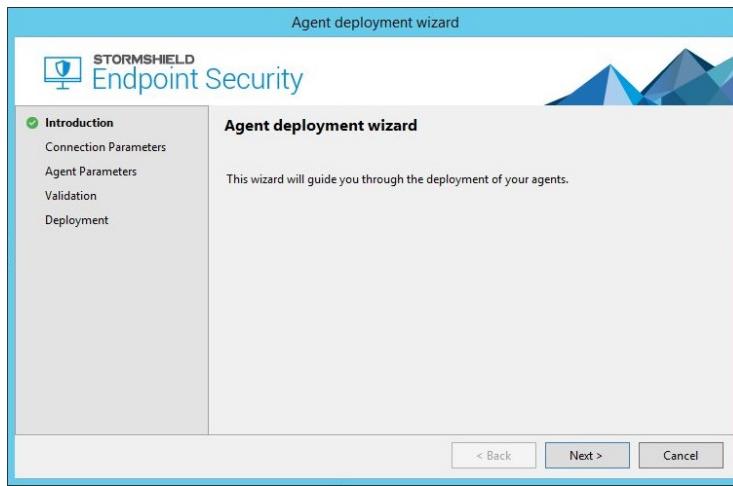
To deploy agents, follow the steps below:

1. After configuring your environment, the agent deployment window will open if you checked the box **Agent deployment** in the Stormshield Endpoint Securityinstallation tool.

> **⚠ WARNING**
> If you did not check the box, before manually launching the agent deployment wizard, configure your environment and click **Deploy to the environment**.

Click on **Next**.

2. Enter the following connection parameters:

   ○ The domain name.

   ○ The user name.

   ○ The user password.

   ○ The Stormshield Endpoint Securityserver address:

- The port number of the web server installed with the Stormshield Endpoint Securityserver.

Click on **Next**.

> ### ⓘ NOTE
> The account used must have Administrator rights on the workstation.

3. Customize the agent parameters:

  - Define the list of machines on which to install the agent by:

    - IP address range.

    - IP addresses.

  - Select the Stormshield Endpoint Security package to be installed:

    - Stormshield Endpoint Security Agent Professional Edition.

    - Stormshield Endpoint Security Agent Secure Edition.

  - Click on **Next**.

4. The following window displays. It summarizes the settings that you have just defined.

Click **Next** to validate your settings.

5. The following window displays.

Wait until the agent deployment is completed.

Click **Finish**.

> ### ⓘ NOTE
> In order to use the agent deployment wizard, make sure that:
>
> - The Web service of the Stormshield Endpoint Security server can be accessed by any machine on which the agent is going to be deployed.
>
> - Administrative Tools can be accessed by workstations.
>   If another application or a user already accesses Administrative Tools on the machine on which the agent is going to be deployed, deployment fails.
>
> If problems arise, check that access is not blocked by a firewall and that simple file sharing is disabled.

Installing additional servers

Additional servers are optional. They are used to distribute the load of requests between agents and servers and ensure high availability of servers.

The agent load is distributed among the servers assigned to the agent, which are at the closest hierarchical level among its parent OUs. Moreover, when the principal server encounters a problem, an agent automatically establishes the communication with an additional server.

Number of additional servers

The number of additional servers depends on:

- The number of agents deployed.

- The network speed.

- The configuration size.

- The number of alerts and logs returned. For information on how communication is distributed among servers and agents, see section Deploying policies on agents and collecting logs.

Procedure

To install an additional server, follow the steps below:

1. Double-click `setup.exe`.

2. Select a language and click OK.

3. Define the following parameters:

   - In **Installation type**, select **Server Only**.

   - Uncheck **Generate certificates** as these refer to console certificates that were generated when the principal server was installed (**Installation type** switches to **Custom Install**).

   - Define the server installation path on the target machine.

   - Click **OK** to validate your settings.

4. In the following window, check the **Attach to existing server** box and specify the path to access the two files that were generated when installing the principal server:

   - `root.pem` (Certificate Authority).

   - `rootcert.pem` (certificate).

   These files were placed in the principal server installation directory, by default: `[Program Files]\Stormshield\Stormshield Endpoint Security Server`.

   Enter the IP address of the main server and the ports used by the embedded web server.

(i) NOTE

By default, ports 80 and 443 are used. These values must be changed if a web server already uses these ports on the target machine.

5. In the **Random number generation** step, click **Next**. The random number has already been generated at the installation of the main server.

6. The installation wizard details the components that will be installed. Click on **Next**.

7. Check the installation report.

   This report shows the installation status of the selected components (in this case, only the **Server** part).

8. When the additional server is installed, you must declare it in your configuration via the management console. You must then assign the additional server to OUs of the Active Directory or to agents from the internal directory so that agents can exchange information with the server.
   For more information, see section Adding an additional Stormshield Endpoint Security server.

Installing the agent from the client workstation

Downloading the agent from the Web server

Downloading the Stormshield Endpoint Security agent from a Web server is the default deployment mode when no other remote deployment tool is available.

In this mode, the agent installer is downloaded and run manually from each client workstation.
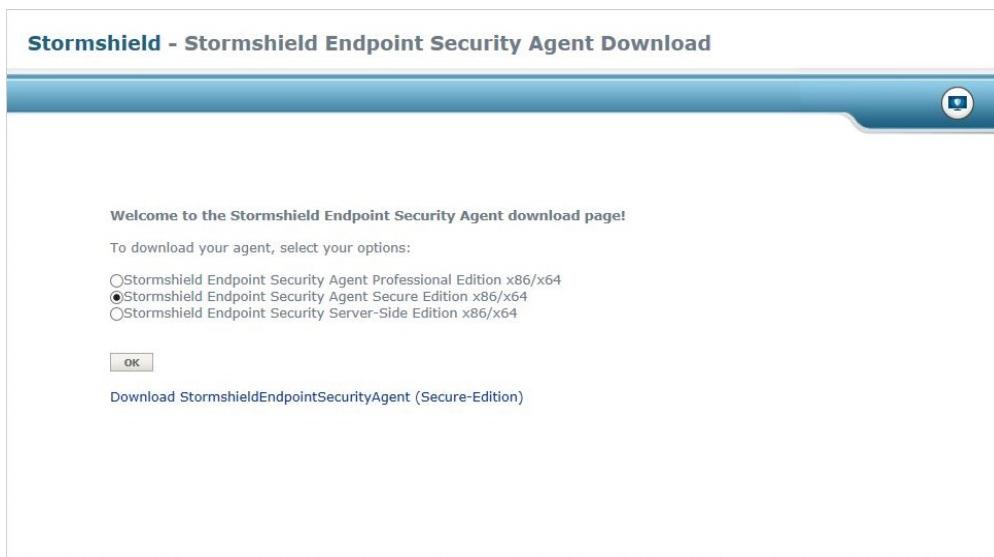
The access address for this page is the Web server IP address as entered when the server was installed. If port 80 by default has been changed, you need to specify the port assigned as a suffix to the IP address in the web browser address field.

Installation

(i) NOTE

Before installing an agent, the administrator must make sure that the client on which the agent will be installed can contact the Stormshield Endpoint Security server.
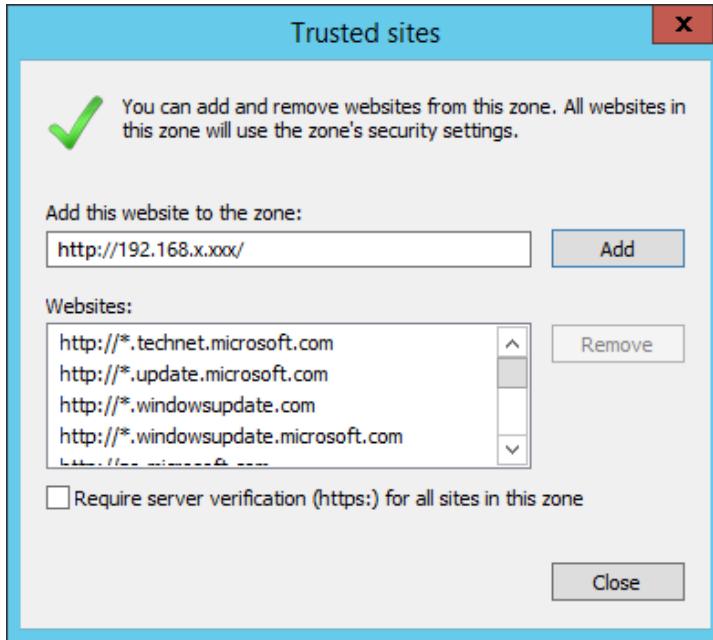
The agent installer can be run directly from the Web page or stored locally for a later installation.

This is a silent procedure, therefore no particular information is requested during agent installation.

⚠️ **WARNING**

If you wish to download the `.MSI` setup file for the Stormshield Endpoint Security **Server-Side Edition** agent with Internet Explorer, add the Stormshield Endpoint Security server's IP address to your **Trusted Sites**.

A message is displayed in a pop up window above the taskbar when the installation is completed. The computer must be rebooted to activate the agent.

Since this installation mode must be repeated on each client workstation, it is mostly used for testing and pilot environments.

> ⚠️ **WARNING**
> You must use the **Administrator** account to install the Stormshield Endpoint Security agent. If you install the agent with any other account, the installation will start but will not finish properly.

Agent installation directory

The agent can be installed in a directory other than the directory used by default, that is:

```
c:\Program Files\Stormshield\Stormshield Endpoint Security Agent\
```

Changing the agent installation path

To change the agent installation path, follow the steps below:

1. On the server side, open the following file:

   ```
   [program files]\Stormshield\Stormshield Endpoint Security
   Server\Apache\cgi-bin\msi.nsi
   ```

   Locate the following line:

   ```
   ;;WriteINIStr '$TEMP\sky.tmp\sky.cnf' Agent Install_path
   'C:\Program Files\company'
   ```

2. Remove the comments (`;;`).

   Replace `C:\Program Files\company` with the target installation path `[custom path]`.

   > ℹ️ **NOTE**
   > If the line is commented, the default value `%program files%\ SkyRecon` will be used.

3. Save the file.

4. Run `[program files]\Stormshield\Stormshield Endpoint Security Server\generate_msi.exe`.

The Stormshield Endpoint Security agent will be installed in the custom path. The path will resemble: `[custom path]\StormShield Endpoint Security agent\`.

Using GPO to deploy agents

Active Directory® Group Policy Objects (GPO) are used to deploy applications using the Microsoft Windows Installer service. This is a silent procedure as no particular information is requested from the user during installation.

Remote deployment using GPO requires a specific file format called `MSI`. This type of file can be used to perform remote installations without user intervention.

The `MSI` file is located in the `files` subfolder of the server installation directory that is by default:

```
c:\Program Files\Stormshield\Stormshield Endpoint Security
Server\files
```

> ⚠️ **WARNING**
> System cloning tools are not compatible with the **Secure Edition** agents.

Before creating the system image, check that there is no certificate file (`agent.srn`) in the Stormshield Endpoint Security agent installation directory.

Integrating policies in the agent installation program

If the workstation on which the agent is installed cannot reach the SES server, it is possible to integrate policies to be applied in the agent installation program.

To do so:

1. In the console, apply the dynamic and static configuration and the security policy directly on the environment root.
2. Synchronize.
3. In the server folder, copy the file *sync\Agent.srz*.
4. Restore the server back to the previous state (initial configuration).
5. Backup the MSI file which is located in the *files* subfolder of the server installation directory.
6. Copy the file *sync/Agent.srz* in the folder *Apache/cgi-bin* at the server root.
7. Restore the installation programs by running *generate_mis.exe* as an administrator.
8. Take the MSI file which is located in the *files* subfolder of the server installation directory in order to deploy the agent,
9. Delete the *Agent.srz* file in the folder *Apache\cgi-bin* and restore the MSI file to go back to the initial state.
10. When installing the agent, install an agent's certificate for the agent to be operational: before restarting the agent for the first time, replace the *agent.srn* agent's certificate by a *agent.srn* file downloaded from the site `https://<Adresse IP Serveur>/ssl/cgi`. This *agent.srn* file must be different for each agent. For more information, see the section **Login and password for downloading certificates**.

In this way, it is possible to deploy functional and configured agents even if they do not have access to the SES server.

3.3.3 About Stormshield Endpoint Security

Once Stormshield Endpoint Security has been installed, you will be able to view its status and version number:

1. Right-click on the Stormshield Endpoint Security icon in the taskbar.
2. Select **Status** in the pop-up menu.

3.4 Downloading certificates

To secure communication between Stormshield Endpoint Security components (console, server and agent), each component uses its own certificate.

Each agent must have a unique certificate to securely communicate with the server.

When an agent has just been installed on a workstation, no certificate is provided for the Stormshield Endpoint Security agent instances. They need to obtain a certificate for communicating with the Stormshield Endpoint Security server.

For this purpose, a certificate server is installed on the Stormshield Endpoint Security server which is accessible by default through TCP port 443.

> **ⓘ NOTE**
> For more information on how to configure, uninstall the agent or deactivate protections, see **Stormshield Endpoint Security Agent Configuration**.

3.4.1 Certificate validity period

For security reasons, downloading certificates should be restricted to a limited time period, usually the time necessary to deploy the Stormshield Endpoint Security agent instances on the network.

The time period can be configured in the management console by selecting the server configuration policy in the **Policies** tree view.

The required settings are in the **Authentication Service** part of the server configuration policy.

⊟ 🔒 **Authentication Service**	
Checking server source	✅ Enabled
Start time	3/30/2018 12:00:00 AM
End time	3/30/2028 12:00:00 AM
Login for CGI authentication	
CGI authentication password	
Certificate validity (day(s))	3650

By default, the certificate time period is limited to **10 years** from the console installation date.

Change the value of the certificate availability **End Time** if you prefer a shorter period.

3.4.2 Login and password for downloading certificates

It is possible to define a login and a password to allow an administrator to download certificates from a web page.

To do so, use the fields **Login for CGI authentication** and **CGI authentication password** of the **Authentication Service** part of the server configuration policy.

⊟ 🔒 **Authentication Service**	
Checking server source	✅ Enabled
Start time	3/30/2018 12:00:00 AM
End time	3/30/2028 12:00:00 AM
Login for CGI authentication	
CGI authentication password	
Certificate validity (day(s))	3650

To download a certificate, point your web browser to:

```
https://<Server IP address>/ssl/cgi
```

On the certificate server authentication page, enter the user login and password.

If authentication is successful, a dialog box opens to download the file named *agent.srn*. This file must be copied into the agent installation folder.

🚫 WARNING
Accessing the secured page and downloading the certificate require a browser compatible TLS in version 1.1 or 1.2.

3.4.3 Compatibility with system cloning tools

The Stormshield Endpoint Security agent is compatible with system cloning tools.

🚫 WARNING
System cloning tools are **not** compatible with the Stormshield Endpoint Security Secure Edition agents.

To create a disk image of a system containing the agent, install the agent on the principal system as shown in Procedure.

Each agent requires a unique certificate. The installation of an agent on the master workstation must not include its certificate.

To prevent this, in the **Authentication Service** parameter of the management console, we recommend that you define an invalid date before the creation date of the master.

Before creating the master image, you must check that the Stormshield Endpoint Security agent installation directory contains no:

- `agent.srn` file
- `host_guid.sro` file
- file in the `vfs` directory.

If this is not the case, you must delete these files.

The **Authentication Service** parameters are available in the server configuration policy.

When clone systems are deployed, reset the period of availability of the Authentication Service to allow each Stormshield Endpoint Security agent to retrieve its own certificate.

3.5 Post-installation tests

3.5.1 Component tests

It is recommended to test all Stormshield Endpoint Security components after product installation.

Follow the steps below to test the whole Stormshield Endpoint Security operating sequence:

1. Identify a target machine through the network description.
2. Define a simple and easily testable configuration.
3. A simple configuration example consists in preventing the NotePad application from opening any text file with a `.txt` extension.
   For more information, see Security Policies.
4. Send the configuration (and deploy the agent on the target machine if this has not already been done).
5. Check that the rule set out is applied on the target machine.
6. Check access to the events stored in the database.

Should a problem arise, see Troubleshooting.

3.6 Possible changes

3.6.1 Changing a Stormshield Endpoint Security server IP address

After installing and configuring Stormshield Endpoint Security, you may at some point need to change the IP address of a Stormshield Endpoint Security server (hosting the web server used for installing new agents).

To do so, you must have at least one other server on which all agents can connect to when the server is not available with the former IP address.

With an environment based on an Active Directory, you do not need to configure anything in the management console. All changes automatically apply when the Active Directory resolves the DNS name of the principal server.

With an environment based on an internal directory:

1. Add a server with the new IP address in the **Servers** panel in the console.

2. Assign the new server to the same agents groups.

3. Deploy changes to the environment.

4. Once every agent has been updated:

   ◦ Remove the server with the former IP address from the **Servers** panel in the console.

   ◦ Change the IP address on the server.

5. Apply again changes to the environment.

You must also update the **agent installer** so that new agents can use the same IP address.

To do so, follow the steps below:

1. Go to the installation directory of the principal server.

2. Update all references to the IP address in the following file:

   ```
   [install directory]\Apache\cgi-bin\conf.srx
   ```


3. Double-click the following file:

   ```
   [install directory]\Generate_msi.exe
   ```

   The installer has been updated, you can now download new agents from the Web server.

3.6.2 Changing the database server IP address

To change the database server IP address in the management console:

1. Reconnect to the console by specifying the new IP address of the database in the SQL server instance.

2. To give Stormshield Endpoint Security servers the new IP address of the database server, select the server configuration policy(ies) and change the database instance in **Log Monitoring Configuration** and in **Encryption**.

3. To give the console the new IP address of the database server, select **Configuration** in the **Console Manager** section. Then select the new IP address for the key database and log database.

3.6.3 Changing the server TCP ports for HTTP and SSL services

To modify the server TCP ports for HTTP and SSL services (after installation), follow the steps below:
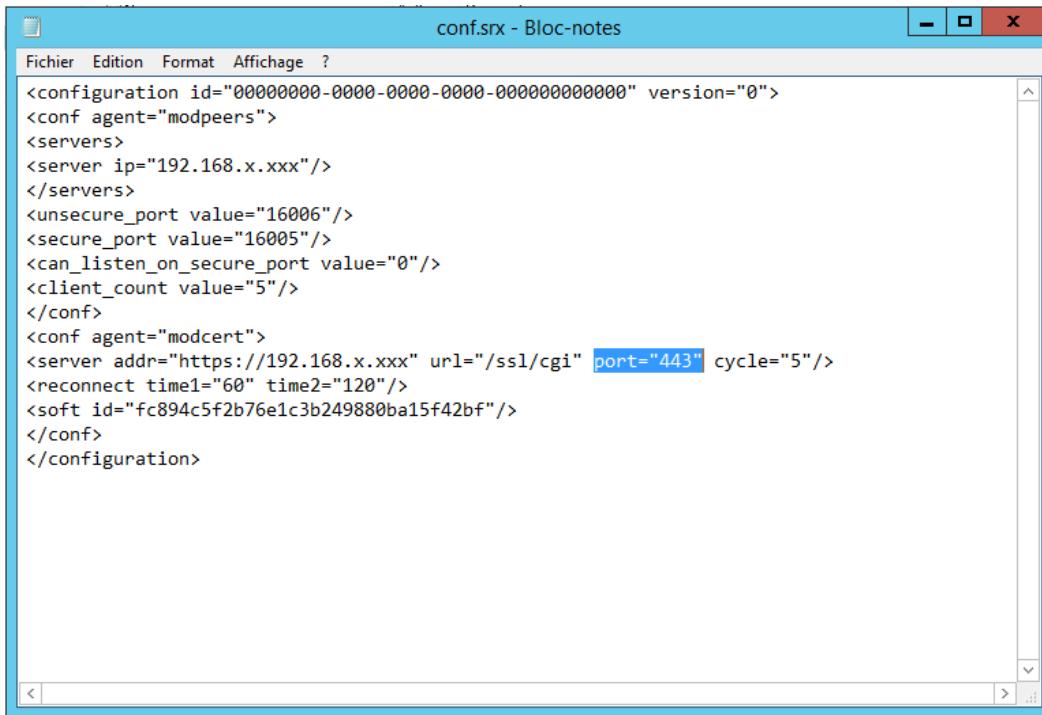
1. After installing the server, you can change the two TCP ports used for the HTTP/SSL server by editing the following server files:

   `C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\conf\httpd.conf`

   `C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\conf\ssl.conf`

2. In the `httpd.conf` file, change the port values assigned to **Listen** and **ServerName WebServer** (default port is 80).

3. In the `ssl.conf` file, change the port values assigned to **Listen**, **ServerName WebServer** and **VirtualHost** (default port is 443).

4. Restart the server.

Now, you must update the agent installer for it to take into account the new TCP ports of the server.

1. Go to the default installation directory of the server:

   `C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\cgi-bin\`

2. In the `conf.srx` file, change the TCP port value (default port is 443).

```
                                    conf.srx - Bloc-notes                          _  □  ✕

Fichier  Edition  Format  Affichage  ?

<configuration id="00000000-0000-0000-0000-000000000000" version="0">
<conf agent="modpeers">
<servers>
<server ip="192.168.x.xxx"/>
</servers>
<unsecure_port value="16006"/>
<secure_port value="16005"/>
<can_listen_on_secure_port value="0"/>
<client_count value="5"/>
</conf>
<conf agent="modcert">
<server addr="https://192.168.x.xxx" url="/ssl/cgi" port="443" cycle="5"/>
<reconnect time1="60" time2="120"/>
<soft id="fc894c5f2b76e1c3b249880ba15f42bf"/>
</conf>
</configuration>
```

3. Double-click the following file:

   `C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Generate_msi.exe`

   The installer has been updated, you can now download new agents from the Web server.

3.7 Uninstalling components

3.7.1 Uninstalling the server and the console

The management console and the Stormshield Endpoint Security servers can be uninstalled using the uninstall tools accessible from:

- The **Start** menu on the systems that host these components.

- The Windows **Add/Remove Programs** service accessible via the control panel.

3.7.2 Uninstalling the agent

The agent can be uninstalled via the **Windows Apps & features** control panel on the user's workstation or from the *Srend.exe* file found in the installation folder.

Before uninstalling the agent, ensure that the following requirements have been met:

- The user is the administrator on his workstation,

- The **Stop agent** option in the agent's dynamic configuration has been set to **Allowed**,

- Protection against the creation of executable files has been disabled,

- The default behavior in the general application control settings has been set to **Allow execution (blacklisting)**.

If the agent was installed by remote deployment using GPO, you can also use this same tool to uninstall the agent silently.

> ### 🛈 NOTE
> If a SES administration console is installed on the same workstation, we recommend uninstalling the console before the agent.

Uninstalling the agent from Windows utility

To uninstall the agent from Windows utility, follow the steps below:

1. Open the **Uninstall or change a program** Windows utility:
   - In Windows Seven or Windows 8.1: **Control panel \ Programs \ Programs and features**,
   - In Windows 10: **Settings \ Apps \ Apps and features**.
2. Click on **Stormshield Endpoint Security Agent**.
3. Click on **Uninstall/Change** or **Uninstall \ Uninstall**.
4. Follow the instructions. Most agent files and directories are removed when the workstation restarts.

Uninstalling the agent from the *Srend.exe* file

To uninstall the agent from the *Srend.exe* file, follow the steps below:

1. Select the folder *[Program Files]\Stormshield\Stormshield Endpoint Security Agent* on the user's workstation.
2. Double-click on the *Srend.exe* file. The Stormshield Endpoint Security icon is grayed out and a window notifies the user to restart the computer.
3. Restart the computer to complete the agent uninstallation procedure. Most agent files and directories are then removed.

Uninstalling the agent when data is encrypted

If the workstation disk is encrypted, we recommend decrypting it before uninstalling the agent.

When a file encryption policy is applied on the workstation and the user entered the encryption password, the workstation needs to be restarted twice. If the user canceled and did not enter the password, the workstation needs to be restarted just once.

3.7.3 Removing the databases

The MS SQL Server 2012, 2014, 2016, 2017 or 2019 database is uninstalled using the Windows **Add/Remove Programs** service or the Stormshield Endpoint Security database installer.

> ### 🛈 NOTE
> The database must be removed before uninstalling the console.
> If you uninstall the console before removing the database, DBInstaller will be uninstalled and you will no longer be able to remove the database.

To remove the database, follow the steps below:

1. Go to **Start>All programs>Stormshield >DBInstaller**.

   The database management tools window opens.

2. Click **Uninstall Stormshield Endpoint Security database**.

3. The following window displays.

   Click on **Next**.

4. Enter the SuperAdmin information to connect to the database:

   ◦ The SuperAdmin login.

   ◦ The SuperAdmin password (by default `sa`).

   ◦ The database path.

   Click on **Next**.

5. Select the databases to be uninstalled.

   Click on **Next**.

6. Before starting the uninstallation process, check the information displayed.

Click on **Next**.

7. The uninstallation process is finished.

4. Migrating and Updating Stormshield Endpoint Security

This chapter describes the procedures for migrating from StormShield 6.0 to Stormshield Endpoint Security 7.2 and the procedures for updating Stormshield Endpoint Security 7.2:

Release Notes contain highly important information. Please refer to them before updating Stormshield Endpoint Security.

If you need to migrate StormShield from a version lower than version 6.0/10, the automatic policy migration will not be able to import all settings. You are strongly advised to manually recreate the various policies and configurations in the version 7.2.

You need a MS SQL Server 2012, 2014, 2016, 2017 or 2019 server for your 7.2 database. Then you need either to update your version of MS SQL Server, or install a new server.

> ℹ️ NOTE
> The version 7.2 of Stormshield Endpoint Security is the first version named with the brand Stormshield. The software installation paths have been thus updated. Stormshield Endpoint Security 7.2 is installed by default in the directories:
> -C:\Program Files\Stormshield\Stormshield Endpoint Security Server
> -C:\Program Files\Stormshield\Stormshield Endpoint Security Management Console
> -C:\Program Files\Stormshield\Stormshield Endpoint Security Agent
>
> If migrating from previous versions, directories remained the same as they cannot be moved. A version 7.2 updated from version 6.0 remains in the directories:
> - C:\Program Files\SkyRecon\StormShield Server
> - C:\Program Files\SkyRecon\SkyRecon Management Console
> - C:\Program Files\SkyRecon\StormShield Agent

4.1 Migrating StormShield 6.0 to version Stormshield Endpoint Security 7.2

4.1.1 Complete migration
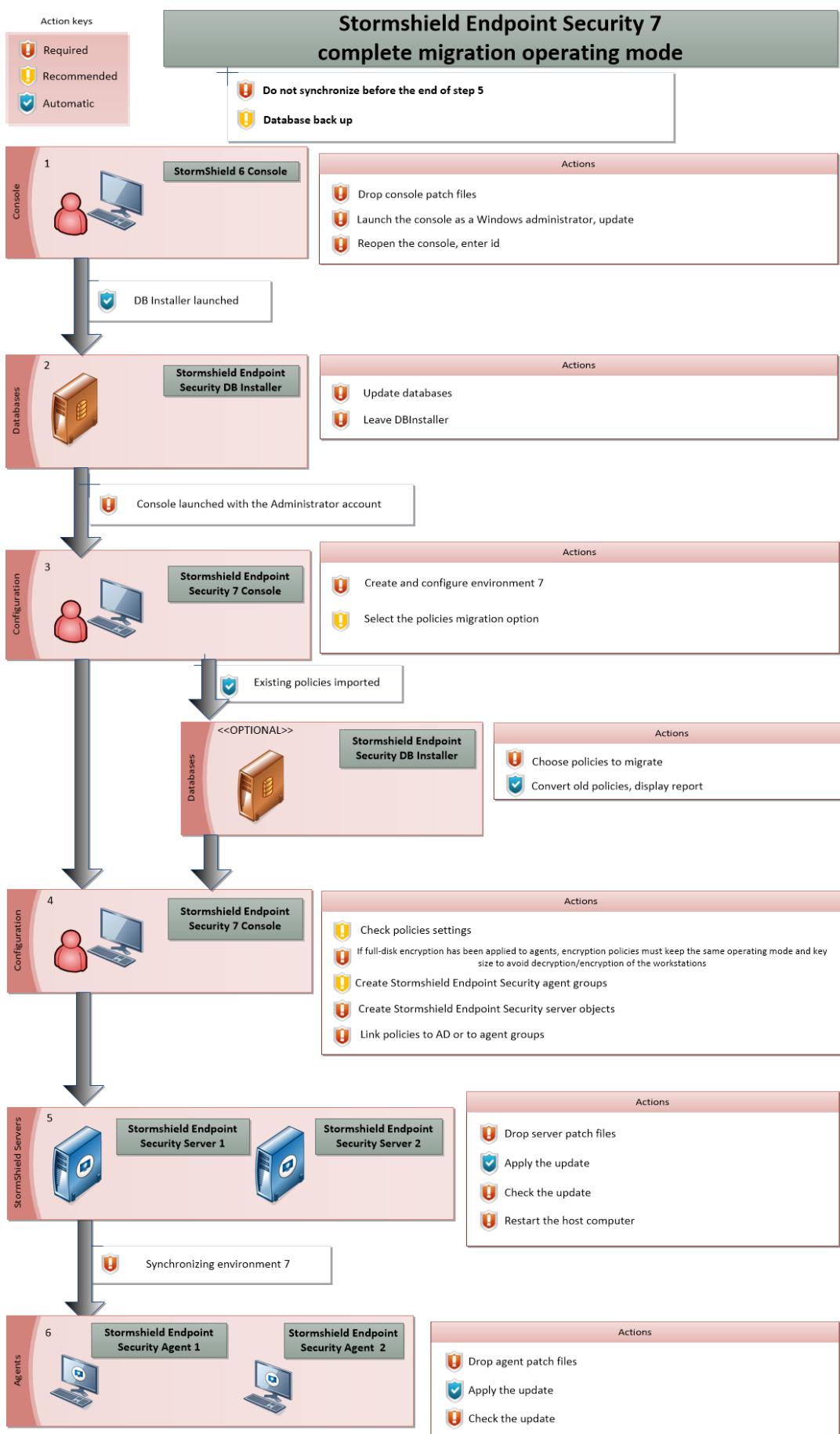
This migration mode allows migrating every agent from a 6.0 environment to the 7.2 version.

As the configuration of the console may take some time (7.2 environment setting), we recommend that you continue using an operational 6.0 console in the meantime so that you can update the policies and configurations applied to the agents during the migration if needed.

Until the 7.2 server and agent updates are sent to the Stormshield Endpoint Security servers, the 6.0 console will be able to update policies applied on the agents of the existing organization.

We recommend you to backup each database before migrating StormShield. The Stormshield Endpoint Security configuration wizard allows backing up configuration and key databases with the maintenance menus.

Once the 7.2 console is installed, the DBInstaller will no longer allow backing up/restoring the configuration database of the 6.0 environment. To do this, you will need to use a 6.0 console depending on the previous migrated version. The DBInstaller provided with the 7.2 console only allows performing maintenance operations on the configuration database from the 7.2 environment. The 6.0 database must be backed up before migrating the console.

Action keys

🛡 Required
🛡 Recommended
🛡 Automatic

Stormshield Endpoint Security 7 complete migration operating mode

🛡 Do not synchronize before the end of step 5

🛡 Database back up

1 Console — **StormShield 6 Console**

Actions
🛡 Drop console patch files
🛡 Launch the console as a Windows administrator, update
🛡 Reopen the console, enter id

🛡 DB Installer launched

2 Databases — **Stormshield Endpoint Security DB Installer**

Actions
🛡 Update databases
🛡 Leave DBInstaller

🛡 Console launched with the Administrator account

3 Configuration — **Stormshield Endpoint Security 7 Console**

Actions
🛡 Create and configure environment 7
🛡 Select the policies migration option

🛡 Existing policies imported

<<OPTIONAL>> Databases — **Stormshield Endpoint Security DB Installer**

Actions
🛡 Choose policies to migrate
🛡 Convert old policies, display report

4 Configuration — **Stormshield Endpoint Security 7 Console**

Actions
🛡 Check policies settings
🛡 If full-disk encryption has been applied to agents, encryption policies must keep the same operating mode and key size to avoid decryption/encryption of the workstations
🛡 Create Stormshield Endpoint Security agent groups
🛡 Create Stormshield Endpoint Security server objects
🛡 Link policies to AD or to agent groups

5 StormShield Servers — **Stormshield Endpoint Security Server 1** — **Stormshield Endpoint Security Server 2**

Actions
🛡 Drop server patch files
🛡 Apply the update
🛡 Check the update
🛡 Restart the host computer

🛡 Synchronizing environment 7

6 Agents — **Stormshield Endpoint Security Agent 1** — **Stormshield Endpoint Security Agent 2**

Actions
🛡 Drop agent patch files
🛡 Apply the update
🛡 Check the update

Migrating the management console

The complete migration process starts with the installation of one or more 7.2 management consoles. To install management consoles, you can either reinstall the existing consoles, update the consoles or install a new console.

Reinstalling

This option consists in uninstalling the console already deployed on the workstation first, and then installing a console the normal way with the Stormshield Endpoint Security setup by checking the **Console only** box as the installation type.

Updating

This option consists of using the console update mechanism by dropping the two files below in the `patchs` folder of the Stormshield Endpoint Security server (XXX being the version targeted by the update):

```
skyreconconsole_win32_7.XXX.srh
skyreconconsole_win32_7.XXX.sru
```

Once these files have been dropped:

1. Run the console again as an administrator (administrator privileges are required for the installation of the update),
2. Click on the "?" menu,
3. Select the search for updates,
4. Accept the suggested installation.

New installation

Install the console as usual on a new workstation by using the Stormshield Endpoint Security setup and checking the **Console Only** option as the installation type.

> ⚠️ **WARNING**
> The 7.2 management console uses .NET Framework n.n.n: Ensure that it is installed before the console is updated.

Migrating databases and the environment

When the console has been updated, open it again. A user must log in. The database configuration wizard automatically opens.

Database setup wizard

The database setup wizard allows setting up and applying updates of the structure and content of the configuration, alerts and keys databases.

For more information on installing the 7.2 environment, refer to section Updating Stormshield Endpoint Security databases

When updating databases, all the users from the 6.0 console are migrated to the new configuration database. As roles are not compatible with 7.2roles, all users other than the main administrator will then take on the public role.

New 7.2environment configuration

After the configuration of the databases, restart the console in order to configure the new 7.2 environment.

For more information on installing the 7.2 environment, refer to section Environment configuration wizard.

Migrating 6.0 policies to the new configuration database

After configuring the console, you will be able to migrate policies and configurations created in version 6.0. All settings from the different policies will then be preserved.

⚠ WARNING

Policies will no longer be related to agent groups. You will need to apply them to the various elements of the directory as explained in the section Management Console Configuration.

Policies will not be removed from the 6.0 configuration database: they will be duplicated in the 7.2 configuration database and converted to the new format in order to match the new 7.2environment.

⚠ WARNING

There is no synchronization between 6.0 policies and policies converted to 7.2: if a 6.0 policy is edited after the migration, changes will not be reflected in the 7.2 policy.

Checking policies

Settings have been modified, added or removed between versions 6.0 and 7.2. It is thus recommended to check the settings of the imported policies to be sure they are still relevant.

The table below shows a list of the modifications between both versions.

	Removed settings	Changed settings	New settings
Server policy	"IP Address"	"Max. clients" (default value: 200) is replaced by: "Maximum number of handled clients" (default value: 1000)	
Security Policy			"Removable devices enrollment" (*Device control* tab)
Encryption Policy		- "Protection mode" is replaced by the two settings "Full-disk encryption" and "File encryption" - Encrypted folders and files management is now under the "Encrypted zones" setting	

These policies are displayed in a catalog above the directory.

⚠ WARNING

Full-disk encryption policies must keep the same algorithm and encryption type to avoid decrypting and encrypting workstations again.

The new 7.2 environment is ready to be configured. Refer to chapter Management Console Configuration for more information about setting up a 7.2 environment.

Migrating Stormshield Endpoint Security servers

After configuring the environment, you will need to migrate Stormshield Endpoint Securityservers.

Updating

To update servers, drop both of the following files in the `patchs` folder (XXX being the version targeted by the update):

```
stormshieldserver_win32_7.XXX.srh
```

```
stormshieldserver_win32_7.XXX.sru
```

After these files have been dropped, the server will update independently after the period defined in the **Frequency of update checks** setting in the server configuration.

You can also drop these two files in the folder defined in the **Updates download folder** parameter during the configuration of the server. You need to create a file named *version.sro* which only contains the version number of updates to download, in a "7.223" format.

Checking version

During the server update, the file `update.sro` is created in the `patchs` folder of the server. The file is deleted at the end of the configuration.

To check the server version, open the `version.sro` file in the `conf` folder. You can also see the server version in the **Monitoring** > **Software Logs** panel of the management console. A log displays with the status 'SERVER_VERSION'.

Restarting

After the update has successfully completed, restart the machine hosting the server in order to update the service of the Stormshield Endpoint Security server (`srservice.exe`).

Application of changes to the environment

After updating and restarting the servers, restart the management console and deploy changes to the environment so that the policies will be properly applied to all the agents. This is a very important step to be sure that the latest policies are applied to the agents.

Updating agents

When the Stormshield Endpoint Security servers are updated and when changes are applied, you need to update the agents currently deployed to end the migration process.

To update the agents, drop both of the following files in the `patchs` folder of the servers (XXX being the version targeted by the update):

```
stormshieldagent_win32_7.XXX.srh
```

```
stormshieldagent_win32_7.XXX.sru
```

The server will then propose the update to the agents connected to the server. The update will be applied after each agent restart.

Checking version

To check whether the agent was successfully updated, open the agent interface by double-clicking on the Stormshield Endpoint Security icon in the taskbar and check the version number at the bottom right.

All updates, successful or unsuccessful, are recorded in the logs available from the interface.

Specificity for encrypted agents (full disk encryption)

When migrating from a version 7.2.06 or higher, you have to change the USER password on encrypted workstations. If any, GUEST and AUTOBOOT accounts are automatically disabled on these workstations and the password of the ADMIN account is changed.

4.1.2 Partial migration
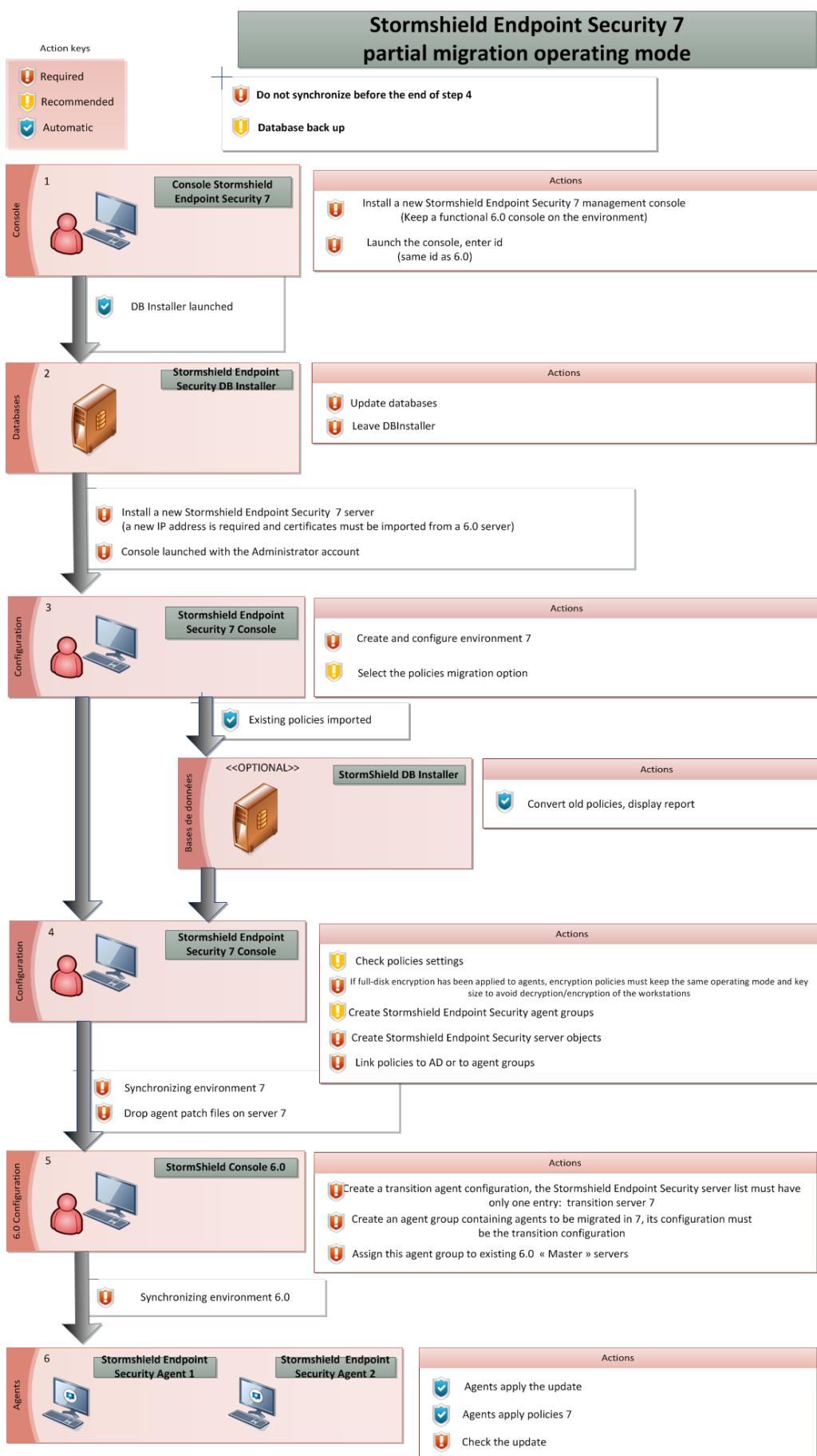
This migration mode enables to progressive migration of agents from 6.0 to 7.2.

You will be able to keep both 6.0 and 7.2 environments during the migration period.

To perform a partial migration, the workstation must be new.

We recommend you to backup each database before migrating StormShield. The Stormshield Endpoint Security configuration wizard allows backing up configuration and key databases with the maintenance menus.

Once the 7.2 console is installed, the DBInstaller will no longer allow backing up/restoring the configuration database of the 6.0 environment. To do this, you will need to use a 6.0 console. The DBInstaller provided with the 7.2 console only allows performing maintenance operations on the configuration database from the 7.2 environment. The 6.0 database must be backed up before migrating the console.

**Stormshield Endpoint Security 7
partial migration operating mode**

Action keys

- Required
- Recommended
- Automatic

- Do not synchronize before the end of step 4
- Database back up

1 — Console — Console Stormshield Endpoint Security 7

Actions

- Install a new Stormshield Endpoint Security 7 management console
  (Keep a functional 6.0 console on the environment)
- Launch the console, enter id
  (same id as 6.0)

DB Installer launched

2 — Databases — Stormshield Endpoint Security DB Installer

Actions

- Update databases
- Leave DBInstaller

- Install a new Stormshield Endpoint Security 7 server
  (a new IP address is required and certificates must be imported from a 6.0 server)
- Console launched with the Administrator account

3 — Configuration — Stormshield Endpoint Security 7 Console

Actions

- Create and configure environment 7
- Select the policies migration option

Existing policies imported

Bases de données — <<OPTIONAL>> — StormShield DB Installer

Actions

- Convert old policies, display report

4 — Configuration — Stormshield Endpoint Security 7 Console

Actions

- Check policies settings
- If full-disk encryption has been applied to agents, encryption policies must keep the same operating mode and key size to avoid decryption/encryption of the workstations
- Create Stormshield Endpoint Security agent groups
- Create Stormshield Endpoint Security server objects
- Link policies to AD or to agent groups

- Synchronizing environment 7
- Drop agent patch files on server 7

5 — 6.0 Configuration — StormShield Console 6.0

Actions

- Create a transition agent configuration, the Stormshield Endpoint Security server list must have only one entry: transition server 7
- Create an agent group containing agents to be migrated in 7, its configuration must be the transition configuration
- Assign this agent group to existing 6.0 « Master » servers

Synchronizing environment 6.0

6 — Agents — Stormshield Endpoint Security Agent 1 — Stormshield Endpoint Security Agent 2

Actions

- Agents apply the update
- Agents apply policies 7
- Check the update

Migrating the management console

The partial migration process starts with the installation of one or more 7.2 management consoles. To install management consoles, you can either reinstall the existing consoles, update the consoles or install a new console.

> ⚠️ **WARNING**
> For a partial migration, make sure your 6.0 environment is functional. You need at least one 6.0 management console.

Reinstalling

This option consists in uninstalling the console already deployed on the workstation first, and then installing a console the normal way with the Stormshield Endpoint Security setup by checking the **Console only** box as the installation type.

Updating

This option consists of using the console update mechanism by dropping the two files below in the `patchs` folder of the Stormshield Endpoint Security server (XXX being the version targeted by the update):

`skyreconconsole_win32_7.XXX.srh`

`skyreconconsole_win32_7.XXX.sru`

After that, restart the console, click the "?" menu, select the update search and accept the proposed installation.

New installation

Install the console as usual on a new workstation by using the Stormshield Endpoint Security setup and checking the **Console Only** option as the installation type.

> ⚠️ **WARNING**
> The 7.2 management console uses .NET Framework n.n.n: Ensure that it is installed before the console is updated.

Migrating databases

When the console has been updated, open it again. A user must log in. The database setup/installation wizard automatically opens.

Database setup wizard

The database setup wizard allows setting up and applying updates of the structure and content of the configuration, alerts and keys databases.

For more information on installing the 7.2 environment, refer to section Updating Stormshield Endpoint Security databases

When updating databases, all the users from the 6.0 console are migrated to the new configuration database.

> ⚠ **WARNING**
> The console users' roles other than the main administrator role (shown in bold in the list of users) will not be kept. All console users will have the public role in the 7.2 environment. The main administrator is required to create new 7.2 roles and to assign users to these roles.

Migrating Stormshield Endpoint Security servers

After updating databases, you need to install a new 7.2 server, which is a "transition" server, in order to continue the partial migration process.

Install the server as usual by using the Stormshield Endpoint Security setup and checking the **Server only** option as the installation type.

Certificates must not be generated but imported from a 6.0 server from your environment.

> ⚠ **WARNING**
> The IP address of the server(s) must be a new one. It cannot be an IP address from a 6.0 server still listed in the console.

New 7.2 environment configuration

After the configuration of the databases and the installation of the transition server, restart the console in order to configure the new 7.2 environment.

For more information on installing the 7.2 environment, refer to section Environment configuration wizard.
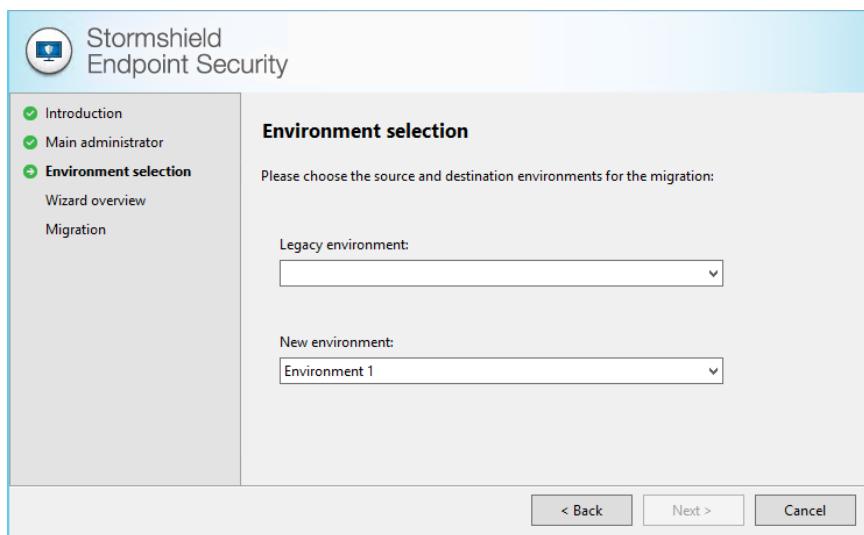
Migrating 6.0 policies to the new configuration database

After configuring the console, you will be able to migrate policies and configurations created in version 6.0 of Stormshield Endpoint Security. All settings from the different policies will then be preserved.

> ⚠ **WARNING**
> Policies will no longer be related to agent groups. You will need to apply them to the various elements of the directory as explained in the section Management Console Configuration.

If there were several environments in 6.0, first select the environment which contains policies to migrate.

Policies will not be removed from the 6.0 configuration database: they will be duplicated in the 7.2 configuration database and converted to the new format in order to match the new 7.2environment.

⚠ WARNING
There is no synchronization between 6.0 policies and policies converted to 7.2: if a 6.0 policy is edited after the migration, changes will not be reflected in the 7.2 policy.

Checking policies

Settings have been modified, added or removed between versions 6.0 and 7.2. It is thus recommended to check the settings of the imported policies to be sure they are still relevant.

To find out these settings, refer to the table in section Checking policies in Complete migration.

These policies are displayed in a catalog above the directory.

⚠ WARNING
Full-disk encryption policies must keep the same algorithm and encryption type to avoid decrypting and encrypting workstations again.

The new 7.2 environment is ready to be configured. Refer to chapter Management Console Configuration for more information about setting up a 7.2 environment.

Application of changes to the environment

Once the transition server is properly related, deploy changes to the environment and finalize the migration.

Dropping agent update files on the server

After applying changes to the environment and in order to allow agents to be updated, drop the two files below in the `patchs` folder of the transition server (XXX is the version targeted by the update):

`stormshieldagent_win32_7.XXX.srh`

`stormshieldagent_win32_7.XXX.sru`

The server will then propose the update to the agents connected to the server.

6.0 environment configuration

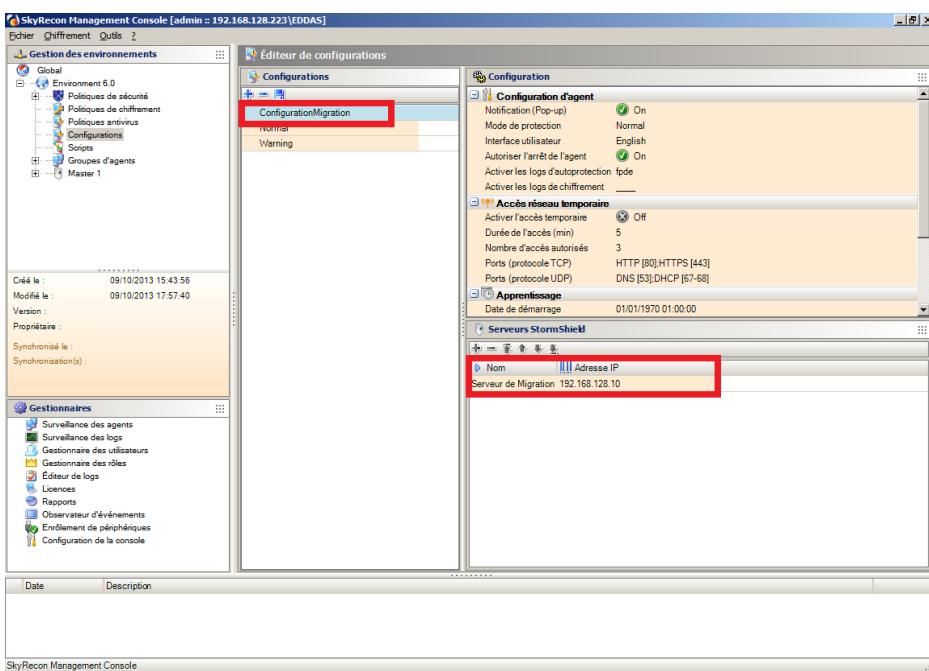After the 7.2 environment has been configured, the 6.0 environment can still be updated with a 6.0 management console.

To enable a selected 6.0 agent group to migrate, declare the transition server in the 6.0 configuration.

Creating a new agent configuration

You need to create a new agent configuration in the 6.0 console.

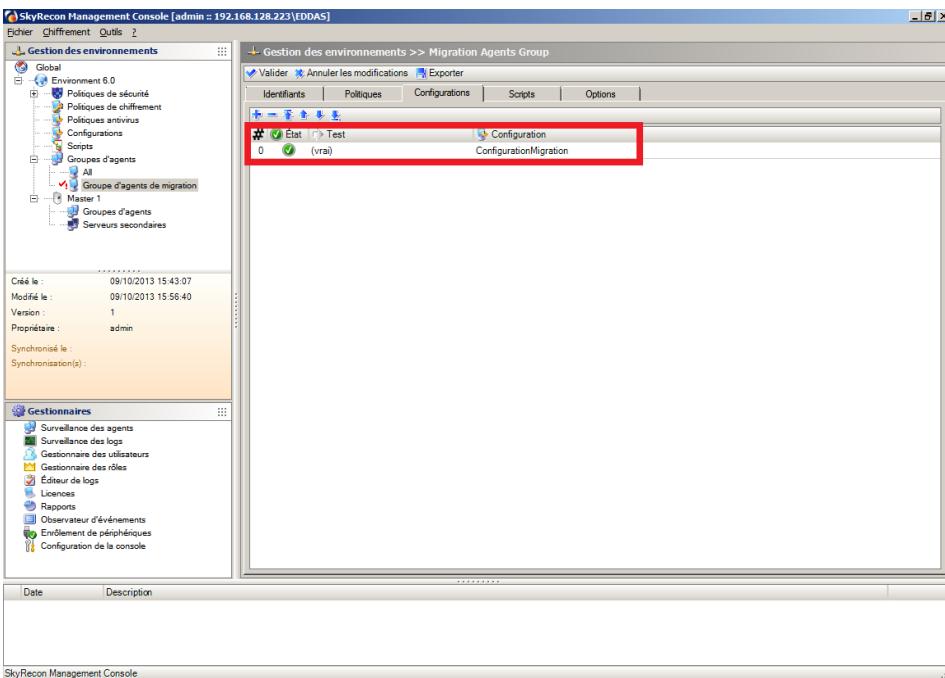You do not need to configure anything in the configuration itself.

Before validating the configuration, remove the 6.0 server(s) in the Stormshield Endpoint Security *servers* tab and then add a new server. This new server is actually the transition server. Enter its IP address (in this case 192.168.128.10).

Creating and configuring the "migration" agent group

After validating the transition configuration, you need to create an agent group. This group includes the workstations that need to be migrated.
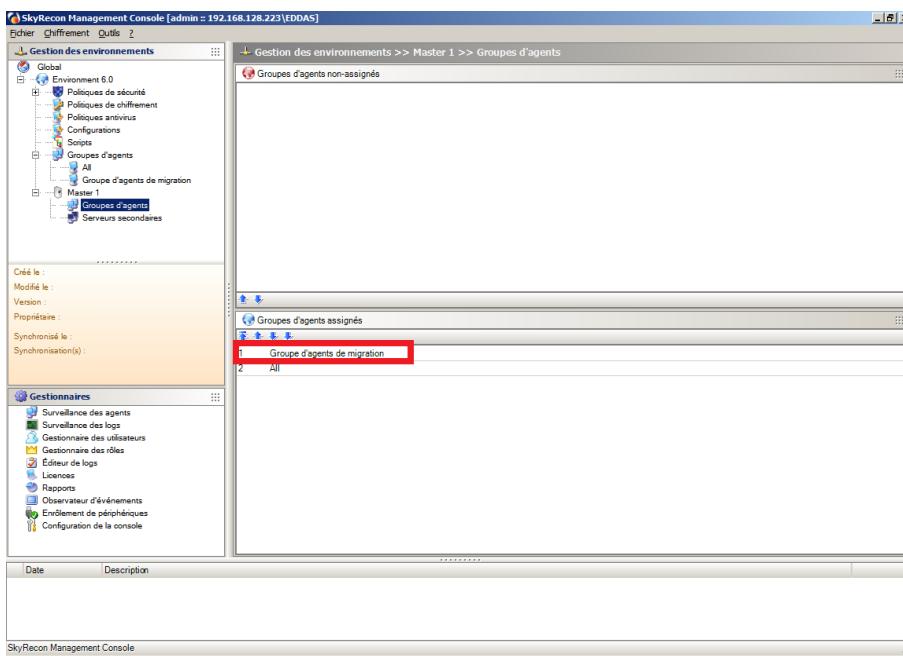
Once you have created the group, apply the **Agents transition** configuration on it with the test **true** and validate.

This agent group must be configured with the policies and configurations already applied on agents. If an agent had an encryption policy, the migration group must also contain this policy. It is possible to create several transition groups in order to migrate agents belonging to different groups in 6.0.

Assigning the agents group to the 6.0 server

The created agents group must be assigned to the existing 6.0 Masters.

Application of changes to the environment

Once the agent group has been assigned, deploy changes to the environment.

Updating agents

When changes are applied to the 6.0 environment, the migration process automatically starts. Agents which must be migrated connect to the transition server after reconnecting to their 6.0 server.

The automatic and silent update is applied to agents. Users will be prompted to restart their workstation.

You can set the reconnection time in the 6.0 Master server configuration which is assigned to the transition agents group (**Reconnection time** setting in the transition server configuration in the 6.0 console; the default value is 5 minutes).

Agents automatically apply policies configured in the 7.2 environment.

Checking version

To check whether the agent was successfully updated, open the agent interface by double-clicking on the Stormshield Endpoint Security icon in the taskbar and check the version number at the bottom right.

All updates, successful or unsuccessful, are recorded in the logs available from the interface.

4.2 Updating Stormshield Endpoint Security 7.2

4.2.1 Requirements

Saving databases

> **NOTE**
> The Stormshield Endpoint Security databases include:
> - The configuration databases.

- Log and monitoring databases.

- Encryption key databases.

NOTE
To back up your database in a directory other than the default directory (example:
`.\Mssql\Backup`), assign Read/Write rights to the security group
`SQLServer2012MSSQLUser$NomDuServeur$InstanceSQL`.

Saving the configuration databases, encryption key databases and log and monitoring databases
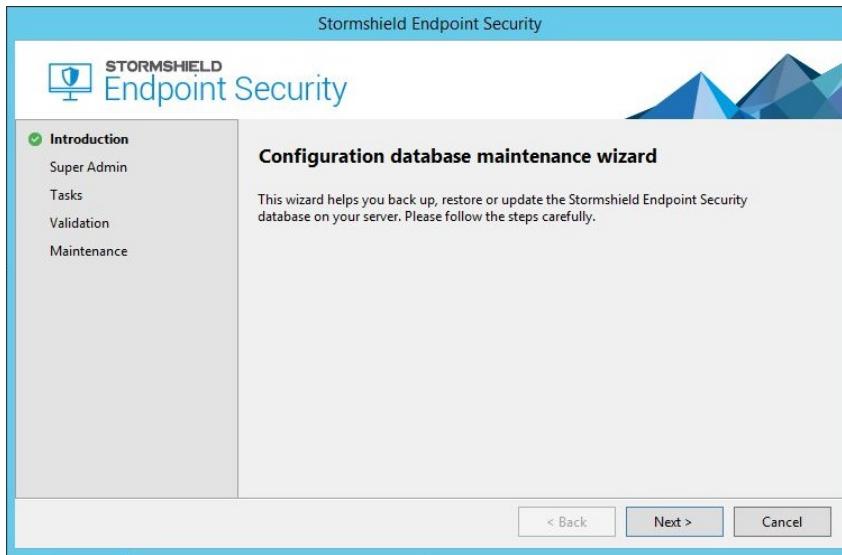
To save the configuration or encryption keys databases, follow the steps below:

1. Close the management console.

2. Launch `DbInstaller.exe` located by default in (also directly accessible from the `Start` menu):

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security
   Management Console\DBInstall
   ```

   This will start the Stormshield Endpoint Security database management tool.

3. Select **Configuration databases maintenance** or **Encryption key databases maintenance** (the log and monitoring databases cannot be backed up with the DBInstaller).

4. Click **Next** to open the window that establishes a connection to the Stormshield Endpoint Security database.

5. Select the Windows authentication or the authentication via the SA MSSQL account. You must use an account with the sysadmin rights on the SQL instance on which SES is installed.

6. Enter the IP address or the NetBIOS name of the database server. If there are several instances, precise the one on which you want to perform the operation.
   Example: [`database IP instance]\SES`.

7. Click on **Next**.

8. Below **Operation type**, click the **Backup** radio button.

9. Click ⊡ to select the backup filepath and enter a backup filename. Click **Save**. The backup will be saved on the machine that hosts the database.

10. Click on **Next**.

11. A summary is displayed. Click on **Next**.

12. Click **Finish** to complete the backup.

Download updates

Before updating Stormshield Endpoint Security, you must first download the update files using the link provided.

> ### ⓘ NOTE
> If you only wish to update the Stormshield Endpoint Security server, download only the server update.

For any higher version of Stormshield Endpoint Security 7, there are **six** patch files to be downloaded:

- **Server**:
  - ° `stormshieldserver_win32_7.2xx.srh`
  - ° `stormshieldserver_win32_7.2xx.sru`
- **Console**:
  - ° `skyreconconsole_win32_7.2xx.srh`
  - ° `skyreconconsole_win32_7.2xx.sru`
- **Agent**:
  - ° `stormshieldagent_win32_7.2xx.srh`
  - ° `stormshieldagent_win32_7.2xx.sru`

Explanations:

- The symbol **xx** corresponds to the update version number.
- Files with a **.srh** extension are patch headers.
- Files with a **.sru** extension are patch update files.
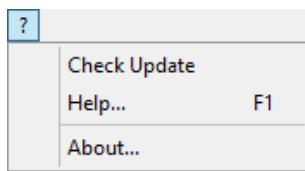- Patch headers are used to authenticate patch files.

During the update process, files with the extension *.srr* and *.srv* are automatically generated by the server and the agent. These internal files are necessary for the update process. You can delete them at the end of the process.

4.2.2 Complete update

Update mode

The console and the databases can be updated on demand.

For the console, click ? and select **Check Update**.

> ⚠️ **WARNING**
> The 7.2 management console uses .NET Framework n.n.n: Ensure that it is installed before the console is updated.

For the databases, use the DBInstaller utility. Refer to Updating Stormshield Endpoint Security databases.

For the server and the agent, the update modes can be configured from the management console via the server configuration policy in **Environment Manager > Server configuration > [server configuration policy name] > Software Updates Settings**.

The parameters for updating Stormshield Endpoint Security components are the following:

⊞ ⬇ Software updates	
Frequency of update checks	03h00m00s
Updates download folder	
Default update to deploy (ex: 7.2.23)	Latest version

- **Frequency of update checks**:

  This is the frequency (for example every 03h00m00s) with which the server and the agents check if updates are available.

- **Updates download folder**:

  This is local folder or Windows share where the updates are located.

- **Default update to deploy**:

  This is the maximum number of the Stormshield Endpoint Security version applied to the agents.

  If you do not wish to use this parameter, select **Latest version**. Agents will automatically be updated to the latest Stormshield Endpoint Security version.

  If you wish to use a specific version, the agents will not be updated to a higher version than the one selected.
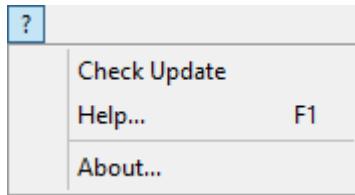
Updating the management console

To update the management console, follow the steps below:

1. Copy the console update files in the `patchs` folder located by default in the Stormshield Endpoint Security server installation directory in:

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security
   Server
   ```

2. On the console, click ? and select **Check Update**.

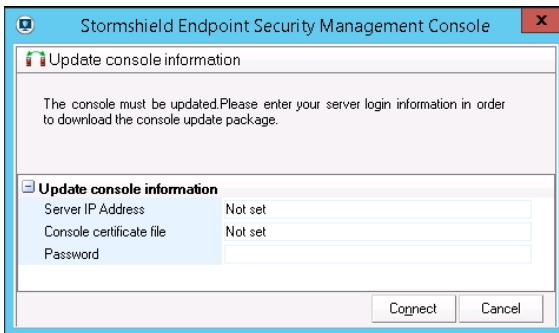 | ? | |
   |---|---|
   | Check Update | |
   | Help... | F1 |
   | About... | |

   > ⚠️ **WARNING**
   > The SES 7.2 management console uses .NET Framework n.n.n: Ensure that it is installed before the console is updated.

3. A dialog box opens to inform you that an update is available.
   Click **Yes** to install the update.

4. To update other consoles, follow the steps below:

- Start the consoles.

- A dialog box warns that the version of the database is not the same as the console version. Select **Yes** to proceed.

- The update window opens.

- Update the following console information using ⊡:

  - Server IP address.

  - Certificate file: Specify the path to the **Console certificate file**. This file protects communications between the principal server and the console.

  - Passphrase: Enter the password set when installing the server to prevent any illegal use of certificates.

5. Click **Connect**. The management console opens:

   ⚠️ **WARNING**
   The version of the Stormshield Endpoint Security databases (configuration databases, log and monitoring databases and encryption key databases) must match the console version. If required, update databases.
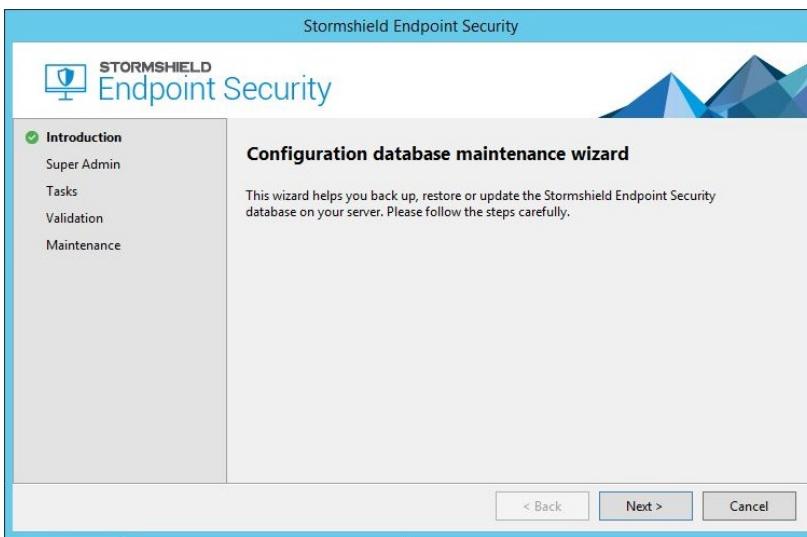
   ℹ️ **NOTE**
   In the case of an update from a version previous to SES 7.2.09, make sure to verify the policies and configurations applied to the Active Directory. From this version, the **Environment** node contains the default policies whereas previously the policies were applied to the Active Directory roots. For example, it is possible that an agent which is no longer in the Active Directory applies the SES default policies after an update.

Updating Stormshield Endpoint Security databases

Updating the configuration database

To update the database configuration, use the DBInstaller utility which is directly accessible from the **Start** menu.

1. Launch `DbInstaller.exe`.

2. Select **Configuration database maintenance**. The following window displays.

3. Click on **Next**.

4. Select the Windows authentication or the authentication via the SA MSSQL account. You must use an account with the sysadmin rights on the SQL instance on which SES is installed.

5. Enter the IP address or the NetBIOS name of the database server. If there are several instances, precise the one on which you want to perform the operation.
   Example: [`database IP instance]\SES`

6. Select **Update**. Click on **Next**.

7. Check information. Click on **Next**.

8. Wait until the update process is completed. Click **Finish**.

Updating the log and monitoring databases

1. It is recommended to have at least 1.5x the size of the log and monitoring database (`.mdf` files) available on your machine.

1. Launch `DbInstaller.exe`.

2. Select **Log and monitoring databases maintenance**.

3. Follow the same steps as those in **Updating the configuration database**.

If you use the **Professional Edition** package, the update process is over.

If you use the **Secure Edition** package, refer to **Updating the encryption key databases**.

Updating the encryption key databases

If you use the **Secure Edition** package, follow the steps below:

1. Launch `DbInstaller.exe`.

2. Select **Encryption key databases maintenance**.

3. Follow the same steps as those in **Updating the configuration database**.

The update process is over. You can now use the management console.

You can now update the Stormshield Endpoint Security server and agents.

Updating the Stormshield Endpoint Security Server

To update the server, follow the steps below:

1. Copy the server update source files in the `patchs` folder located by default in the Stormshield Endpoint Security server installation directory in:

```
C:\Program Files\Stormshield\Stormshield Endpoint Security
Server
```

2. The server will automatically update according to the settings defined in **Environment Manager** > **Server Configuration** > **Software Updates Settings**.

3. When the Stormshield Endpoint Security server begins the automatic update, the `updater.sro` file appears in the `patchs` folder.

   The update runs in background mode and takes about five minutes.

   When the update is completed:

   ◦ The `updater.sro` file is removed.

   ◦ The `log.txt` file is created in the `Log` folder which is located at the root of the Stormshield Endpoint Security server.

   ◦ The server also sends updates to the others servers. The additional servers share the same update process as the principal server.

4. Reboot the server on which server updates are installed. The reboot can be postponed but the update of the Stormshield Endpoint Security server service (`srservice.exe`) is required.

   > **ⓘ NOTE**
   > The configuration of the Apache server is not updated when the Stormshield Endpoint Security server is updated from a version previous to 6.0.18 or 7.2.06. You can manually apply updates by executing «skyapache.exe --update» located in `Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\conf` from an administrator command line. The former configuration files are renamed httpd.conf.old and ssl.conf.old. Restart the Stormshield Endpoint Security server to apply these modifications.

Updating the Stormshield Endpoint Security agent

There are two ways to update the Stormshield Endpoint Security agent:

- Automatic update.
- Manual update.

Auto update

Copy the agent update files in the `patchs` folder located by default in the Stormshield Endpoint Security server installation directory in:

```
C:\Program Files\Stormshield\Stormshield Endpoint Security Server
```

> **ⓘ NOTE**
> If an agent connects to an additional server, the server will download the updates from the principal server in order to distribute them to the connected agents.

If the version of the update available in the server directory is lower or equal to the limit specified in the static agent configuration or in the server configuration (if there is no limit specified in the static agent configuration), agents will download the update and install it automatically. The user does not need to do anything.

The update is applied only after the agent has been rebooted. However, Stormshield Endpoint Security continues to protect the computer until it reboots.

Manual update

> ⚠️ **WARNING**
> The agent must be able to connect to the Stormshield Endpoint Security server to be manually updated.

To manually update the server, follow the steps below:

1. Check the agent version by opening the `version.sro` file located in:

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security
   Agent\Srend.exe
   ```

2. Rename the update file by changing the version number to match the agent version currently installed.

   For example, if you are updating from version 7.2.01 to version 7.2.08, rename the update:

   ◦ `stormshieldagent_win32_7.208.srh` with `stormshieldagent_win32_7.201.srh`

   ◦ `stormshieldagent_win32_7.208.sru` with `stormshieldagent_win32_7.201.sru`

3. Copy the agent update files in the `patchs` folder located by default in the agent installation directory in:

   ```
   c:\Program Files\Stormshield\Stormshield Endpoint Security
   Agent\
   ```

4. To update immediately, force the agent to connect to the server:

   ◦ Right-click the Stormshield Endpoint Security 🛡 icon in the taskbar.
   ◦ Go to **Other operations > Reconnect to server**.

   A notification and a message in the Stormshield Endpoint Security agent's user interface will be displayed when the update is completed.

   Changes made to the agent will be applied after reboot.

5. Reboot the computer when receiving the reboot notification issued when the update is completed.
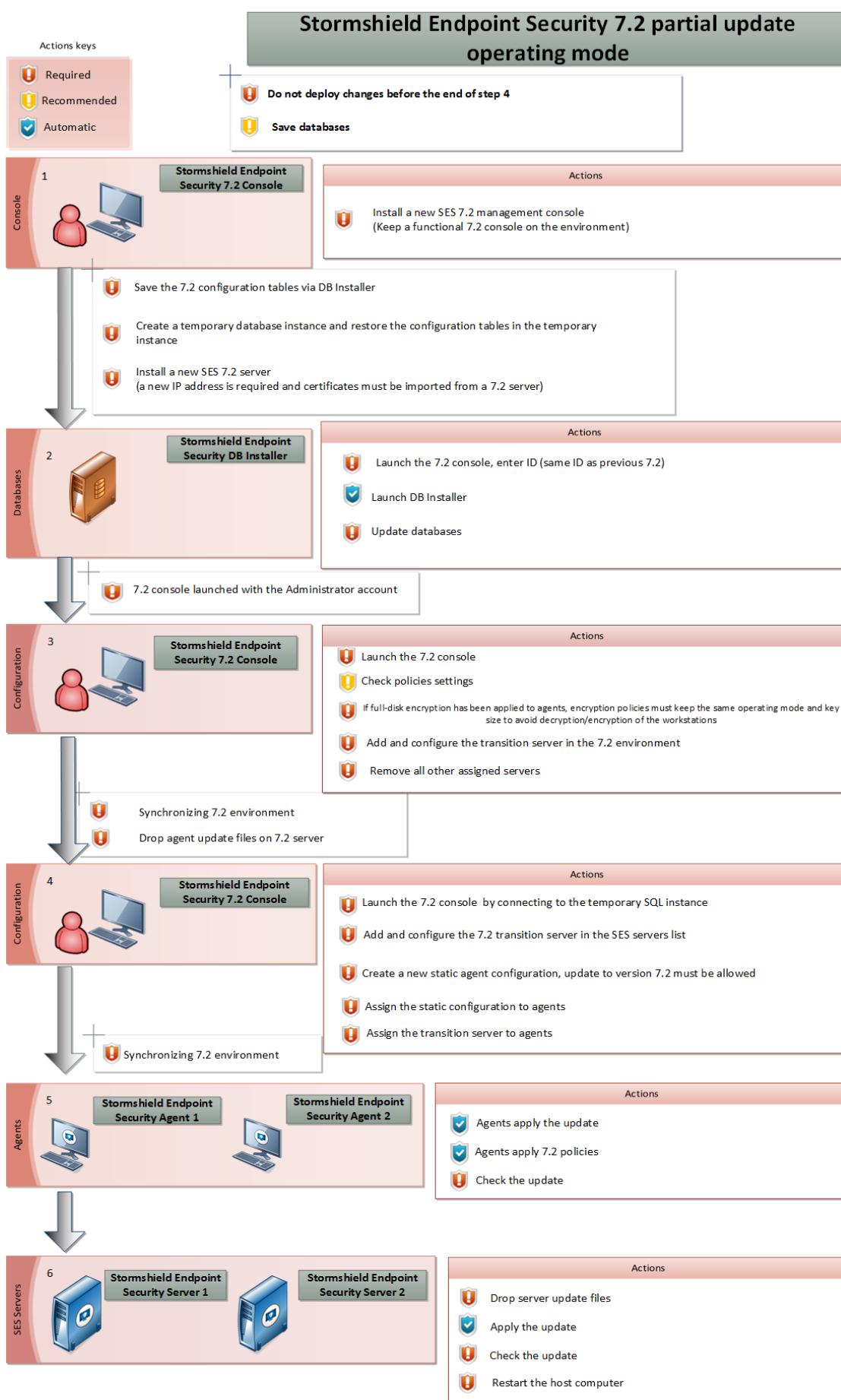
4.2.3 Partial update

This partial update mode makes it possible to gradually update a pool of SES agents from an older 7.2 version to the latest 7.2 version.

To perform a partial update, you will need:

- A new computer (new IP address) for the transition server,
- A new SQL database instance.

⚠ WARNING

We recommend that you back up each database before updating, as explained in the Requirements section; The DB Installer database maintenance utility allows backing up configuration and key databases with the maintenance menus.

Stormshield Endpoint Security 7.2 partial update operating mode

Actions keys

- 🛡 Required
- 🛡 Recommended
- 🛡 Automatic

🛡 **Do not deploy changes before the end of step 4**

🛡 **Save databases**

1 — Console

Stormshield Endpoint Security 7.2 Console

Actions

🛡 Install a new SES 7.2 management console
(Keep a functional 7.2 console on the environment)

🛡 Save the 7.2 configuration tables via DB Installer

🛡 Create a temporary database instance and restore the configuration tables in the temporary instance

🛡 Install a new SES 7.2 server
(a new IP address is required and certificates must be imported from a 7.2 server)

2 — Databases

Stormshield Endpoint Security DB Installer

Actions

🛡 Launch the 7.2 console, enter ID (same ID as previous 7.2)

🛡 Launch DB Installer

🛡 Update databases

🛡 7.2 console launched with the Administrator account

3 — Configuration

Stormshield Endpoint Security 7.2 Console

Actions

🛡 Launch the 7.2 console

🛡 Check policies settings

🛡 If full-disk encryption has been applied to agents, encryption policies must keep the same operating mode and key size to avoid decryption/encryption of the workstations

🛡 Add and configure the transition server in the 7.2 environment

🛡 Remove all other assigned servers

🛡 Synchronizing 7.2 environment

🛡 Drop agent update files on 7.2 server

4 — Configuration

Stormshield Endpoint Security 7.2 Console

Actions

🛡 Launch the 7.2 console by connecting to the temporary SQL instance

🛡 Add and configure the 7.2 transition server in the SES servers list

🛡 Create a new static agent configuration, update to version 7.2 must be allowed

🛡 Assign the static configuration to agents

🛡 Assign the transition server to agents

🛡 Synchronizing 7.2 environment

5 — Agents

Stormshield Endpoint Security Agent 1

Stormshield Endpoint Security Agent 2

Actions

🛡 Agents apply the update

🛡 Agents apply 7.2 policies

🛡 Check the update

6 — SES Servers

Stormshield Endpoint Security Server 1

Stormshield Endpoint Security Server 2

Actions

🛡 Drop server update files

🛡 Apply the update

🛡 Check the update

🛡 Restart the host computer

Backing up the older environment

Save the current 7.2 environment on a new temporary database instance in order to keep the environment running during the whole update process. The current database instance will be updated to the new 7.2 version.

To back up the database, use the DB Installer utility:

1. Run the **Configuration database maintenance** menu.
2. Choose the Backup option.

Creating and configuring the new temporary database instance

You need to create a new temporary database instance in order to manage the section of the pool that has remained in the older version of SES. To do so, you can use the DB Installer to restore the configuration database that was backed up in the previous step.

This temporary database will be used to manage agents which remain in the older version so that they can be updated gradually to the new 7.2environment.

To do so, you can use the *setup.exe* installation file in the new version by selecting all the options except certificate generation as you will need to reuse the same certificates as those used in the older environment.

1. Connect to the temporary database instance with DB Installer,
2. Run the **Configuration database maintenance** menu.
3. Choose the Restore option and select the backup file from the previous step.
   You may delete the temporary database when all the agents have been updated to the new 7.2 version.
4. Log on with a console that has remained in the older version on this new database,
5. Check that it has been properly restored,
6. Deploy the changes in the environment (which has not yet been updated) with the new database; this will allow you to manage servers and agents that have remained in the older version.

Setting up the new version of the 7.2 environment

Updating the management console

⚠ WARNING
At least one management console must be kept in the older version to keep an operational environment for agents that have remained in the older version.

The partial update process starts with the installation of one or more management consoles with the new 7.2 version. To install management consoles, you can either update the consoles or install a new console.

Updating

This option consists of using the console update mechanism by dropping the two files below in the `patchs` folder of the SES server (XXX being the current version):

```
skyreconconsole_win32_7.XXX.srh
skyreconconsole_win32_7.XXX.sru
```

Once these files have been dropped:

1. Run the console again as an administrator (administrator privileges are required for the installation of the update),
2. Click on the "?" menu,

3. Select the search for updates,

4. Accept the suggested installation.

New installation

Install the console as usual on a new workstation by using the SES setup and checking the **Console Only** option as the installation type.

If you are installing a new console, you need to import the console certificate from the older 7.2 environment.

Installing the transition server

To carry on with the partial update process, you need to install a new 7.2 server, which will be a transition server.

Install the server as usual by using the SES setup and checking the **Server only** option as the installation type.

Certificates must not be generated but imported from the older 7.2 server in your pool.

> ⚠️ **WARNING**
> The IP address of the transition server must be a new one. It cannot be an IP address from a server still listed in the console.

Updating databases and configuring the 7.2 environment

> ⚠️ **WARNING**
> Do not click on **Deploy to the environment** before the end of this step.

Once the transition server has been installed, use the 7.2 console to connect to the original instance (which will be updated). The DB Installer database maintenance utility automatically opens. It allows setting up and applying updates to the structure and contents of the configuration, alerts and keys databases. Proceed with the database update.

For more information on installing the 7.2 environment, refer to section Updating Stormshield Endpoint Security databases.

Configuring the newly updated 7.2 environment

Setting up the transition server

When all update steps are completed, restart the console in order to add the transition server to the list of available SES servers for the new 7.2 environment. Then configure the server:

1. Add the transition server to the list of servers for the environment.

2. Assign the server's configuration policy to it and confirm in order to view it in the list of available servers.

3. Link it to the environment so that it becomes "global server".

4. Delete all other assigned servers.
    You must keep only the transition server in the list of SES servers for the updated 7.2 environment. Only servers that have already been updated to the latest 7.2 version must be listed in this environment.

5. Deploy changes in the environment and finalize the update.

Dropping agent update files on the transition server

To update agents, drop the two files below in the *patchs* folder of the transition server (XXX is the new version):

- stormshieldagent_win32_7.XXX.srh
- stormshieldagent_win32_7.XXX.sru

Configuring the 7.2 environment that has remained in the older version

After the new 7.2 environment has been configured, the older 7.2 environment can still be updated with a management console that has remained in the older 7.2 version.

In order to update targeted agents:

1. Connect to the temporary SQL instance with a management console that is still in the older 7.2 environment.
2. Next, add the 7.2 transition server to the list of SES servers.
3. Configure it by applying a server configuration policy.

> ℹ **NOTE**
> From version 7.2.22 onwards, the 7.2 server will not apply what a console in a lower version may send to it.

Creating a new agent configuration

Create a configuration to inform agents to get updated:

1. In the console that manages the environment that has not yet been updated, create a new static agent configuration. This configuration must allow agents to update to the new 7.2 version.
2. Apply this configuration to the targeted agents.

Assigning the transition server to agents

After the static configuration has been applied to agents:

1. Assign the transition server to them by linking the server to the group of agents, an Active Directory group or an organizational unit that contains agents that need to be updated.

> ⛔ **WARNING**
> Do not assign the transition server to organizational units, Active Directory groups or agent groups that do not have static configurations allowing updates to a 7.2 version.

2. Deploy changes to the environment.

Updating agents

When changes are deployed to the older environment, the update process automatically starts. Agents that must be updated connect to the transition server after reconnecting as usual to their server which has remained in the older version.

The update is applied automatically and transparently to agents when they connect to the transition server. Users will be prompted to restart their workstation.

Agents automatically apply policies configured in the new 7.2 environment.

Checking versions

To check whether the agent was successfully updated, open the agent interface by double-clicking on the SES icon in the taskbar and check the version number at the bottom right.

All updates, successful or unsuccessful, are recorded in the logs available from the interface.

Updating SES servers

When all agents are in the new 7.2 version, the server(s) can be updated.

Updating

To update servers, drop the two files below in their *patchs* folder (XXX is the new version):

- stormshieldserver_win32_7.XXX.srh
- stormshieldserver_win32_7.XXX.sru

After these files have been dropped, the server will update independently after the period defined in the **Frequency of update checks** setting in the server configuration.

You can also drop these two files in the folder defined in the **Updates download folder** parameter during the configuration of the server. You need to create a file named *version.sro* which only contains the version number of updates to download, in a "7.223" format.

> ⚠ **WARNING**
> Do not update the last server to the updated environment as long as there still are agents that are not yet in the updated version of the environment.

Checking versions

During the server update, the file *update.sro* is created in the *patchs* folder of the server. The file is deleted at the end of the configuration.

To check the server version, open the *version.sro* file in the *conf* folder. You can also see the server version in the **Dashboard > Software logs** panel of the management console. Look up the log with the status 'SERVER_VERSION'.

Restarting

After the update has successfully completed, restart the machine hosting the server in order to update the service of the SES server (*srservice.exe*).

Updating the server to the updated version of the environment

After the server(s) has/have been updated and restarted:

1. Run the new 7.2 management console again,
2. Add the newly updated server(s) to the updated environment,
3. Deploy changes in the environment.

Deleting the temporary SQL instance and the transition server

Once changes have been applied to the new 7.2 environment containing all servers, and once all agents have been updated, you can uninstall the temporary SQL instance.

Before deleting the transition server, ensure that all agents updated to the new 7.2 version are able to communicate with another server if their servers do not respond:

1. In the 7.2 environment, at least one server updated from the pool with the older 7.2 version must be configured as the global server (linked to the environment). This server must be linked to the same agents as the transition server.
2. Deploy changes in the 7.2 environment.
3. In the **Monitoring** > **Agents** panel, check that all agents in the pool are there and have been updated: the column **Agent version** for all agents must display the value of the new 7.2 version.
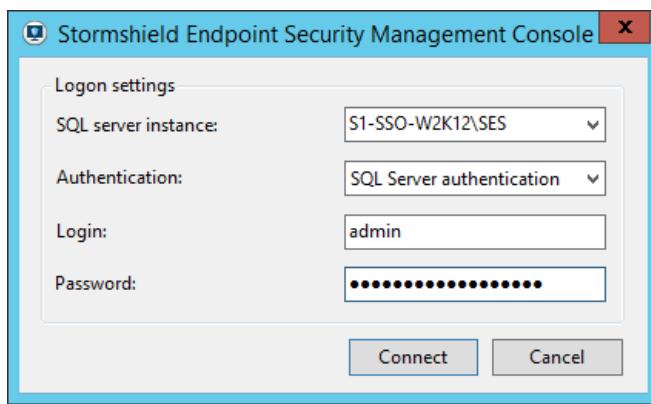
5. Management Console Configuration

5.1 Getting started with the console

5.1.1 Connection with an internal account

To start the management console, select **Start** > **Programs** > **Stormshield** > **Stormshield Endpoint Security** or double-click the management console icon on the desktop:

1. Choose **SQL Server authentication** in the **Authentication** field.
2. Enter the login and password.
3. Click **Connect** to access the management console.
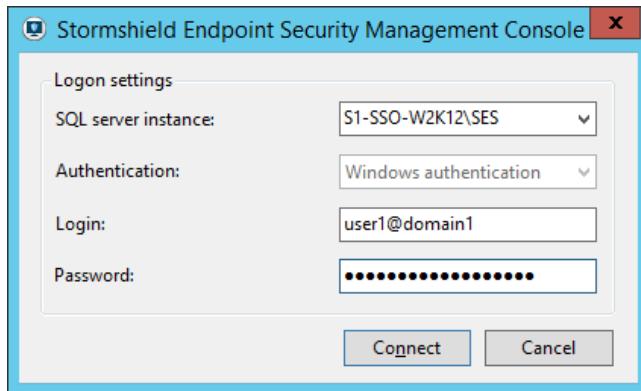
5.1.2 Connection with a Windows account

To connect to the Stormshield Endpoint Security management console with a Windows account, you will need to configure the account in the **Users** section of the console first. Refer to the section "Monitoring" section for help on creating a Windows user.

To start the management console with a Windows account:

1. Choose **Windows authentication** in the **Authentication** field.
2. Enter the login with the format user@domain or domain\user.
3. Click **Connect** to access the management console.

5.2 Console overview

5.2.1 "Environment Manager" section

The **Environment Manager** section is used to manage policies on an internal directory or an Active Directory (domain or forest).

This area manages:

- Policies (security, encryption).
- Configurations.
- Tests and actions.
- Application of policies and configurations on the Active Directory or internal directory objects.
- Server assignment to agents.
- Agent logs configuration.

Policies

Policies are handled in **three** stages:

1. Policy creation:

   Click on the ＋ button to create a new policy, on the ± button to import one or more policies or on the ⊹ button to duplicate an existing policy.

   Types of policies are:

- Server configuration: Stormshield Endpoint Security server configuration policy (mandatory for each server). For more information, see chapter Stormshield Endpoint Security Server Configuration
- Dynamic Agent Configuration: conditional configuration policy of agents deployed on workstations. For more information, see chapter Stormshield Endpoint Security Agent Configuration.
- Static Agent Configuration: enables choosing five scripts remotely executable via a challenge and limiting the agent update. For more information, see chapter Stormshield Endpoint Security Agent Configuration.
- Encryption: full disk encryption, secure file removal and swap cleaning policy. For more information, see chapter Encryption .
- Script: Creation and implementation of your own scripts. For more information, see chapter Scripts.

- Security: control policy for system behavior, applications, device management, network access, wireless network security and kernel components. For more information, see chapter Security Policies

> **ⓘ NOTE**
> Default policies are created when installing Stormshield Endpoint Security for Dynamic Agent Configuration, Static Agent configuration and Security. They apply to each principal node of the domain and cannot be removed. They appear in italics.

> **ⓘ NOTE**
> To rename a policy, including default policies, press F2.

2. Policy configuration:

The policy edition panel is displayed on the right of the console.

The policy version is displayed between brackets in the title of the policy edition panel.

While a policy is edited, a lock icon and the name of the user currently editing the policy are visible by other users connected to the console at the same time. These users will not be able to edit the policy.

Only administrators with the **User Manager** privilege can break an existing lock. In this case, the user whose lock has been removed will not be able to validate changes. An error message will inform him that the policy has been validated by another user. However, he will still be able to export his policy to keep changes that he made locally. To access an up-to-date version of the policy, he will need to use the **Cancel changes** button or refresh the console's Active Directory tree.

- ◦ Policy export:

  You can export a policy into a file in order to store its configuration. The **Export** button is available at the top of the policy edition panel. The generated file has the *.sczp* (Stormshield Console Zipped Policy) or *.scep* (StormShield Console Exported Policy) extensions.

A security policy uses external resources (identifiers and digital signature certificates. For more information, see chapter Security Policies). As such, simply exporting settings is not enough, unlike other policies. Two options are suggested when exporting the security policy:

- export the policy only: allows exporting only the policy settings, without including the various identifiers that the policy uses. The policy must be imported into the same environment and the identifiers used in the policy must not be removed from the console in the interval between the export and import.

- export the policy with its resources: allows creating a full backup of the policy with the identifiers and certificates used in the applicative rules. The policy will be exported in SCZP format.

  - ◦ Policy import:

It is also possible to import a policy. The **Import** button is available at the top of the policy edition panel. For more information, refer to the section Importing security policies.

It is also possible to import policies exported by a previous version of StormShield (from version 6.0 onwards). The extension of exported policies is *.scep*.

A conversion is required because of format differences between versions. A dialog box reminds the administrator of the version of the imported policy and the expected one. After the conversion, a report is displayed. It contains:

- The settings which became obsolete.

- The new settings (with the default values).

- The number of dependencies on other policies, which may have been lost if the other policies are missing.

- Errors on settings.

- The success or failure of the conversion.

When the conversion is complete, it is still possible to cancel the policy import. If the conversion is validated, a file containing a copy of this report is recorded in the user directory for future reference (the complete path is displayed in the console log).

When an action, test or script is imported, some references may be invalid or missing. Such references are displayed in red and must be resolved before checking in the policy.

3. Policy application:

Policies must be applied to Active Directory or internal directory objects displayed in the **Environment** menu of the **Environment Manager** section.

To apply a policy, select the object on which you want to apply the policy. Select the *Policies linked* tab and select a policy.

Click **Deploy to the environment** to update servers.

Active Directory environment management

In Active Directory mode, when an object is selected in the Active Directory tree view, *Policies linked, Servers* and Group tabs are displayed on the right of the console.

For more information about the *Policies linked* and *Servers* tab, see sections Exporting agent groups and Servers tab.

Active Directory environment tree view

Stormshield Endpoint Security servers, whether or not they belong to the Active Directory, are listed in the 🖥 Servers **Servers** panel .

The Active directory tree view enables viewing the organizational units of the domain or forest selected when installing Stormshield Endpoint Security, as well as the Stormshield Endpoint Security groups. Organizational units are shown with the icon 🗁 , domain nodes with the icon 🌐 and Stormshield Endpoint Security groups with the icon 🖵 .

You can also display computers belonging to organizational units by clicking 🖥 .

In the tree view, computers appear with different icons:

- 📄 : Stormshield Endpoint Security server

- 🖥 : computer on which the Stormshield Endpoint Security agent is installed

- ⬚ : computer on which the Stormshield Endpoint Security agent is not installed

Stormshield Endpoint Security group management
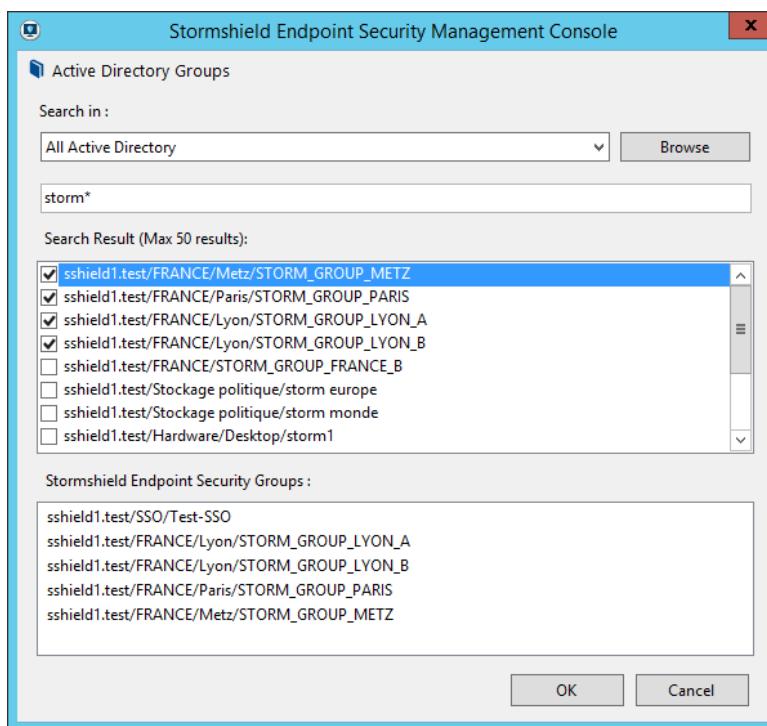
You can apply policies to Active Directory groups rather than to organizational units.

If a computer or Stormshield Endpoint Security group belongs to a Stormshield Endpoint Securityparent group, policies of the parent group apply. A computer or Stormshield Endpoint Security group can only belong to one Stormshield Endpoint Security parent group. The *Group* tab allows viewing the parent of each Stormshield Endpoint Security group.

For more information about the *Group* tab, refer to Group tab.

Stormshield Endpoint Security groups do not inherit policies applied to the organizational unit in which they have been created.

To select groups, click ⬚ . The window **Active Directory Groups** opens.

1. In the **Search in** field, select the Active Directory part containing the searched groups using the drop-down list or the **Browse** button.

2. In the **Search** field, enter the full name or the first few letters of the searched groups.

3. The search results appear in **Search Result**. Check the groups to be displayed in the tree view.

4. Click on **OK**.
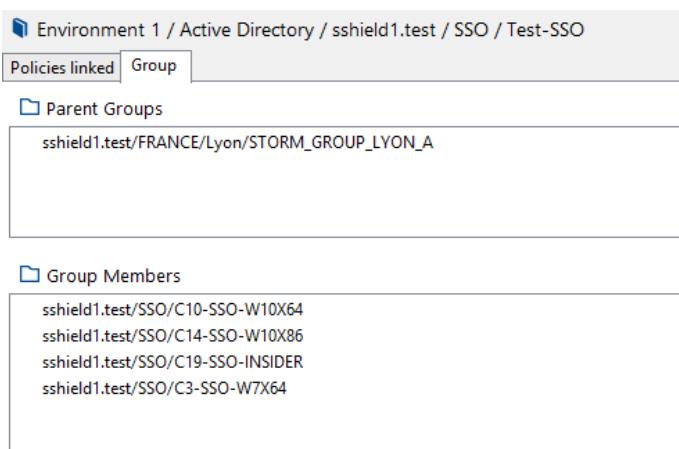
   ### ℹ NOTE
   Only groups created in an organizational unit are displayed in the Active Directory tree view.

When groups are selected in the console to appear in the Active Directory tree view of the **Environment Manager** section, they become Stormshield Endpoint Security groups.

Group tab

The *Group* tab is displayed when a Stormshield Endpoint Security group or a computer is selected in the Active Directory tree view of the **Environment** menu. It is divided into two parts:

the **Parent Groups** panel and the **Group Members** panel.

To consult characteristics of another Stormshield Endpoint Security group of the **Parent Groups** or **Group Members** list, click on the group from the *Group* tab. It is highlighted in the Active Directory tree view of the **Environment** menu.

Internal directory environment management

In internal directory mode, when an object is selected in the directory tree view, *Group, Policies linked* and *Servers* tab are displayed on the right of the console.

For more information about the *Policies linked* and *Servers* tab, see sections Policies linked tab and Servers tab.

Internal directory environment tree view

Stormshield Endpoint Security servers, whether or not they belong to the internal directory, are listed in the Stormshield Endpoint Security **servers** panel   .

The internal directory tree view shows the agent groups represented by the icon   .

To add an agent group, click   to create a new one or   to duplicate an existing group in the tool bar above the directory view.

An internal directory can be renamed if it is not currently being edited by another user.

Create as many internal directories as you need by right-clicking the tree view environment node. However the directories cannot have Stormshield Endpoint Security servers in common.

You may consider using several internal directories only if rules by IP addresses or NetBios names do not allow handling agents precisely enough.

Managing agent groups

Agent groups are defined by two rule types: rules based on IP addresses and rules based on NetBios names. You are allowed to add, remove and rename agent groups.

Rules based on IP addresses allow defining:

- standard addresses (IPv4).

- address ranges (defined by a start address and an end address).

- subnetworks (defined by a subnetwork IP address and a mask).

Rules based on NetBios names allow defining host names:

- standard names can contain letters (a-Z, A-Z), numbers (0-9) and hyphens (-) but no space character or period (.).

- names cannot contain only numbers.
- the following characters are not authorized: ` ! @ # $ % ^ ( ) = + [ ] { } \ | ; : . " # , = @ [\ ] .
- the maximum length is 15 characters.
- the asterisk (*) can be used as a wildcard.

Importing rules in agent groups

You can directly import an IP- or NetBios-based list of rules from a CSV file.

It must be a valid CSV file with two columns. The first column shows the value (IP, IP range, subnetwork or NetBios name). The second column shows the (optional) description of the rule. IP- and NetBios-based rules cannot be contained in the same file.

The CSV file must be exported with semicolons as the separator character and quotation marks as delimiter and escape characters.

CSV data	Interpretation	
COLUMNS: IP/COMMENT	*IP*	*COMMENT*
192.168.0.1;IP	192.168.0.1	IP
192.168.0.5-192.168.0.50;IP range	192.168.0.5-192.168.0.50	IP range
192.168.1.0/24;subnet mask	192.168.1.0/24	Subnet mask
192.168.2.0/24;"network""r&d"""	192.168.2.0/24	network "r&d"
192.168.3.0/24;"accounting service; RH network"	192.168.3.0/24	accounting service; HR network

Moving rules between agent groups

Use the **Move to** button in the IP or NetBios configuration rules to move them in another group. Both groups must be checked out.

Then, check in modifications in both groups.

Exporting agent groups

You can export a group into a file in order to store its configuration (IP- and NetBios-based list of rules). The **Export** button is available at the top of the rule edition panel. The generated file has the SCEC extension (Stormshield Console Exported Configuration).

Importing agent groups

It is also possible to import a group. Create a group first. The **Import** button is available at the top of the rule edition panel. The expected file is the one generated by the console during export, i.e. the SCEC file.

Managing ranks of agent groups

Groups' ranks can be modified in the internal directory node panel.

1. Click the **Internal Directory** node.
2. In the right panel, click the tab *Agent groups ranks* and then click **Check out**.
3. Use the arrows to change the rank.

An agent belongs to the first group in which it matches a rule (IP matching the agent IP, agent IP matching the IP range, agent belonging to the subnetwork or NetBios name matching the agent name).

The directory contains all the agents which do not belong to any group.

Managing multi-console edition

A lock system guarantees data integrity when several users edit the agent groups configuration at the same time.

There are two types of locks:

- Directory lock: prevents ranks from being edited and adding/removing agent groups.

- Agent group lock: prevents editing of agent group names and manipulation of its data (IP addresses, IP address ranges, etc.).

When User A is editing the directory, User B cannot edit group ranks or add/remove agent groups at the same time.

When User A is editing an agent group, User B cannot edit the same group at the same time, i.e. edit the group name or data.

Moreover, when User A locks the directory, User B cannot edit the agent groups of this directory. User A can continue editing any agent group.

Finally, when User A locks an agent group, User B cannot edit the directory but he/she can edit other agent groups (not locked).

While User A is editing a directory or agent group, a lock icon appears for other users indicating that the directory or agent group is currently being edited and the name of User A is shown between brackets next to the name of the edited element.

Stormshield Endpoint Security servers management

All Stormshield Endpoint Security servers are listed in the **Stormshield Endpoint Security servers** panel. This menu indicates the status of each server.

It is possible to define other IP addresses for each server (agent synchronization IP). This way, agents contact them via an IP address different to the one used by the console for updates. This panel also enables choosing the server configuration policy to apply to each server.

Each server can belong to only one internal directory and/or Active Directory.

The directories to which a server belongs (if any) is displayed in the **Directory** column and is read-only.

When the Stormshield Endpoint Security administration console relies on an Active Directory, it is possible to add one or more internal directories to complete agent management.

It is thus possible to manage agents (whether they are in the Active Directory or not) through their IP address or NetBIOS name.

If you need to manage two agents with the same IP address and/or NETBIOS name in an internal directory, you have to create a second internal directory and assign a dedicated server to it.

Be careful to take into account this difference when installing agents. Each agent must be installed with the package generated by one of its assigned servers.

After a server has been assigned to a directory (internal or Active Directory) and has been synchronized, it must not be reassigned to another directory to avoid directing agents from the former directory to the new one.

Policies linked tab

The list of policies assigned to the environment, to a directory, to an Active Directory object or to an agent group is displayed by policy type.

You can select an application condition for each Dynamic agent configuration, Script and Security policy. Tests created in the **Script Resources** folder are available in the listed conditions. For more information about tests, refer to Tests.

To set a policy priority order, use the arrows at the top of the panel. To change the order, the object on which policies are directly applied must be selected in the Active Directory tree view. These policies are displayed on a white background.

For each policy type, the agent applies the first policy satisfying the condition. For each policy type, if listed policies have similar conditions, only the first policy is applied. The following policies are crossed out in the list.

In the Active Directory, if some policies are applied to computers, Stormshield Endpoint Security groups, organizational units and domains at the same time, then the checking order of policies to apply is:

- computer

- Stormshield Endpoint Security group and Stormshield Endpoint Security parent groups

- organizational unit and parent organizational units

- domain

- environment

For each policy type, if no condition is matched, the default policy assigned to the domain applies to Stormshield Endpoint Security agents.

In the internal directory, the policies applied are the policies of the group to which the agent belongs, if they are defined.

If some policy types are not defined in the agent group, the policies applied are the default policies defined at the environment root.

> ⚠ **WARNING**
> If there are policies defined in several agent groups, the policies of the first group to which an agent belongs apply for this agent, whatever the rank of its group. If policies are defined in groups which rank is superior to the group of an agent, they will not apply to this agent.

Servers tab

This tab enables the selection of servers to assign to a directory, organizational unit or agent group. The Stormshield Endpoint Security server set up during the installation procedure is assigned by default to the environment.

Servers assigned in the *Servers* tab distribute policies to agents and receive logs from the agents.

A load balancing system defines the choice of the server by the agent. To better distribute the agent load among the servers, an agent connects to a server randomly selected among those assigned at the closest hierarchical level of organizational units in Active Directory mode. In internal directory mode, the only hierarchy is the directory itself which is considered as above the agent group.

In case the server to which the agent connects cannot be reached, the agent turns to another server within the same level (organizational unit or agent group). In the same way, if a server rejects an agent because it is overloaded, the agent is redirected to another server within the same level. Finally, if all servers of the same level are overloaded, the agent forces the connection to an overloaded server. The latter cannot reject the connection and a log message is sent to notice the administrator of the servers overload.

In Active Directory mode, when all servers of the hierarchically closest OU cannot be reached, the agent selects the server from the next OU, until no more OUs contain servers.

In internal directory mode, when all servers of the agent group cannot be reached, the agent selects the server among the servers assigned to the directory itself.
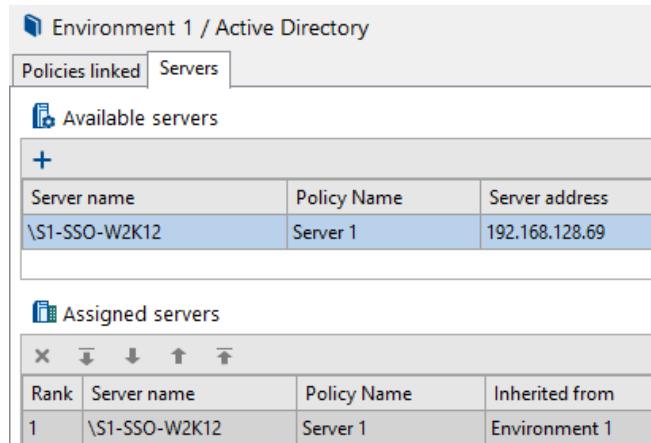
For the Active Directory and the first internal directory, if no server is available, the environment server(s) will be used.

If there are any other internal directories, the servers linked to the directory itself only will be used.

As soon as a server configuration policy has been assigned to them, Stormshield Endpoint Security servers listed in the Stormshield Endpoint Security **servers** panel of the environment appear in part **Available servers**.

If a server is already assigned to another directory, it will not be available. The line is grayed out and it is not possible to link the server to an object.

1. Click ➕ to add an available server in the list of assigned servers.
2. Use the arrows to change the order of assigned servers. Agents communicate in priority with the first server of the list. If the server does not respond, the agent tries to connect to the following servers.

For more information on communication between servers and agents, see section Deploying policies on agents and collecting logs.

3. In internal directory mode, if a server is not assigned to any agent group, a message is displayed and indicates that the application of changes to the environment is not possible as long as the server is not assigned or removed.

4. If you remove a server from the console, ensure that you shut down or uninstall the server to avoid disrupting agents.

Log Manager

The **Log Manager** menu is used to customize log messages and Stormshield Endpoint Security agent notifications.

It is used to select where logs will be reported:

- Agent event logs (user interface).
- Pop-up window.
- Database.
- Third application (Syslog or SMTP).

Logs are systematically written into the local log file.

For more information, see the section Log Manager.

5.2.2 "Monitoring" section

The **Monitoring** section is used to manage and monitor the elements below:

- The dashboard.
- The agents.
- The Software logs sent by the agents.
- The System logs sent by the agents.
- The Network logs sent by the agents.
- The Device logs sent by the agents.
- The reports.

Dashboard

The administrator can see the status of all the agents in the **Dashboard** menu, thanks to various indicators. This panel allows a quick overview of the information sent by all the agents when opening the console.

For more information, see Dashboard.

Agents

This menu provides the administrator with a clear and global view of the agent status to check the versions of policies and agents.

For more information, see Agent monitoring.

Software Logs

The **Software logs** menu displays any activity of the agents related to their action on client and server workstations.

System Logs

The **System logs** menu displays any activity of the agents on client and server workstations related to the protection of the operating system and the corresponding reaction of the Stormshield Endpoint Security agent.

Network Logs

The **Network logs** menu displays any activity of the agents on client and server workstations related to the protection of the network firewall part and of the intrusion detection system and the corresponding reaction of the Stormshield Endpoint Security agent.

Device Logs

The **Device logs** menu displays any activity of the agents on client and server workstations related to the devices control and to the WIFI and the corresponding reaction of the Stormshield Endpoint Security agent.

Reporting

The **Reporting** menu displays real-time and historical reports. These reports are used to collect and consult information on:

- Agents.
- Servers.
- Policies.
- Configurations.
- Removable devices.
- Licenses.
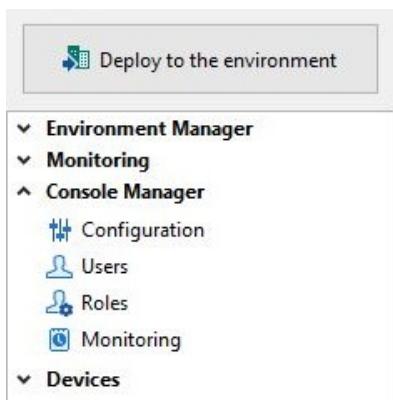
For more information, see Stormshield Endpoint Security Reporting.

5.2.3 "Console Manager" section

The **Console Manager** section is used to manage the elements below:

- The console.
- The console users.

- The roles.
- The events.

Configuration

The **Configuration** menu is used to modify and configure the management console.

The **Configuration** menu includes two areas: **Options** and **Secure Connections**.

Options

In the **Options** area, the administrator can modify the following:

- **Date format**

  You can change the date format used throughout the console. For more information about date format, see Appendix Date and time format strings

- **Layout**

  You can adjust the size of panels and columns and save your modifications.

  > **NOTE**
  > You must restart the console for the new layout to take effect.

- **Console language (You must restart the console)**

  You can change the console display language by using one of the following methods:

  ◦ Double-click in the column on the right until the required language appears.

  ◦ Click in the column on the right, then on the ⊡ button and finally select the required language from the list.

  You must restart the console for the new language to take effect.

- **CSV separator**

  Select the separator character used while importing files in CSV format. Possible choices are:

  ◦ A semicolon ";" (generally used by Microsoft Excel with regional options for "France").

  ◦ A comma "," is used in all other cases.

  > **NOTE**
  > During installation or a migration from an older version to the 7.2 version, the semicolon is used on consoles configured in French. Otherwise, commas are used.

- **Log monitoring database**

  Select the SQL server instance that you want to use to monitor logs.

- **Encryption key database**

  Select the SQL server instance that you want to use to manage encryption keys.

- **Agent monitoring refresh time (sec.)**

  Enter in seconds the refresh frequency for agent monitoring (interval between each refresh).

- **Log monitoring refresh time (sec.)**

  Enter in seconds the refresh frequency for log monitoring (interval between each refresh).

Secure Connections

In the **Secure Connections** area, you can modify:

- The filepath used for the security certificates that protect communications between the console and the Stormshield Endpoint Security server.

- The certificate password set when installing the server to prevent any illegal use of the certificates.

Users

This area is used to define the users who can access the management console, and the roles assigned to them.

To add an internal user (SQL) or a Windows user (Active Directory), follow the steps below:

1. Click on **Users**.
2. Click on the ➕ button at the top of the window.
3. Select the user type: SQL user or Active Directory user.

SQL user

1. Fill in the **Login** and **Password** fields.

   > ℹ️ **NOTE**
   > A user name must not contain the special characters "\" and "@".

2. Select the role to be assigned to the user.
3. Edit the console configuration settings if needed.

Active Directory user

The following requirements must be met so that a user with a Windows account can use the Stormshield Endpoint Security administration console:
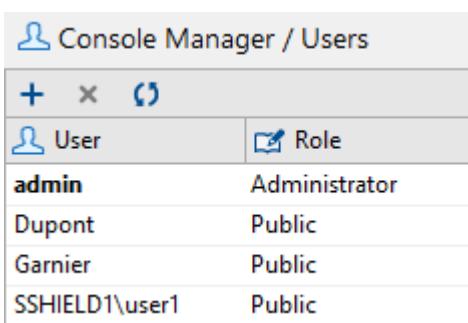
- If the user belongs to a domain other than the SQL server, a trust relationship must be established between both domains.

- If the user belongs to a domain other than the console, a trust relationship must be established between both domains.

   > ℹ️ **NOTE**
   > In general, any user who can "Run as..." on the workstation hosting the Stormshield Endpoint Security SQL instance can be added.

1. Click **Search**.

   ◦ If the user to be added belongs to the Active Directory configured during the installation of the management console, the window **Active Directory Search** opens. Search and select the user name.

- ◦ If the environment is based on an internal directory or if the user belongs to another Active Directory domain, the **AD Credentials** window opens:
    - Fill in the AD credentials and click on **OK**.
    - Select the user search DN to add.
    - Click on **OK**.
    - The window **Active Directory Search** opens.
    - Search and select the user name.

2. Click on **OK**. The **Login** field is automatically filled in.
3. Select the role to be assigned to the user.
4. Edit the console configuration settings if needed.

User	Role
admin	Administrator
Dupont	Public
Garnier	Public
SSHIELD1\user1	Public

Roles

This area is used to create the roles assigned to management console users. These roles are then assigned through the **Users** menu.
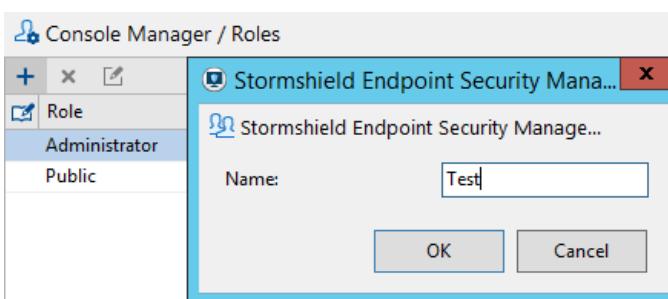
The roles by default are the following:

- **Administrator**:

    Access rights to all operations in the management console.

- **Public**:

    Read-only access rights to some panels of the management console.

The **Roles** menu is used to create and name the users to which roles and environments are assigned.

To add a role, follow the steps below:

1. Click on **Roles**.
2. Click ➕ .
3. Enter the **Name** of the new role and validate.

Console Manager / Roles

Role
Administrator
Public

Stormshield Endpoint Security Mana...

Stormshield Endpoint Security Manage...

Name: Test

OK   Cancel

4. Click the role name in the **Role** column and check the appropriate boxes.

🛑 **WARNING**

Granting too many permissions to a user may compromise security. Make sure you give a role only the required rights for performing the requested operations.

Audit

The **Monitoring** menu displays the actions performed by an administrator of the management console.

Actions such as the following are displayed:

- Sending configurations to the server.
- Assigning policies to a directory object.
- Updating policies.

For more information, see the section Console monitoring.

5.2.4 "Devices" section

The **Enrollment** menu allows enrolling devices which could then be switched to a "trusted" status by a Stormshield Endpoint Security agent.

These "enrolled" and "trusted" statuses allow managing a set of USB drives and checking the contents of removable devices.

For more information, see chapter Removable Device Administration.

5.2.5 Status bar
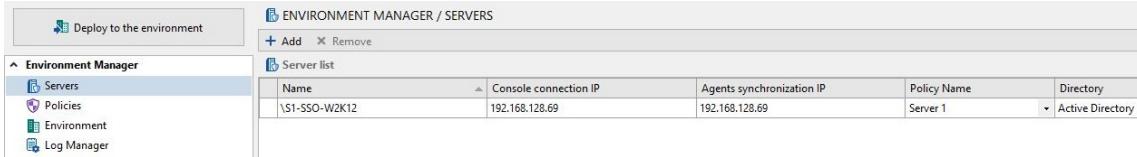
This bar displays the **Date** and **Description** of the status messages related to the operations performed by the console.

ℹ️ 13/07/2018 11:55:28   Changes have been applied to server S3-SSO-W2K12R2

6. Stormshield Endpoint Security Server Configuration

6.1 Stormshield Endpoint Security Server list

Stormshield Endpoint Security servers are listed in the **Servers** panel, which can be accessed via the **Environment Manager** section.

This panel enables adding, editing or deleting a server. It is possible to add servers that are not part of the Active Directory. The panel allows adding servers, in one of the following ways:

- by browsing the Active Directory.

- by typing the IP address (if the server is not part of the Active Directory).

- by typing the NetBIOS name (if the server is not part of the Active Directory).

The **Servers** panel contains the following fields:

- **Name**: if the server is affiliated to a domain, the server name is preceded by the domain name. If the computer name could not be resolved by the management console, the computer IP address is used.

- **Console connection IP**: IP address used by the console to apply changes to the server.

- **Agents synchronization IP**: list of IP addresses that can be used by agents to communicate with the server. This field can be edited and it must contain at least one IP address. Several IP addresses can be defined by separating them with a semi-colon. (example: 192.168.1.1;127.0.0.1) . The agent will attempt to contact these IP addresses in the order in which they have been added to this list.

- **Policy Name**: applied server configuration policy.

- **Directory**: directory to which the server is currently assigned.

- **Last changes applied**: date and time of the last application of changes which succeeded.

- **Status**: indicates whether the server is up to date with the latest versions of policies and configurations transmitted when applying the last changes to the environment.

Select a server in the list in order to display the assignment list (internal directory agent groups or Active Directory objects) for this server in the lower panel.

6.2 Adding an additional Stormshield Endpoint Security server

6.2.1 Declaring an additional server
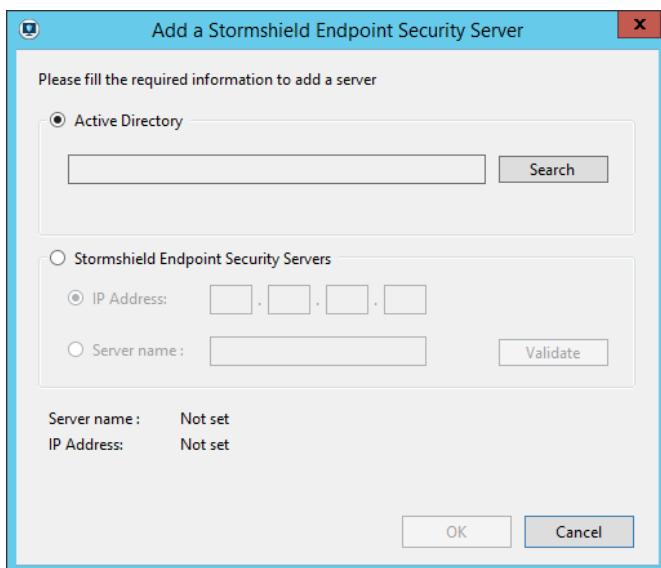
After installing an additional server, you must declare it in the management console. For more information on how to install additional servers, see **Installing additional servers**.

To declare an additional server:

1. Open the **Servers** panel.

2. Click the **Add** button.
The window **Add a Stormshield Endpoint Security Server** opens.

If the server belongs to the Active Directory domain:

1. Select **Active Directory**.

2. Click **Search**.
The window **Active Directory Search** opens.

3. Select the server from the Active Directory.

   The server NetBIOS name and its IP address are displayed in the **Add a Stormshield Endpoint Security Server** window.

4. Click **OK** to add the server in the list.

If the server belongs to the Active Directory domain:

1. Select **Servers**.

2. Select **IP address** or **Host Name**.

3. Enter the NetBIOS name or the IP address and validate.
The server name and its IP address are displayed in the **Add a Stormshield Endpoint Security Server** window.

4. Click **OK** to add the server in the list.

5. Add secondary IP addresses if necessary.

6.2.2 Configuring an additional server

After declaring the additional server, you must assign a server configuration policy and a directory to configure it.

Assigning a server configuration policy

From the **Servers** panel, select the server configuration policy in the column **Policy Name**.

To create the server configuration policy, see section **Creating a server configuration policy**.

Assigning a directory

If the installation is based on an Active Directory, the additional server can be assigned to the whole domain or to an organizational unit (OU).

If the installation is based on an internal directory, the additional server can be assigned to all the directory or to a particular group of agents.

To assign a directory to the additional server:

1. In the directory tree view (internal or AD), click on the node concerned.
2. Open the **Servers** tab.
3. In the list of available servers, assign the additional server with the icon ➕ .

The added server displays in the list of the assigned servers.
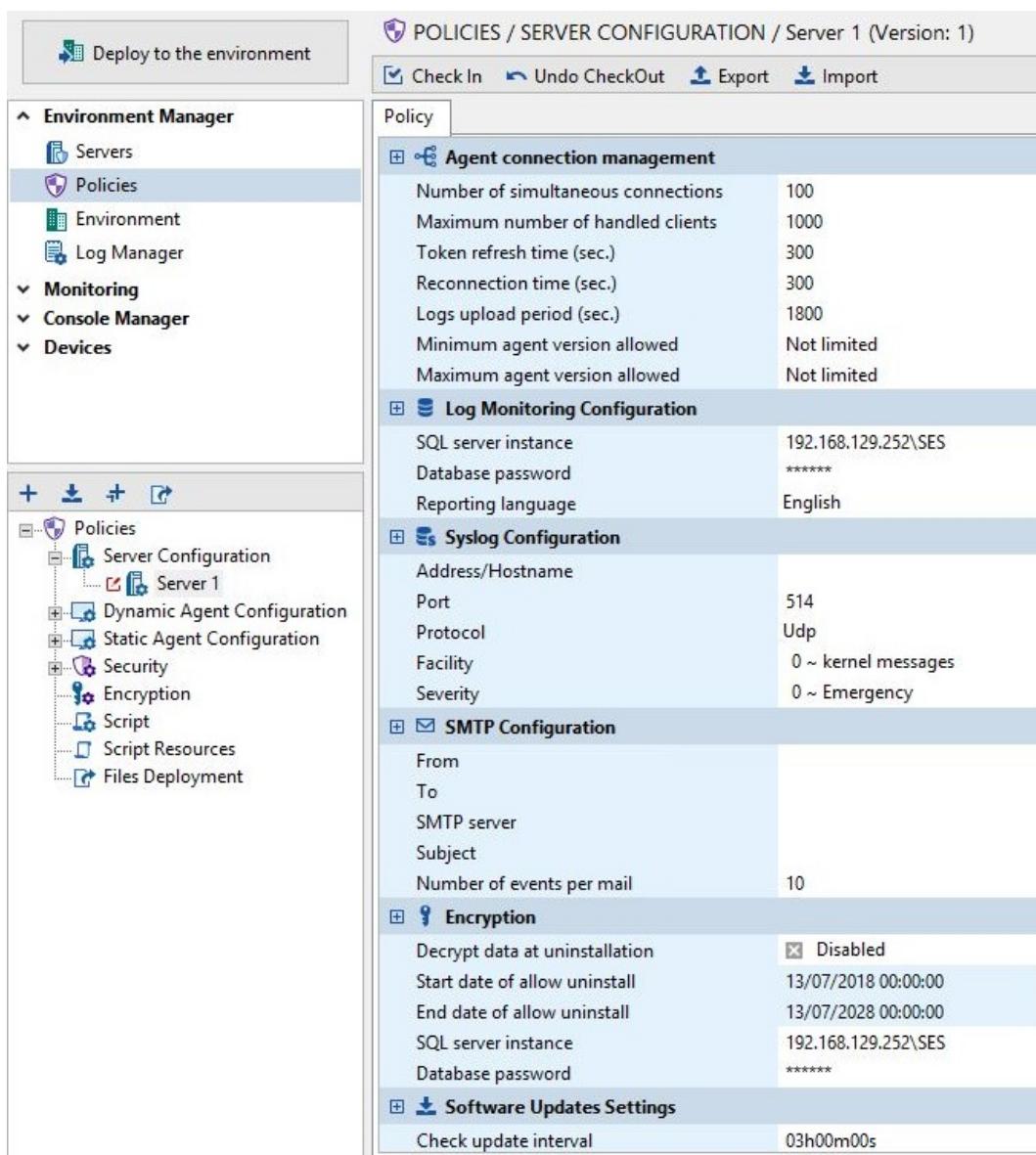
6.3 Creating a server configuration policy

1. Click **Policies** and the ➕ button. The window **Create a new policy** opens.
2. Enter a policy name and select the policy type **Server Configuration**.
3. Click **OK**. The policy edition window opens.

6.4 Editing a server configuration policy

The server configuration policy includes the following areas:

- Agent connexions management.
- Log Monitoring Configuration.
- Syslog Configuration.
- SMTP Configuration.
- Encryption.
- Software Updates Settings.
- Authentication Service.

6.4.1 Agent connection management

The graphical interface of the **Agent connection management** function is displayed as follows:

- **Number of simultaneous connections**:

  This is the number of agents which can connect simultaneously to the Stormshield Endpoint Security server. If too many agents are simultaneously connected to the server, the latter will be regarded as inaccessible for the agents attempting to reach it.

- **Maximum number of handled clients:**

Maximum number of agents handled by a server. When a server reaches this number, it rejects connections of agents which are thus redirected to another server of the same level.

- **Token refresh time (sec.)**:

This is the interval between each token transmission made by the server to the agents. When an agent receives a token, the latter indicates whether the agent has to update its policies.

- **Reconnection time (sec.)**:

This is the time interval between each attempt to reconnect to the server, made by disconnected SES agents.

- **Logs upload period (sec.)**:

Time interval between each logs upload from the agents to the servers. Logs upload is done on a channel different from the channel used to retrieve policies. The port used for logs communication is the 16004 TCP secured port. When it is not available, the policies secured TCP port (16005) is used.

- **Minimum agent version allowed**:

Minimum agent version required to connect to the server. If you do not want to specify a minimum version, keep the default value **Not limited**.

- **Maximum agent version allowed**:

Maximum agent version required to connect to the server. If you do not want to specify a maximum version, keep the default value **Not limited**.
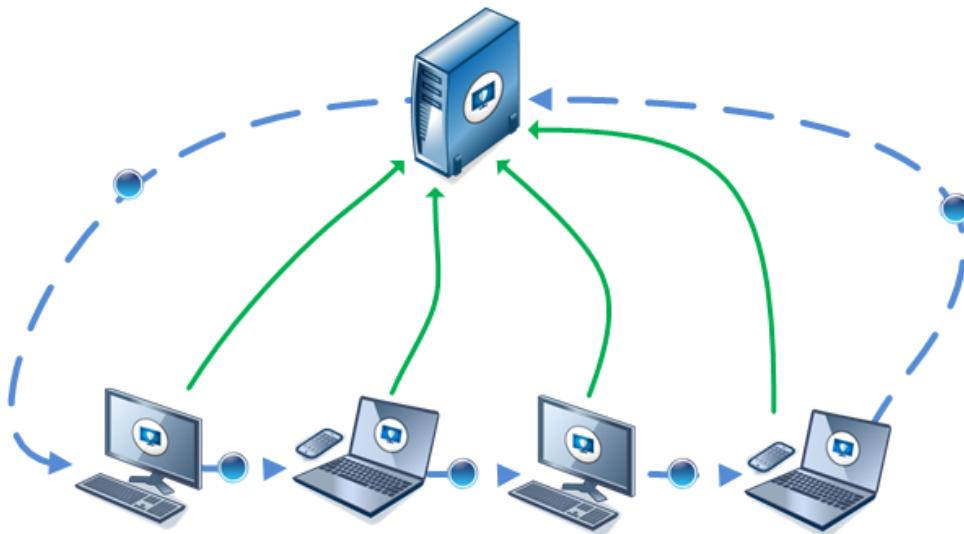
6.4.2 Deploying policies on agents and collecting logs

Security policies are deployed and data on agent activities are collected using **tokens**.

At regular intervals defined by the administrator, the server notifies the agents through the circulation of tokens. These tokens are sent from one agent to another and back to the server.

This communication model protects the network from any denial of service that could be caused by a large number of agents trying to connect simultaneously to the server.

When receiving the token, each agent performs appropriate actions such as policy update or log transmission to the server.

The token rotation period (also called refresh time) is configurable by the administrator to optimize the allocation of bandwidth for Stormshield Endpoint Security.

Number of agents per server	Number of simultaneous connections (LAN)	Token refresh time (in seconds)	Reconnection time in disconnected mode to the server (in seconds)
1 to 500	100 to 50	60 to 600	60 to 300
500 to 2000	70 to 20	600 to 1800	300 to 600
2000 to 4000	50 to 10	1800 to 3600	600 to 1200
4000 to 8000	100 to 10	3600 to 7200	600 to 1200
+ 8000	250 to 50	3600 to 7200	600 to 1200

The maximum number of agents per server is 2 000 000 000.

> **NOTE**
> The console enables to configure up to 2000 simultaneous connections but the Stormshield Endpoint Security server automatically limits to 500 if it is installed on a 32-bit machine (on a 64-bit machine, the maximum number of simultaneous connections managed by the server is 2000).

> **NOTE**
> If agents are connected via a WAN, the number of necessary simultaneous connections significantly increases because the time during which each agent remains connected is longer. The definition of this number strongly depends on the characteristics of the network (throughput, round trip delay, etc.) and on the number of agents concerned.

> **NOTE**
> If more than 200 simultaneous connections must be configured, make sure you have enough RAM (4 Gb on 32-bit machines, 8 to 16 Gb on 64-bit machines) and enough processors.

These details are based on our observations in different configurations.

The less often the token is sent, the fewer the agent connections. This implies that the load distributed across the network and the occupation rate of the servers will decrease significantly.

On the other hand, the alert refresh and policy deployment time intervals are significantly affected by the small number of tokens in circulation.

6.4.3 Log Monitoring Configuration

The graphical interface of the **Log Monitoring Configuration** function is displayed as follows:

Log Monitoring Configuration	
SQL server instance	192.168.128.69\SES
Database password	******
Reporting language	English

- **SQL server instance**:

  Enter the IP address of the SQL server instance used for the log database.

- **Database password**:

  This is the password used for the log database account.

It was defined when installing the Stormshield Endpoint Security database.

- **Reporting language**:

This is the language used for log reporting.

6.4.4 Syslog Configuration

The graphical interface of the **Syslog configuration** function is displayed as follows:

⊟ ≣₅ Syslog Configuration	
Address/Hostname	
Port	514
Protocol	Udp
Facility	0 ~ kernel messages
Severity	0 ~ Emergency

For more information, see the section Exporting logs via Syslog.

6.4.5 SMTP Configuration

The graphical interface of the **SMTP configuration** function is displayed as follows:

⊟ ✉ SMTP Configuration	
From	
To	
SMTP server	
Subject	
Number of events per mail	10

For more information, see the section Exporting logs via SMTP.

6.4.6 Encryption

The graphical interface of the **Encryption** function is displayed as follows:

⊟ ⚷ Encryption	
Decrypt data at uninstallation	☒ Disabled
Start date of allow uninstall	3/30/2018 12:00:00 AM
End date of allow uninstall	3/30/2028 12:00:00 AM
SQL server instance	192.168.128.69\SES
Database password	******

- **Decrypt data at uninstallation**:

Encrypted data on the agent computer will be automatically decrypted when uninstalling Stormshield Endpoint Security.

Only files encrypted with a computer key can be automatically decrypted.

- **Start date of allow uninstall**:

It defines the date and time for starting the uninstallation of the Stormshield Endpoint Security agents.

- **End date of allow uninstall**:

It defines the date and time for finishing the uninstallation of the Stormshield Endpoint Security agents.

- **SQL server instance**:

Enter the IP address of the SQL server instance used for the key database.

- **Database password**:

Enter the password of the key database.

6.4.7 Software Updates Settings

The graphical interface of the Software Updates Settings function is displayed as follows:

⊞ ⬇ Software updates	
Frequency of update checks	03h00m00s
Updates download folder	
Default update to deploy (ex: 7.2.23)	Latest version

- **Frequency of update checks**.

- **Updates download folder**.

- **Default update to deploy**.

For more information about updates, see chapter **Migrating and Updating Stormshield Endpoint Security**.

6.4.8 Authentication Service

The graphical interface of the **Authentication Service** function is displayed as follows:

⊟ 🔒 Authentication Service	
Checking server source	✅ Enabled
Start time	3/30/2018 12:00:00 AM
End time	3/30/2028 12:00:00 AM
Login for CGI authentication	
CGI authentication password	
Certificate validity (day(s))	3650

These parameters are used for downloading certificates. Refer to the section **Downloading certificates**.

- **Checking server source**:

When set to **Enabled,** only the Stormshield Endpoint Security agents deployed from this server installation are authorized to connect to the servers of this environment.

When set to **Disabled,** any Stormshield Endpoint Security agent can connect to the server.

- **Start time**:

This is the date to start the certificate deployment.

- **End time**:

This is the date to finish the certificate deployment.

- **Login for CGI authentication**:

This is the login of the account used to download manually an agent certificate from webpage `https://[server IP address]/ssl/cgi`. Creating this account is not mandatory.

- **CGI authentication password**:

This is the password of the previously created account.

- **Certificate validity** (day(s)): You can modify the period of validity assigned to agent certificates (by default 10 years).

6.5 Applying a server configuration policy

1. When you have finished editing the server configuration policy, click **Check In**.
2. From the **Servers** panel, add the installed servers and select the server configuration policy in column **Policy Name**.
3. Click **Deploy to the environment**.

This action must be performed each time you edit the server configuration policy.

When changes have been deployed to the environment, the column **Status** is updated in the **Servers** panel.

> 🛈 NOTE
> A same policy can be applied to several servers.

> 🛈 NOTE
> A server is regarded as a Stormshield Endpoint Security server if the server component has been installed and if a server configuration policy has been applied.

7. Stormshield Endpoint Security Agent Configuration
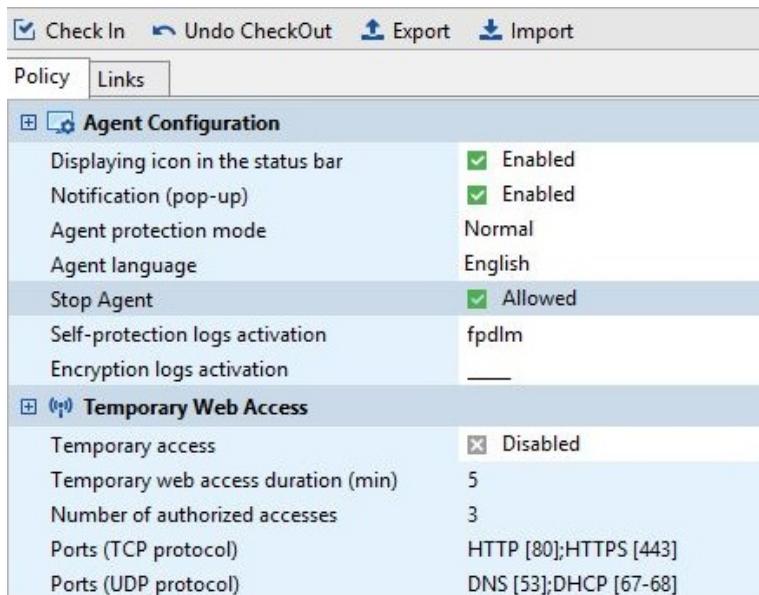
7.1 Creating a Dynamic Agent Configuration Policy

1. Click **Policies** and the ➕ button. The window **Create a new policy** opens.
2. Enter a policy name and select the **Dynamic Agent configuration** policy type.
3. Click **OK**. The policy edition window opens.

7.2 Editing the Dynamic Agent Configuration Policy

The agent configuration edition window includes two areas:

- Agent Configuration,
- Temporary Web Access.

7.2.1 Agent Configuration

The graphical interface of the Agent Configuration function is displayed as follows:
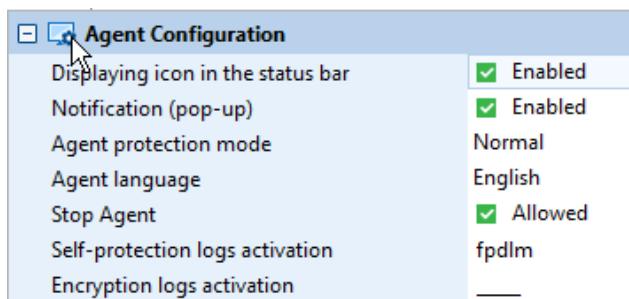
Displaying icon in the status bar
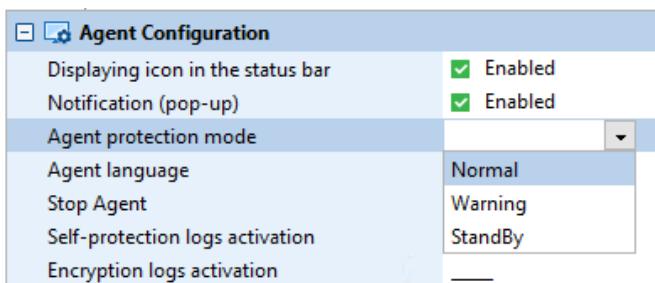
This option is checked by default and allows automatically running the agent monitor. If not checked, the agent monitor icon will not be visible in the status bar. Moreover, if it is not checked, the option about notifications is automatically unchecked and grayed out.

Notification (pop-up)

This option enables/disables the pop-ups displayed on the Stormshield Endpoint Security agent.

Agent protection mode

The graphical interface of the Agent protection mode function is displayed as follows:

There are three agent protection modes:

1. **Normal**:

   The agent applies the policy.

   This mode blocks and logs.

   On the agent, this mode is indicated by the Stormshield Endpoint Security icon: .

2. **Warning**:

   the agent does not apply the policy but it provides a warning log showing what is blocked by the policy.

   This option is used to see what the policy does in order to modify it if need be. This option can be used for simulation.

   This mode does not block but logs.

   On the agent, this mode is indicated by the Stormshield Endpoint Security icon: .

3. **StandBy**:

   the agent applies no policy and keeps no warning log.

   It acts as a "pause" mode that can be used when you do not want to apply a specific policy (example: during server installation).

   This mode does not block and does not log either.

   On the agent, this mode is indicated by the Stormshield Endpoint Security icon: .

Agent language

This option is used to select the user interface language on the Stormshield Endpoint Security agent.

Stopping the agent

You can set this option to **Allowed** or **Denied**:

- If this option is set to **Allowed,** the user who has administrator rights on his workstation can stop the agent by simply running `stopagent.exe`.

  For more information, refer to If the "Stop Agent" option is set to Allowed.

  > **ⓘ NOTE**
  > After the agent is installed but before certificates are downloaded, the default setting for **Stop Agent** is **Allowed**.

- If this option is set to **Denied,** the user can request the administrator that the agent be temporarily stopped.

  For more information, refer to If the "Stop Agent" option is set to "Denied".

Stop Agent is to be used carefully since agent deactivation makes a workstation vulnerable to various attacks (viruses, buffer overflow, keylogging (capture of keyboard events in order to steal passwords and other confidential information).

Nevertheless, it may be useful to stop the agent in a test environment.

Enable Logs

Overview

There are **two** types of Enable log options under **Agent Configuration**:
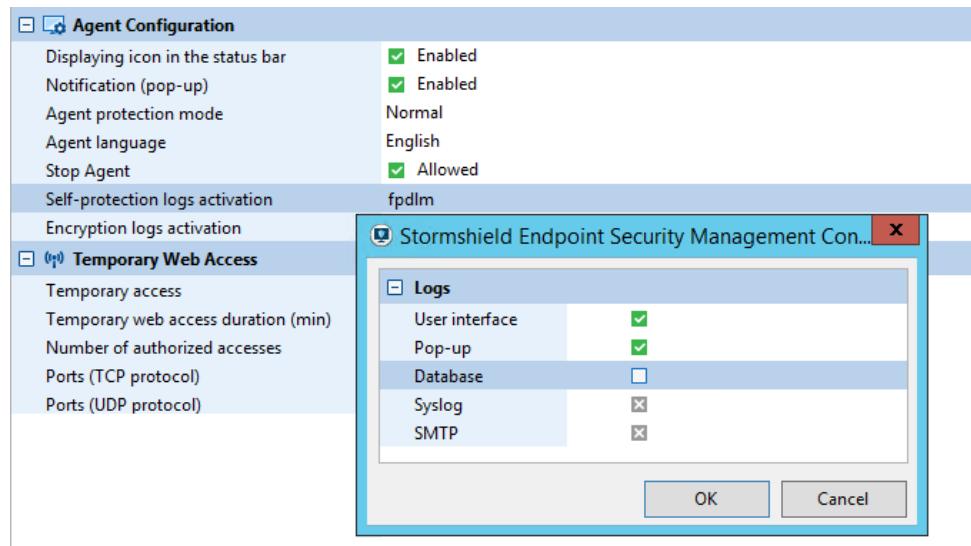
- Enable self-protection logs:

  This covers all logs generated with RID=0.

- Enable system encryption logs:

  This covers all the encryption error logs.

Both options let you decide which Stormshield Endpoint Security logs are displayed and filtered in the **Monitoring** > **Software Logs** panel.

Each log option contains the following parameters to save and consult logs:

- **User interface**:

  Logs are displayed on the user interface (ssmon).

- **Pop-up**:

  Logs are displayed in a pop-up window.

- **Database**:

  Logs are sent to the database. They are displayed in the **Monitoring** menu of the console.

- **External application**:

  Logs are sent to an external system (examples: Syslog or SMTP server).

The default setting is set to `[empty]`. For more information, see **Log Manager** below.

Settings for self-protection logs and system encryption logs

To apply settings to the logs, you must follow the steps below:

1. In the **Agent Configuration** panel, click the second column including **Self-protection logs activation** or **Encryption logs activation**.

   A list of logs is displayed in a window:

   - User interface (F/f).
   - Pop-Up (P/p).
   - Database (D/d).
   - External application (E/e).

2. Select the options to be enabled or disabled.

3. Click **OK**.

Log Status

The settings applied by the administrator to log statuses can be viewed and modified in the security policy edition window (Log column) and in the **Log Manager** menu.

Depending on your settings in **Agent Configuration**, modified log statuses will be visible in the security policy edition window and in the **Log Manager** menu.

There are three log statuses available:

- **Enabled**:

  A green check is displayed in a box.

  In each log field, enabled logs are displayed in uppercase letters (examples: F, P, D, E).

  These logs can also be read in the **Log Manager** menu.

- **Disabled**:

  A red box is displayed.

  In each log field, disabled logs are displayed in lowercase letters (examples: f, p, d, e).

  These logs cannot be read in the **Log Manager** menu.

- **Empty**:

  If the box is left empty , the administrator can select a log to be displayed in the **Log Manager** menu.

  In each log field, a line in the form of an "underscore" is displayed (example: _pde).

  If the log is empty, the behavior will be the one defined in the **Log Manager** menu.

  For more information, see the section Log Manager.

7.2.2 Temporary web access

When a network access is denied, Temporary Web Access allows temporarily opening ports that could be blocked by the security policy (example: http/https).

Network restrictions on applications are ignored throughout the duration of the temporary access.

You can customize the ports enabled by this feature.

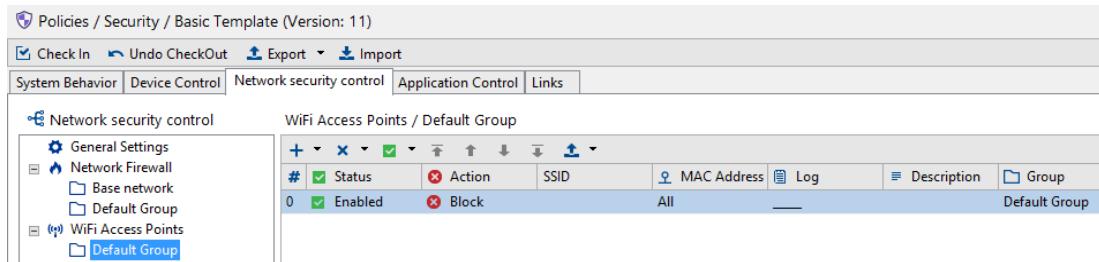**Example**: A user working outside the company network will be able to use a WiFi HotSpot to connect to the company's VPN SSL server.

Configuration from the console

To deny access to WiFi access points and allow use of HotSpots, the administrator must configure the security policy as follows:

1. Edit the security policy. Go to *Network security control > General Settings > WiFi Encryption and Authentication*.

2. Set **WiFi connections** to **Allowed**.

WiFi Encryption and Authentication	
WiFi connections	✔ Allowed
WiFi adhoc connections	✔ Allowed
Open authentication mode	✔ Allowed
WEP authentication mode	✔ Allowed
Open or WEP authentication mode	✔ Allowed
WPA authentication mode	✔ Allowed
WPA (PSK) authentication mode	✔ Allowed
WPA (ADHOC) authentication mode	✔ Allowed
WPA2 authentication mode	✔ Allowed
WPA2 (PSK) authentication mode	✔ Allowed
Other authentication modes	✔ Allowed

3. Under **WiFi Access Points**, deny access by creating a rule. To do so, follow the steps below:

   ◦ Edit the security policy.

   ◦ Add a rule by clicking + .

   ◦ Enter the following parameters:

      - SSID value: *****.

      - Action: **Block**.

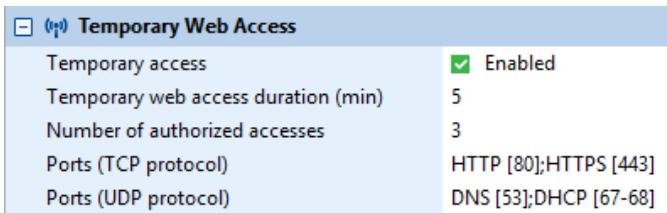| Policies / Security / Basic Template (Version: 11)							
✔ Check In ↩ Undo CheckOut ⬆ Export ▾ ⬆ Import							
System Behavior | Device Control | Network security control | Application Control | Links							
⊶ Network security control	WiFi Access Points / Default Group						
⚙ General Settings	+ ▾ ✖ ▾ ✔ ▾ ⬆ ⬆ ⬇ ⬇ ⬆ ▾						
⊟ ⋀ Network Firewall	#	✔ Status	✖ Action	SSID	⚲ MAC Address	▤ Log	≡ Description	▢ Group
☐ Base network	0	✔ Enabled	✖ Block		All	___		Default Group
☐ Default Group							
⊟ ᵠ WiFi Access Points							
☐ Default Group							

🔴 **WARNING**
The administrator can include a whitelist of authorized access points.
It should be noted, though, that WiFi Access Points rules must be configured as follows:

- Rules with Action set to **Accept** are listed first.

- A final rule (with Action set to Block and SSID set to *) is placed at the bottom of the list.

4. In the dynamic agent configuration edition window, go to **Temporary Web Access** and set **Temporary access** to **Enabled**.

5. Enter the **Temporary web access duration** in minutes.

   By default, this duration is set to 5 minutes, which is usually enough time for the user to connect to the HotSpot.

   The maximum duration is 30 minutes.

6. Enter the **Number of authorized accesses**.

   By default, this value is set to 3 hours. The count is reinitialized at computer restart.
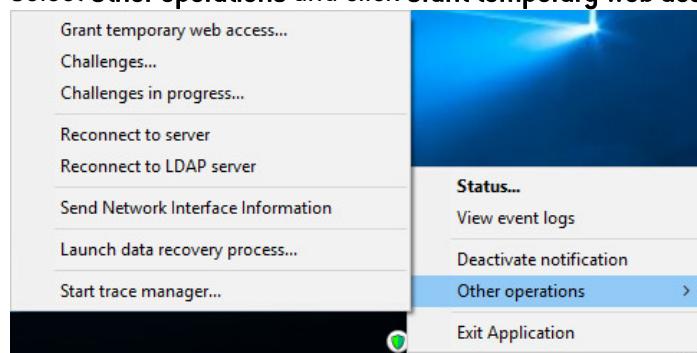
7. If necessary, change or add ports to the ports listed in the **Ports (TCP Protocol)** and **Ports (UDP Protocol)** fields.
   If you include a descriptive comment, you should then include the port number between brackets (example: `HTTP [80]`).
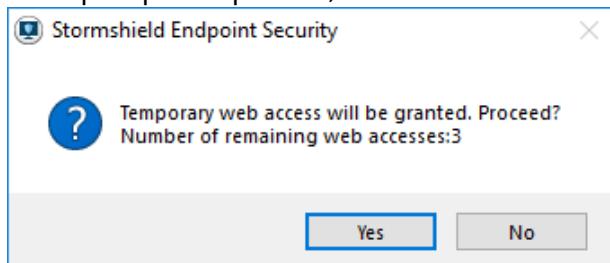
Configuration from the agent

To configure temporary web access from the agent, the user must follow the steps below:

1. Right-click the Stormshield Endpoint Security icon 🛡️ .

2. Select **Other operations** and click **Grant temporary web access**.

3. When prompted to proceed, click **Yes**.
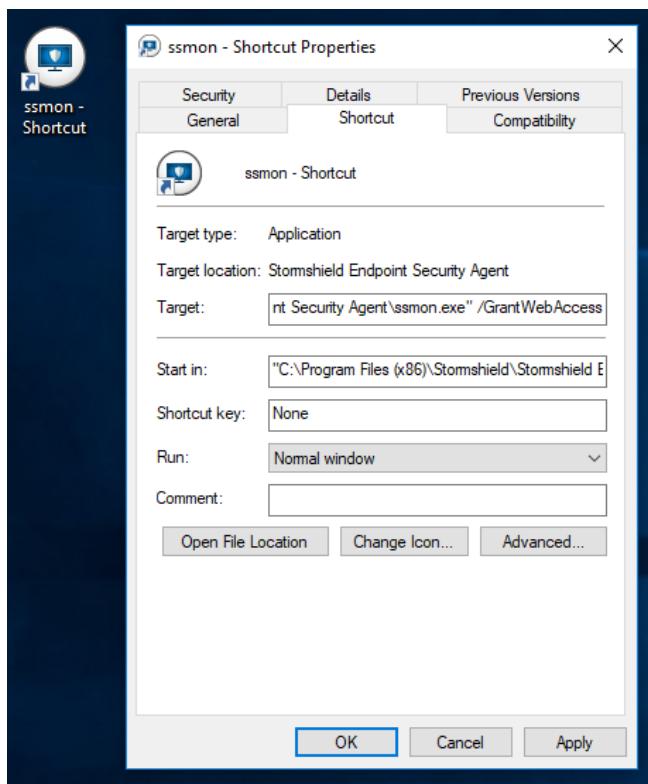
You can now access the web browser for the duration specified by the administrator.

The default duration is usually long enough to use the browser to sign in to a hotspot or to connect to your company's VPN SSL server.

4. A window is displayed to show that temporary web access has expired.

The user may have the possibility to request temporary web access in a faster way than using the Stormshield Endpoint Security menu. You can create a shortcut of the *ssmon.exe* executable file (graphical interface executable located in the agent repository) and place it on the users desktop. In the shortcut target, add the command line argument «/GrantWebAccess». Users just need to double-click the shortcut on their desktop to request temporary web access.

You can also add the option "/NoConfirm" to the argument in order to disable the confirmation window to access the web. Access is therefore immediate, except if there is an error (this feature is not allowed for example or the number of authorized accesses is exceeded).

Send Network Interface Information
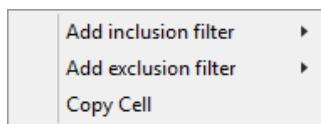
To retrieve the network interface identifier for later use in the active network interface test (see Network > Active Network Interface), follow the steps below:

1. Use a Stormshield Endpoint Security agent that belongs to the network to send network interface information to the server log:
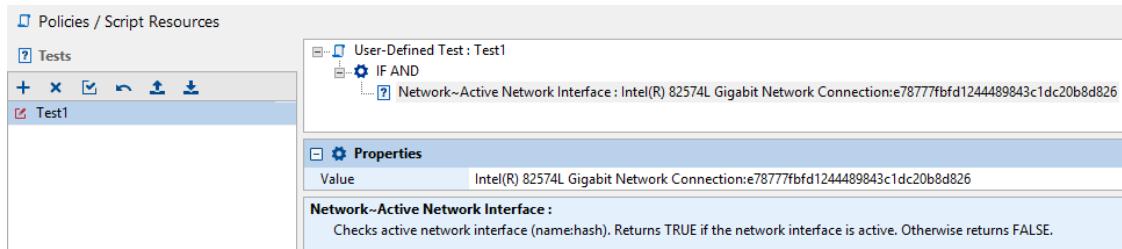
- ◦ Right-click the Stormshield Endpoint Security icon 🛡️ .
- ◦ Select **Other operations** > **Send Network Interface Information**.

2. In the management console, select **Monitoring** > **Software logs**.

3. Locate the log entry of the network interface ID.

   The entry displays the following information:

- **Date**.
- **User Name**: Administrator.
- **Action**: INFO.
- **Status**: NET-INT.
- **Type**: Agent.
- **Mod. Name** : MODENFORCEMENT
- **Log**: Network interface ID.
- **Agent mode**.

Date	Type	Agent Mode	Action	Status	Log	Mod. Name
4/10/2018 11:05:05 AM	Agent	Normal	INFO	NET-INT	Intel(R) 82574L Gigabit Network Connection...	MODENFORCEMENT

4. Right-click the log entry.

Add inclusion filter	▸
Add exclusion filter	▸
Copy Cell	

5. Copy the network interface ID.

6. Paste the network interface ID into the **Value** field in the active network interface **Properties** under **Script**.

7.3 Applying a dynamic agent configuration policy to an object of the directory

1. When you have finished editing the dynamic agent configuration policy, click **Check In.**

2. In the directory tree view, select the object containing the computers on which the policy must be applied.

3. In the **Dynamic Agent Configuration** part in the *Policies linked* tab, select the policy.

4. Click **Deploy to the environment**.

This action must be performed each time you edit the dynamic agent configuration policy.

🛈 **NOTE**

When the agent receives the new dynamic agent configuration policy, an entry is added in the agent logs.
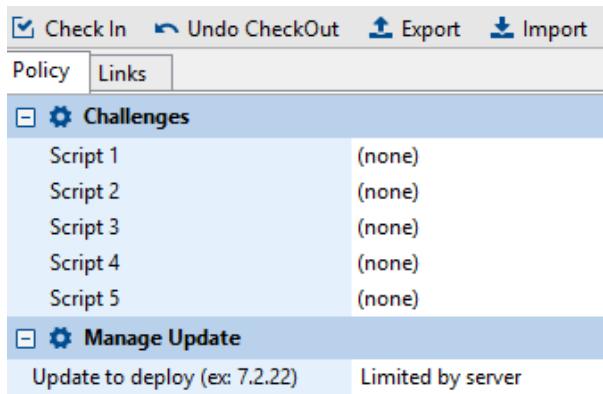
7.4 Creating a Static Agent Configuration Policy

1. Click **Policies** and the ➕ button. The window **Create a new policy** opens.

2. Enter a policy name and select the **Static Agent configuration** policy type.

3. Click **OK**. The policy edition window opens.

7.5 Editing a Static Agent Configuration Policy

The static agent configuration edition window includes two areas:

- Challenges
- Manage Update

7.5.1 Challenges

Overview

Challenges are scripts configured on the console. These scripts are applied to Stormshield Endpoint Security agents on a temporary basis. For more information about the Stormshield Endpoint Security script module, refer to chapter Scripts.

Users request the execution via challenges. The administrator manages challenges from the console.

Applying a challenge request will in no way replace the conventional application of a policy or a configuration through a script defined by the administrator and dedicated to a specific environment. Policies or configurations applied via these scripts take priority over all others.

You are therefore advised to restore the policy or configuration when the application of the challenge is no longer needed.

Challenges are initiated by the **administrator**. Only challenge requests are initiated by the **user**.

Challenges are detailed according to the following steps:

- The administrator applies the static agent configuration policy to an Active Directory object or to an agents group. This policy can contain up to five different challenges.
- User sending a challenge request to the administrator.
- The administrator manages the challenge requests sent by the user.

- The user displays the challenges in progress.
- The user stops a challenge in progress.

Applying a static agent configuration policy to an object of the directory

To apply the policy to an Active Directory object or to an agents group, follow the steps below:

1. In the **Environment Manager** section, select the **Policies** menu and create a static agent configuration policy.

2. In the **Challenges** part of the *Policy* tab, click the right column to view the button ⊡.
   The list of scripts becomes accessible to the administrator.

3. To use an existing script as a challenge, select the script from the drop-down menu. Scripts used for challenges are created in the **Script** folder. For more information, see section Scripts.

4. Apply this policy to an Active Directory object. To link the static agent configuration policy to an object:

   ◦ Select the *Policies linked* tab.

   ◦ In the **Static Agent Configuration** part in the *Policies linked* tab, select the policy to apply.

5. Click **Deploy to the environment**.

This action must be performed each time you edit the policy.

User sending a challenge request to the administrator.

Reminder
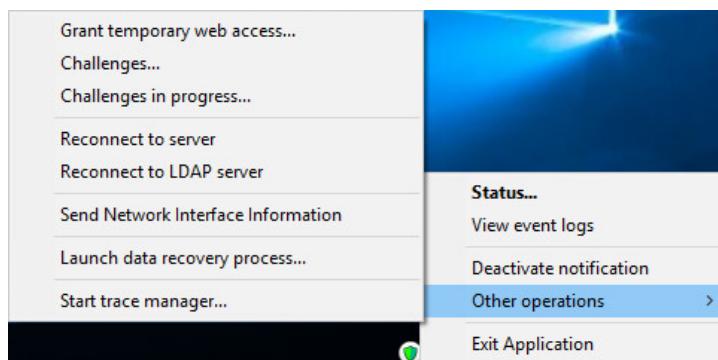
The user should request the right to apply any particular challenge from the administrator. This is a challenge request.

The administrator is in charge of selecting the challenge type and its duration. The challenge selected by the administrator from the console is activated for the time period specified.
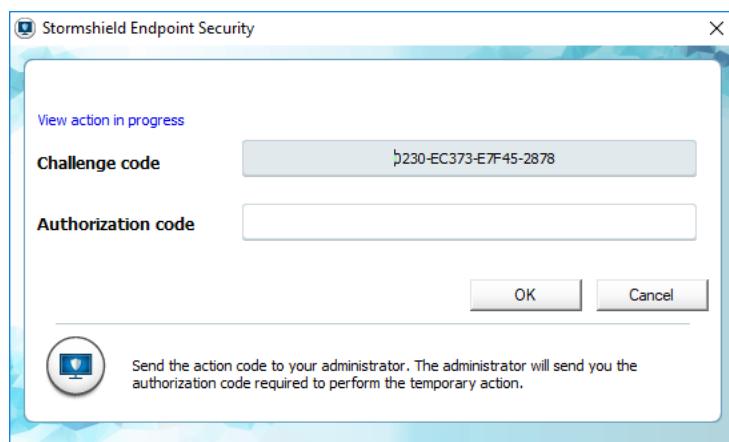
Procedure

To send a challenge request, the user must follow the steps below:

1. Right-click the Stormshield Endpoint Security icon in the taskbar and select **Other operations > Challenges**.

2. Send the **Action code** which is displayed to the administrator.
   The administrator will send you the **Authorization code** which is displayed on his console.

3. In the **Authorization code** field, enter the code given by the administrator.

4. Click **OK**. The challenge selected by the administrator from the console is activated for the time period specified in the **Generate Challenge** window.

   ℹ️ **NOTE**
   If the action selected is **Disable Protections**, you must wait at least 30 seconds before agent protection stops. In other cases, the action selected takes effect immediately.

5. To check that the challenge is in progress:

   ◦ Right-click the Stormshield Endpoint Security icon 🛡️ .

   ◦ Select **Status**.
     Example of window for **Status**: Stand-by mode.

Administrator managing the challenge requests sent by the user

Reminder

Stage 1: The user sends a challenge request. The administrator receives the action code (Stormshield Endpoint Security agent key) assigned to this user.
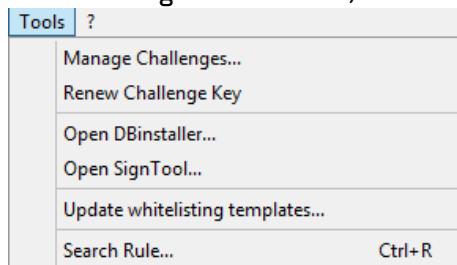
Stage 2: The administrator generates the authorization code assigned to the challenge.

Stage 3: The user enters the authorization code which initiates the challenge on his workstation.
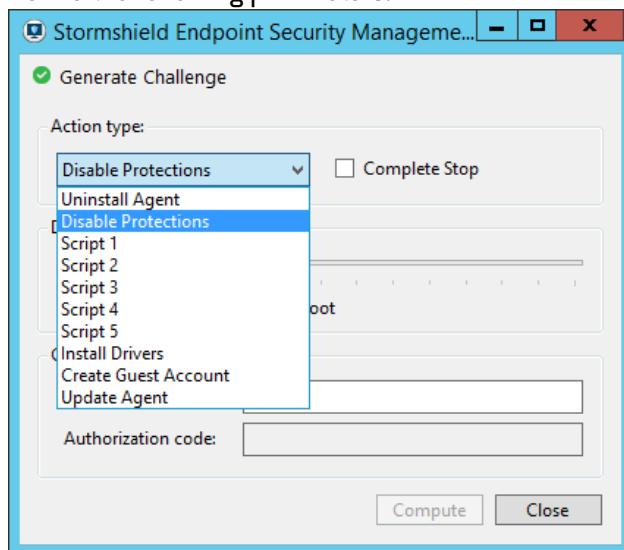
Procedure

To answer the request sent by a user who wants to temporarily deactivate the Stormshield Endpoint Security agent, follow the steps below:

1. On the management console, select **Tools > Manage Challenges**.

Tools	?
Manage Challenges...	
Renew Challenge Key	
Open DBinstaller...	
Open SignTool...	
Update whitelisting templates...	
Search Rule...	Ctrl+R

2. Define the following parameters:

Stormshield Endpoint Security Manageme...

Generate Challenge

Action type:

Disable Protections   ☐ Complete Stop

Uninstall Agent
Disable Protections
Script 1
Script 2
Script 3
Script 4
Script 5
Install Drivers
Create Guest Account
Update Agent

Authorization code:

Compute   Close
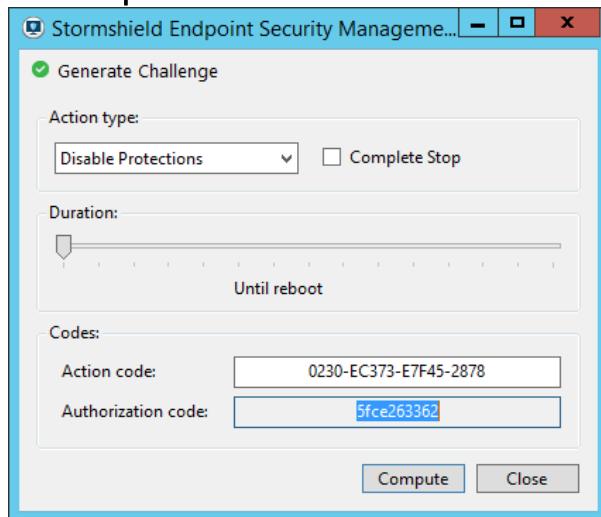
- **Action type** using ☐ to display the list of challenges.
  If you check the **Complete Stop** box opposite **Disable Protections**, the agent will stop completely and will not switch to Activated - Stand-by mode.
  Therefore, no log will be sent and no policy will be applied.
  Scripts from 1 to 5 correspond to challenges selected in the static agent configuration policy applied by the agent.

- Duration of the challenge by sliding the cursor along the timeline.

- Enter the **Action code** sent by the user.
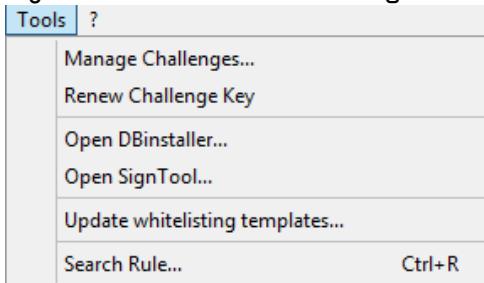
3. Click **Compute** to obtain the Authorization code

4. Send this code to the user.

> **ⓘ NOTE**
> If you want to renew the challenge code key, just click **Tools > Renew Challenge Key**.
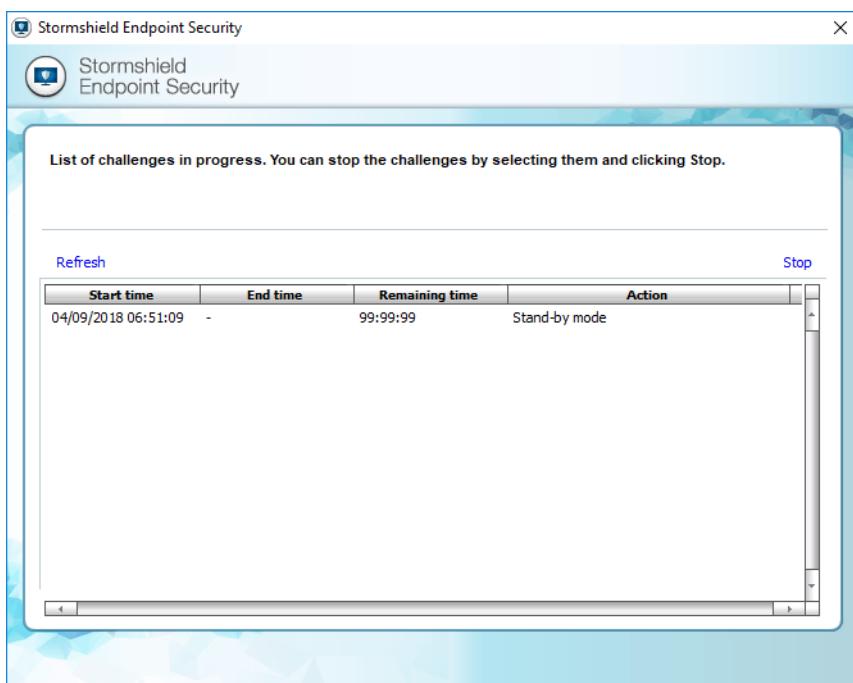
> **⚠ WARNING**
> From Microsoft Windows 8.1, when the Windows "Quick Start" feature is enabled by default, if the agent is stopped with a challenge "until reboot", you will have to manually restart the agent or restart the workstation if the user shutdowns and then starts again the workstation.

The user displays the challenges in progress

The user can consult the temporary actions in progress on his workstation by clicking **Other operations > Challenges in progress**.

The information displayed on the challenges in progress are the following:

- **Start time**:

  The time when the temporary action was applied to the agent.

- **End time**:

  The time when the challenge stops.

- **Remaining time**:

  The time remaining before the challenge stops.

- **Action**:

  Type of temporary action applied to the agent.

The user stops a challenge in progress

To stop a challenge, the user must follow the steps below:
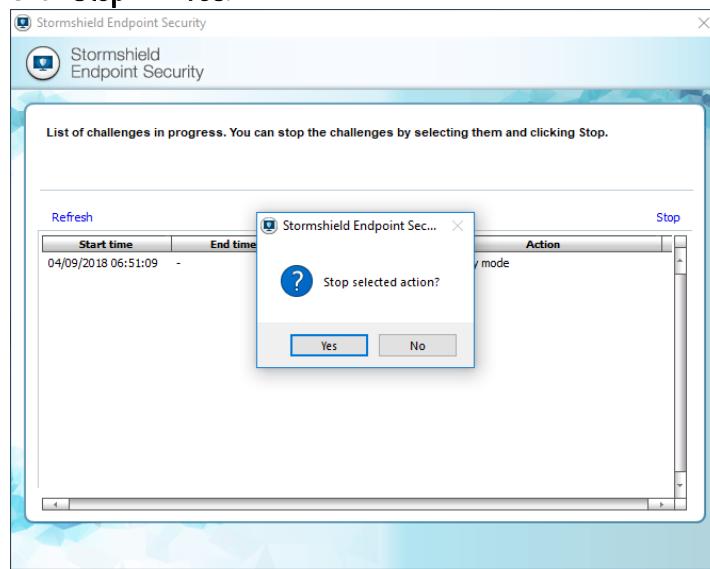
1. In the taskbar:

   ◦ Right-click the Stormshield Endpoint Security icon in the taskbar .

   ◦ Select **Other operations > Challenges in progress**.
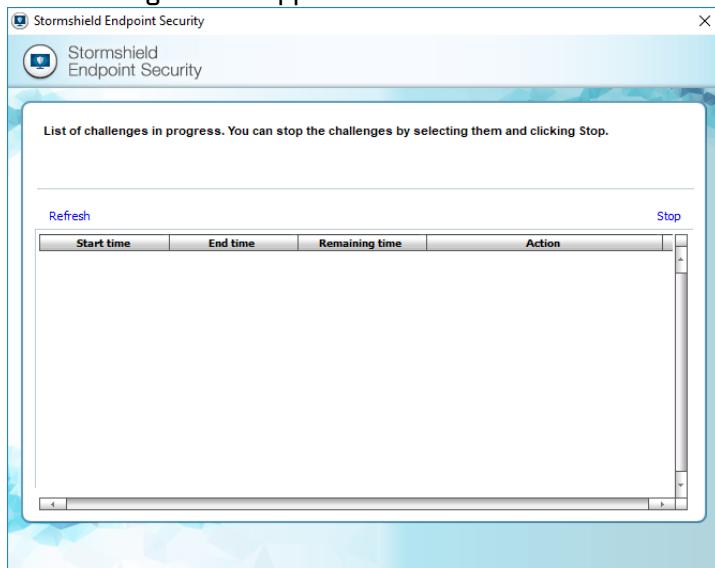
   The list of challenges in progress is displayed.

2. Select the challenge to stop.

3. Click **Stop** and **Yes**.

4. The resulting window appears.

7.5.2 Manage update

Overview

The **Manage update** part allows defining the version in which the agent will update when updates will be deployed on the Stormshield Endpoint Security server. When the administrator does not specify any version, **Limited by server** is displayed. It means that the agent will update until the specified version in the configuration Server. This setting can be ignored by using the **Update Agent** challenge from the Stormshield Endpoint Security 7.2.11 version.

For more information about updates, see chapter Migrating and Updating Stormshield Endpoint Security.

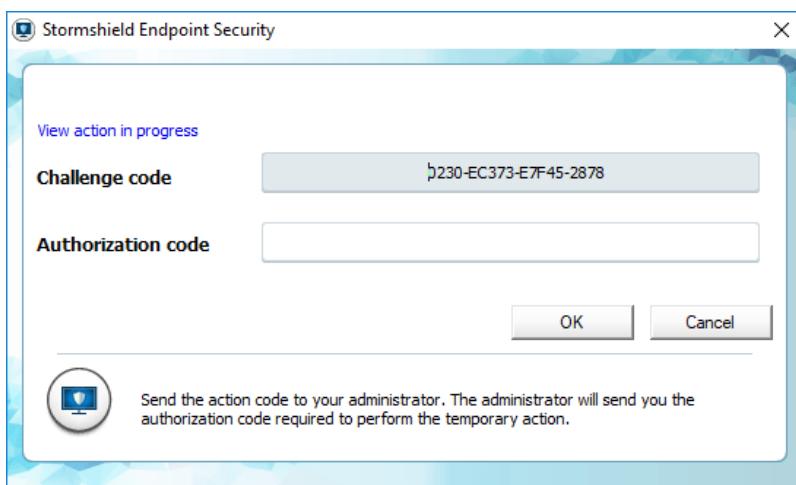## 7.6 Applying a static agent configuration policy to an object of the directory

1. When you have finished editing the static agent configuration policy, click **Check In.**
2. In the directory tree view, select the object containing the computers on which the policy must be applied.
3. In the **Static Agent Configuration** part in the *Policies linked* tab, select the policy.
4. Click **Deploy to the environment**.
5. This action must be performed each time you edit the static agent configuration policy.

7.7 Stopping the agent

Depending on the option selected in **Stop Agent**, procedures to stop or uninstall the agent are the following.

7.7.1 If the "Stop Agent" option is set to Allowed

🛑 **WARNING**
From Microsoft Windows 8.1 onwards, whenever the Windows "Quick Start" feature is enabled by default, if the agent is stopped through *stopagent.exe*, you will have to manually restart the agent or restart the workstation if the user shuts down and then restarts the workstation.

The user with administration privileges on the workstation can shut down the agent in two ways:
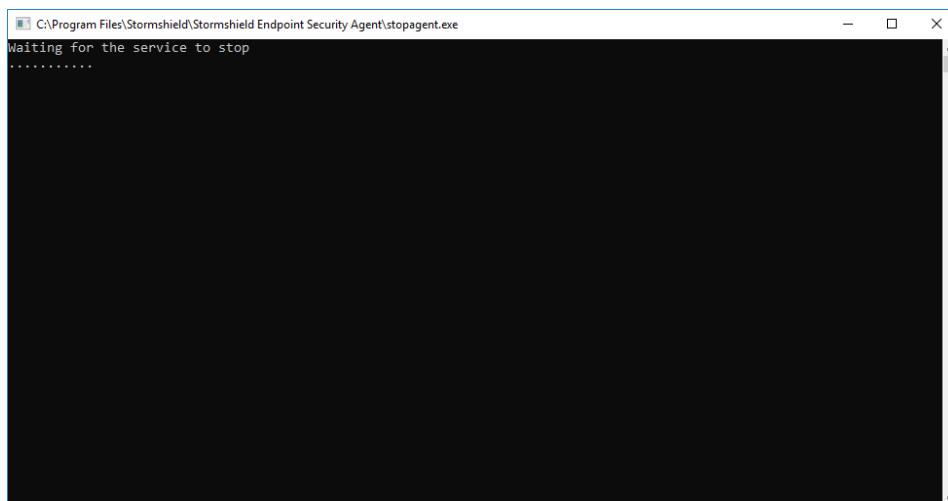
- By clicking on the **Disable** link. This will run the `stopagent.exe` program.
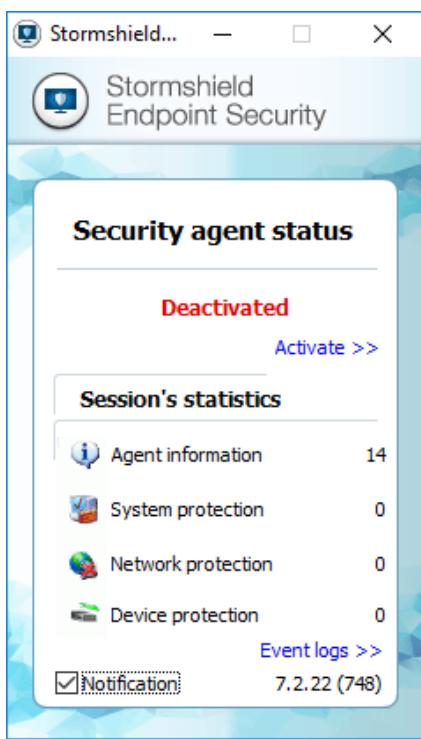
  -or-

- By following the procedure below:

1. Go to the directory below: `[Program Files]\Stormshield\Stormshield Endpoint Security Agent`,
2. Double-click on the `stopagent.exe` file.
3. Wait for the following window to close:

4. Right-click on the Stormshield Endpoint Security icon 🛡 in the taskbar and select **Status** to check that the agent has indeed stopped running.

To re-enable the agent, click on **Activate** in the **Status** window.

7.7.2 If the "Stop Agent" option is set to "Denied"
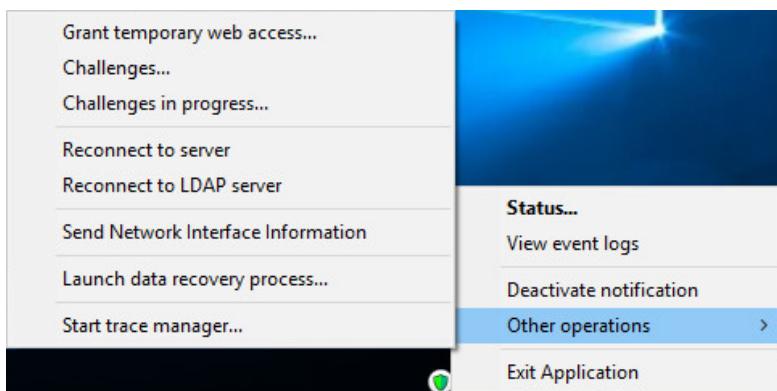
To stop the agent, the user should ask the administrator to deactivate the agent on a temporary basis.

The user and the administrator use the **challenge** procedure. See section Transferring files towards the agents.

User procedure

The user must follow the steps below:

1. Right-click the Stormshield Endpoint Security icon in the taskbar and select **Other operations > Challenges** or from the **Status** window, click **Disable**.

2. Send the **Action code** which is displayed to the administrator.

The administrator will send you the **Authorization code** which is displayed on his console.

3. In the **Authorization code** field, enter the code given by the administrator.

4. Click **OK**.

The agent will be disabled for the time duration specified by the administrator.

> ### ℹ NOTE
> If the action selected is **Disable Protections**, you must wait at least 30 seconds before agent protection stops. In other cases, the action selected takes effect immediately.
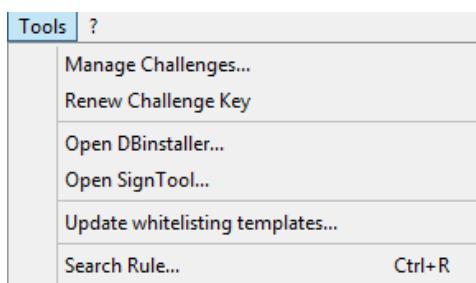
5. Right-click the Stormshield Endpoint Security icon 🛡 in the taskbar and select **Status** to check the agent is effectively in stand-by mode.

Administrator procedure
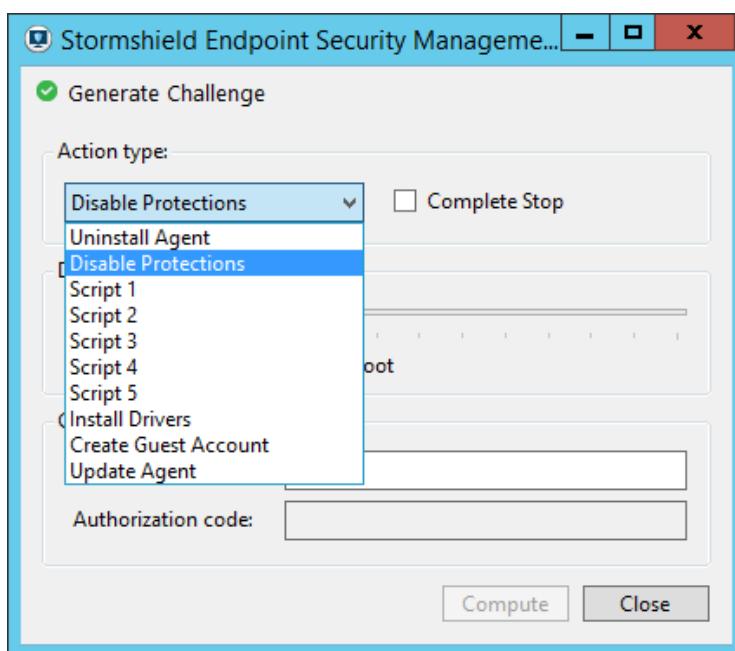
To answer the request sent by a user who wants to temporarily deactivate the Stormshield Endpoint Security agent, follow the steps below:

1. On the management console, select **Tools > Manage Challenges**.

Tools	?
Manage Challenges...	
Renew Challenge Key	
Open DBinstaller...	
Open SignTool...	
Update whitelisting templates...	
Search Rule...	Ctrl+R
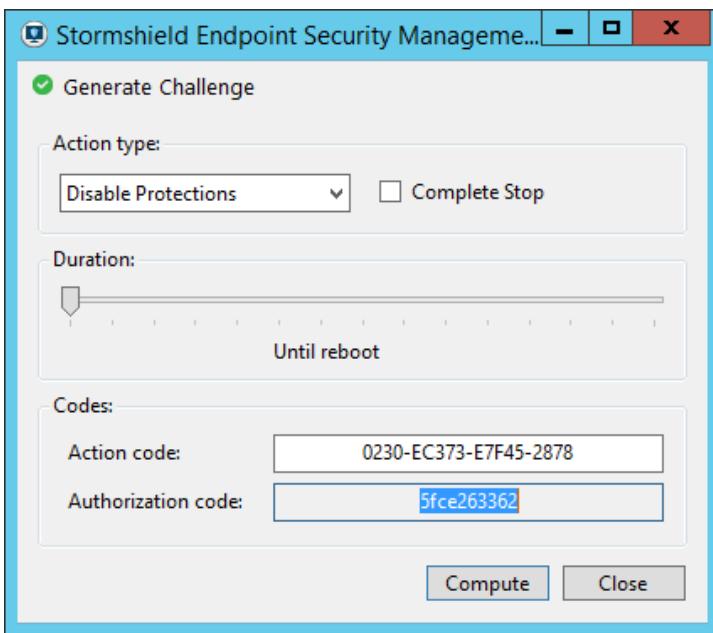
2. Define the following parameters:

   ◦ **Action type** using [⌄] to display the list of challenges.

   If you check the **Complete Stop** box opposite **Disable Protections**, the agent will stop completely and will not switch to **Activated - Stand-by mode**.

   Therefore, no log will be sent and no policy will be applied.

   ◦ **Duration** of the challenge by sliding the cursor along the timeline.

   ◦ Enter the **Action code** sent by the user.
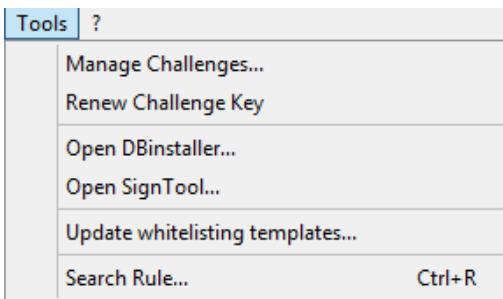
3. Click **Compute** to obtain the Authorization code

4. Send this code to the user.

> 🛈 NOTE
> If you want to renew the challenge code key, just click **Tools > Renew Challenge Key**.
> It is recommended to renew the challenge key every fortnight when using challenges regularly.

7.7.3 If the user wants to uninstall the Stormshield Endpoint Security agent

On condition that the user has administrator rights to the agent computer and the **Stop agent** option is set to **Allowed** on the console, the user can uninstall the agent through the "Uninstall or change a program" Windows utility or by running *Srend.exe*.

To uninstall the agent, see the section Uninstalling the agent.

7.8 Information about the configuration of the agent in the registry base

Information about the configuration of the agent is stored in the registry base on the workstation. This information will remain available in read only mode and indicate the current status of the SES agent, which protects the information.

7.8.1 Availability and location

All keys are volatile, so when they are located in the registry base, they continue to reflect current configurations and policies.

When changes are made to a configuration or policy, the associated key will be deleted and recreated, and its values will be entered. The different values within the same sub-key therefore actually describe the same configuration.

Information is stored in the following keys:

Operating system	Key
32-bit	HKEY_LOCAL_MACHINE\software\Stormshield\Stormshield Endpoint Security Agent\ AppliedPolicies
64-bit	HKEY_LOCAL_MACHINE\software\wow6432node\Stormshield\Stormshield Endpoint Security Agent\AppliedPolicies

7.8.2 Keys and values added to the registry base

Keys contain the following sub-keys:

Name	Type	Description	Remarks
Dynamic configuration	Key	Dynamic configuration	
Static configuration	Key	Static configuration	
Security	Key	Security policy	
Encryption	Key	Encryption policy	Does not appear if no policies have been applied
Agent status	Key	Agent mode	
Challenge	Key	Temporary actions	Does not appear if there are no ongoing challenges

If the agent is in a "Professional" version, the "Encryption" key will either be deleted or not created. If the agent is a "Secure" version but no encryption policy has been applied, the "Encryption" key will not exist either.

"Dynamic configuration", "Security" and "Encryption" keys contain the following values:

Name	Type	Description
Name	REG_SZ	Configuration name
Version	REG_DWORD	Version number of the configuration
Date	REG_SZ	Date applied

The "Static configuration" key contains the following values:

Name	Type	Description
Name	REG_SZ	Configuration name
Version	REG_DWORD	Version number of the configuration
Agent version limit	REG_SZ	Highest update version allowed
Date	REG_SZ	Date applied

The "Agent status" key contains the following values:

Name	Type	Description
Mode	REG_SZ	Agent mode. Possible values: "NORMAL", "WARNING" or "STANDBY" only.
Date	REG_SZ	Date applied
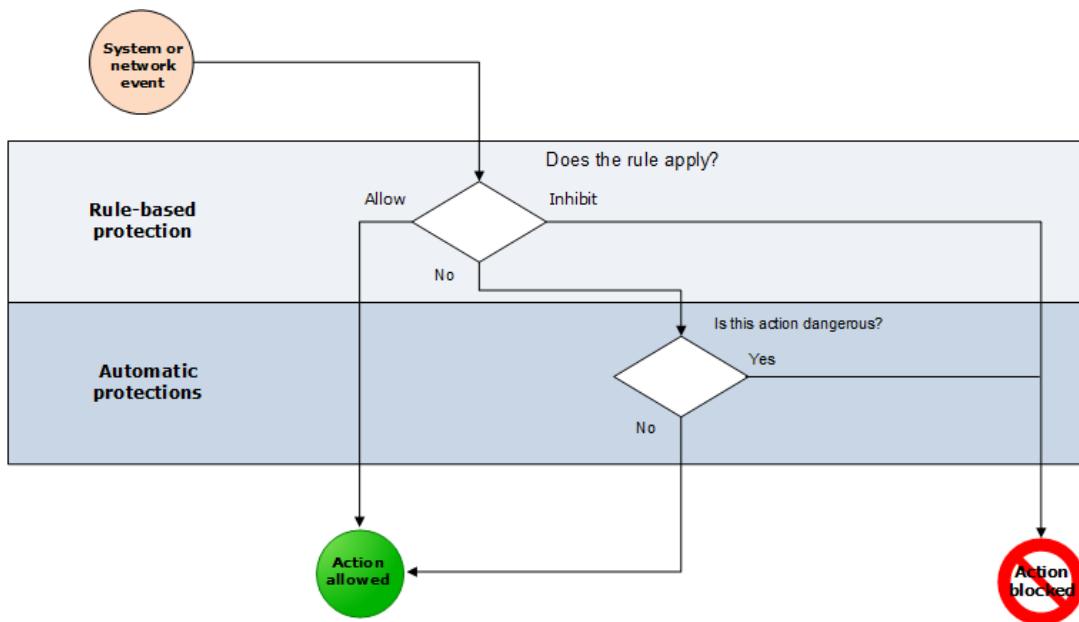
The "Challenge" key contains the following values:

Name	Type	Description	Remarks
Standby	REG_SZ	Date applied	Does not appear if there are no ongoing challenges
AV	REG_SZ	Date applied	Does not appear if there are no ongoing challenges

8. Protection Mechanisms

8.1 Protection mechanisms

To provide optimum protection, Stormshield Endpoint Security uses two protection modes that work in a coherent and complementary fashion.

8.1.1 Automatic protections

Automatic protections cover system and network activities on the client workstation. The administrator can disable these protections partially or totally.

For more information, see Configuring automatic protections.

8.1.2 Rule-based protection

Rule-based protection is used to define a specific policy in an organization. The administrator is in charge of implementing this policy by explicitly setting out permissions and bans on access to the client workstation resources.

For more information, see Security Policies.

8.1.3 Order used to apply protection mechanisms

The two protection modes are applied in a specific order:

1. Rule-based protection.
2. Automatic protections.

This order of precedence gives priority to the policy explicitly defined by the administrator (rule-based protection). Consequently, any ban or formal authorization expressed by the administrator is always applied. Human control always takes precedence over automation.

8.2 Automatic protections

8.2.1 Principles

Automatic protections in Stormshield Endpoint Security:

• Detect anomalies.

• Block anomalies.

• Require no configuration from the administrator.

However, the administrator can adjust Stormshield Endpoint Security 's response to different event types. Depending on the administrator's settings, Stormshield Endpoint Security:

• Ignores the event.

• Generates an alert.

• Blocks the action in progress.

8.2.2 Accessing automatic protections parameters

Automatic protection parameters belong to the **General Settings** category in tabs *System Behavior Control*, *Device Control* and *Network Activity Control* of the security policy edition window.

For more information about configuring automatic protection parameters, see chapter Security Policies.

8.2.3 Configuring automatic protections

Stormshield Endpoint Security keeps on monitoring application and system activities. Collected information is used to protect your workstation from:

• Attempts to corrupt executable files.

• Attempts to access certain services or sensitive data in the system.

Depending on the type of anomalous activity detected and the response level defined by the administrator, Stormshield Endpoint Security can react in **real time** to protect the system.

Protection usually consists in refusing this malicious system call, while the application goes on running.

Stormshield Endpoint Security can also stop the process completely if system integrity is at stake.

Automatic protections can be fine-tuned for each security policy. The administrator can:

• Activate or deactivate a protection.

• Set the protection level.

8.3 Rule-based protection

Rule-based protection lets the administrator define which actions are authorized or banned at system and network level (examples: access to files, registry bases or network protocols).

Rules represent the finest granularity of administrator-defined security policies. They are organized by category in the security policy tabs.

For more information about configuring rule-based protection parameters, see section of chapter Security Policies.

8.3.1 Rule categories

You can chose either of the **seven** categories below:

- **Kernel Components**:

  This category enables control over driver loading and detects suspect drivers on 32-bit workstations only.

  > ⚠️ **WARNING**
  > The agent must be restarted in order to enable this protection. If a policy containing this protection is applied via script, the base policy must also contain this protection.

- **Removable Devices**:

  This category defines removable devices likely to be used by client workstations.

  > ℹ️ **NOTE**
  > To ban the use of removable devices, WiFi and/or WiFi ad hoc connections, go to **General Settings > WiFi Encryption and Authentication > [parameter]** to set the parameter to **Denied**.

- **Network Firewall**:

  This category enables static and dynamic control of the network firewall.

- **WiFi Access Points**:

  This category provides network protection by enabling control over WiFi access points that can be accessed by client workstations.

- **Applicative Rules**:

  This category covers:

  - All the rules relating to running applications.
  - All the rules relating to modifying applications.
  - Application access rights to network, files and registries.

- **Extension Rules**:

  This category is used to define rules according to file type regardless of the application that accesses the file.

- **Trusted Rules**:

  This category is used to free certain applications from any check to avoid irrelevant blocking.

8.3.2 Whitelists and blacklists

Rule-based protection can be used in a whitelist or blacklist approach.

A **whitelist** approach consists in banning everything that is not explicitly authorized.

A **blacklist** approach consists in authorizing everything that is not explicitly banned.

8.3.3 Combining whitelists and blacklists

Both approaches can be combined depending on the environment in which the rules are applied.

It is possible to use a whitelist for everything relating to network access and a blacklist when dealing with applications that users can legitimately use.

8.3.4 Rule management

The following toolbar is used to:
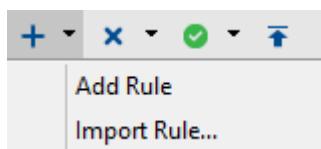
- Add
- Import
- Remove
- Change the status of rules
- Set the rule priority order
- Export

The search field is used to reduce scrolling through the list of rules.

Adding a rule

To add a rule, follow the steps below:

- Click $+$ ▾ to display the drop-down menu.
- Click on **Add Rule**.

- Define the rule settings.

Importing a rule

To import a rule, follow the steps below:

- Click $+$ ▾ to display the drop-down menu.
- Select **Import Rule**.

    A search window opens to allow you to browse for the rule file with the extension `.scer`.
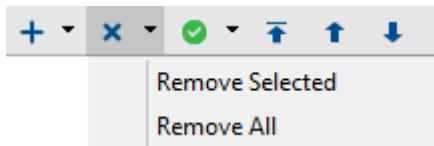
    ⚠ **WARNING**
    Rules or sub-rules (files, registries, networks and extensions) from versions lower than StormShield 7.0 cannot be imported. For older versions, only whole policies can be imported. Policies have to be converted to 7.2 format.

Removing a rule

To remove a rule, follow the steps below:

- Select the rule to be removed.

- Click to display the drop-down menu.
- Click on **Remove Selected** or **Remove All** to delete all the group rules.
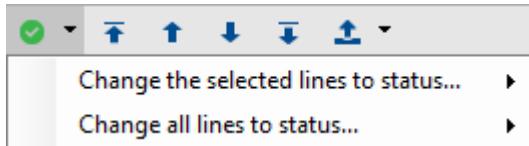
> ℹ️ **NOTE**
> To delete more than one rule at a time, press Ctrl while clicking to select the rules.
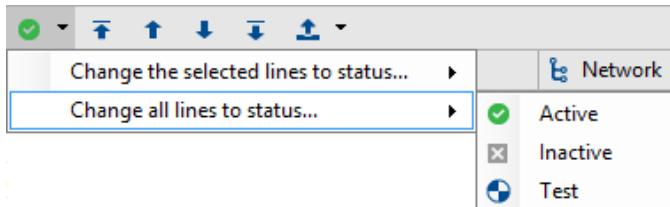
Changing the status of several rules at a time

To change the status of the rules selected simultaneously or of all the rules, follow the steps below:

- Click to display the following drop-down menu:

- Select one option:

> ℹ️ **NOTE**
> Only two statuses apply to most rules: Active and Inactive.

- Select the new status:

#	Status			n	Files	Network
10	Enabl...					Allow all
11	Enabl... Windows Application Error Reporting					Deny All Clien
12	Enabl... Windows Explorer			✓	|systemroot|\syste...	Deny Server (
13	Enabl... Windows Help Center Hosting Server			✓		Deny All Clien
14	Disab... Windows Messages Display			✓		Deny All Clien
15	Enabl... Windows Remote Desktop Protocol Client			✓		Deny All Clien
16	Disab... Windows Nslookup command			✓		Deny Server (
17	Disab... Windows Ping command			✓		Deny Server (
18	Enabl... Windows Telnet			✓		Deny Server (
19	Disab... Custom partition			✓	c:\users*\appdata...	Allow all
20	Enabl... Windows Local Security Authority Subsystem Service			✓	c:\users*\appdata...	Allow all

Menu:
- Change the selected lines to status... ▶
- Change all lines to status... ▶
  - ✓ Active
  - ☒ Inactive
  - 🌐 Test

#	Status	Identifier	Execution	Files	Network
10	Enabl... Windows vssadmin		✗		Allow all
11	Enabl... Windows Application Error Reporting		✓		Deny All Clien
12	Enabl... Windows Explorer		✓	|systemroot|\syste...	Deny Server (
13	Enabl... Windows Help Center Hosting Server		✓		Deny All Clien
14	Disab... Windows Messages Display		✓		Deny All Clien
15	Enabl... Windows Remote Desktop Protocol Client		✓		Deny All Clien
16	Disab... Windows Nslookup command		✓		Deny Server (
17	Disab... Windows Ping command		✓		Deny Server (
18	Enabl... Windows Telnet		✓		Deny Server (
19	Disab... Custom partition		✓	c:\users*\appdata...	Allow all
20	Enabl... Windows Local Security Authority Subsystem Service		✓	c:\users*\appdata...	Allow all

ℹ **NOTE**
To select more than one rule at a time, press Ctrl while clicking the rules.
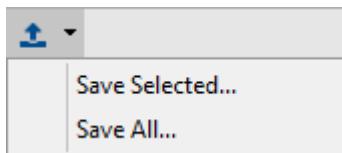
Setting the rule priority order

Two buttons are available to set the rule priority order:

- Click ⬆ or ⬇ to change the rank of the selected rule.

- Click ⬆ or ⬇ to set the selected rule at the top/bottom of the list.

Exporting a rule

To export a rule, follow the steps below:

- Click ⬆▾ to display the drop-down menu.
- Click on **Save Selected** or **Save All** to save all rules or press Ctrl while clicking to select the rules to be saved.
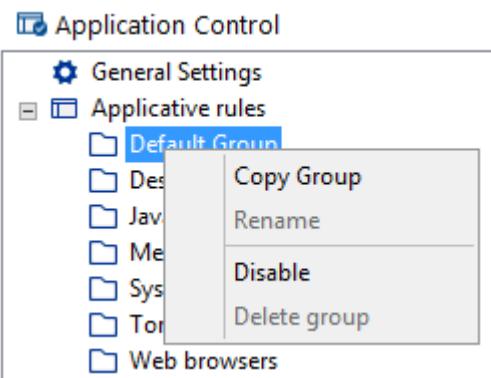

Save Selected...
Save All...

Enabling/disabling a rule group

To enable or disable a rule group, follow the steps below:

- Right-click the appropriate rule group in the settings tree structure.

- Select **Enable** or **Disable**.

ℹ **NOTE**
To disable a rule within a rule group, right-click the rule in the **Status** column.

9. Security Policies

9.1 Application identifiers

Before creating a security policy and implementing application control, you will need to create application identifiers. For more information on creating security policies, please refer to the sections Creating a security policy and Application control.

Application control relies on the concept of application identifiers, which matches the target to which the rule must apply. The first step in generating an applicative rule is to create at least one identifier in the **Application identifiers** panel in the security policy.

9.1.1 Types of application identifiers

Each identifier comprises a limited number of entries. Each entry allows identifying applications by several criteria:

- A partial or full path to the executable file.
- An MD5 or SHA-1 hash of the executable file.
- A digital signature by a specific certificate.
- A combination of a path (full or partial) to the executable file and its digital signature.

Path

Advantages

Identifying an application by its full or partial path provides the advantage of not being affected by changes made to the targeted executable file. This facilitates adaptation when there are several versions of the same application in an environment, for example. Moreover, with partial paths, differences in folders on different workstations (e.g. the "Program Files" folder on 32-bit or 64-bit systems) would not be an issue.

This filtering mode is operational as soon as Windows starts.

Disadvantages

The main drawback of such rules is the need for prior knowledge of the name of the executable file and the guarantee that it would not change after the application is updated. Furthermore, for all executable files received from an external source (Internet, for example), their names may be random, making even partial path identification ineffective. This type of identification may be dangerous if it is used for the purpose of exclusion, especially if a partial path is used. Stormshield Endpoint Security will not prevent the user from adding executable files to a folder that has been excluded in trusted applications, thereby making it possible to execute any application outside the scope of the agent's protection.

Hash

Advantages

Identifying an application by its SHA-1 or MD5 hash provides the advantage of relying not on the path of the executable file, but on its contents. This method is particularly effective in preventing the execution of known malicious executable files, regardless of how they are named and where they are located on the workstation.

An application's hash is calculated when it is executed. It will then be compared against the security policy applied to the workstation in order to ensure that it is not subject to any specific rule. If the execution of the application is prohibited, it will not be loaded.

Disadvantages

The main drawback is the need to maintain a list of hashes while taking into account each version of the same application. This is indeed an issue as the slightest change to a binary file would modify its hash, making it tedious to identify the application. Moreover, in terms of the Stormshield Endpoint Security agent's performance, the list of hashes per security policy must not exceed 50,000 entries.

Signature certificate

Advantages

Identifying an application by certificates provides the advantage of relying not on an application's version or path, but only on its digital signature. In this way, all applications from a specific vendor can be easily and quickly allowed or blocked, regardless of where they are located on the workstation.

When a signed application is executed, its signature will be checked to ensure that its integrity has not been compromised. Once this operation is complete, the agent will search for the certificate that was used to sign the application from among the certificates it has received from the management console. If this certificate appears in the list, the agent will apply the associated applicative rule.

Disadvantages
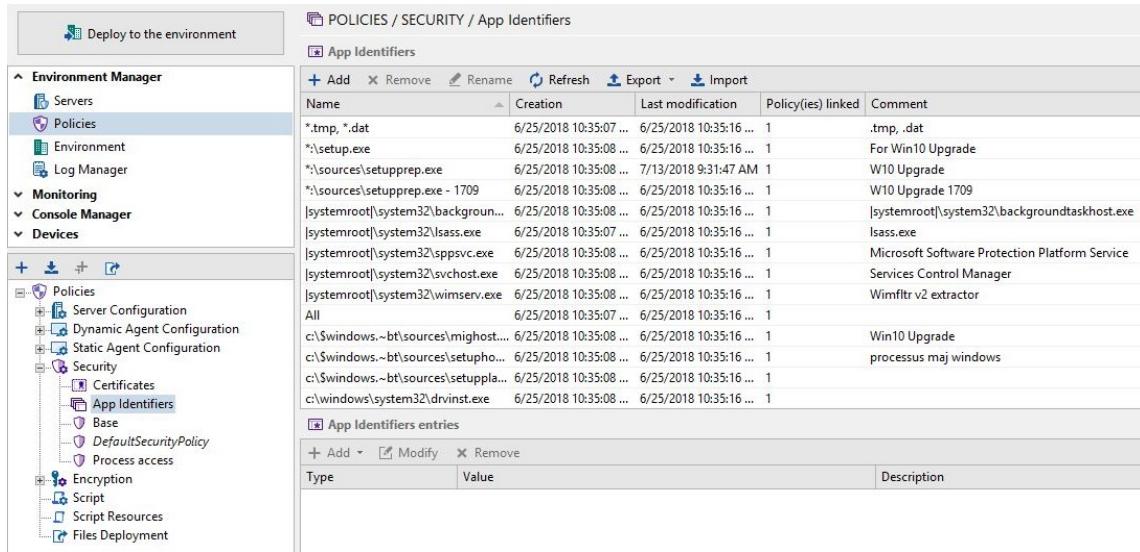
The main drawback is having signed applications so that this type of filtering would function. Most software vendors have several signature certificates and use them when providing their applications. The security of such rules therefore relies on the vendor's trust in the application's signer.

In the event an application is not signed by a certificate, the Stormshield Endpoint Security console will be provided with a signature tool (Stormshield SignTool) that will allow you to sign applications with your own certificate.

You can read the documentation for this tool when you execute it, or by clicking on the help button.

9.1.2 Creating application identifiers

Application identifiers are created in the security policy, in the **Environment Manager** section.

1. Open the **Application identifier** panel and click **Add** at the top of the panel.

2. Enter a name for the identifier and a description. Click on **OK**.

3. Click on the **Validate** button at the top of the **App identifiers** panel in order to save your identifier. Focus remains on the validated identifier.

Application identifier entries
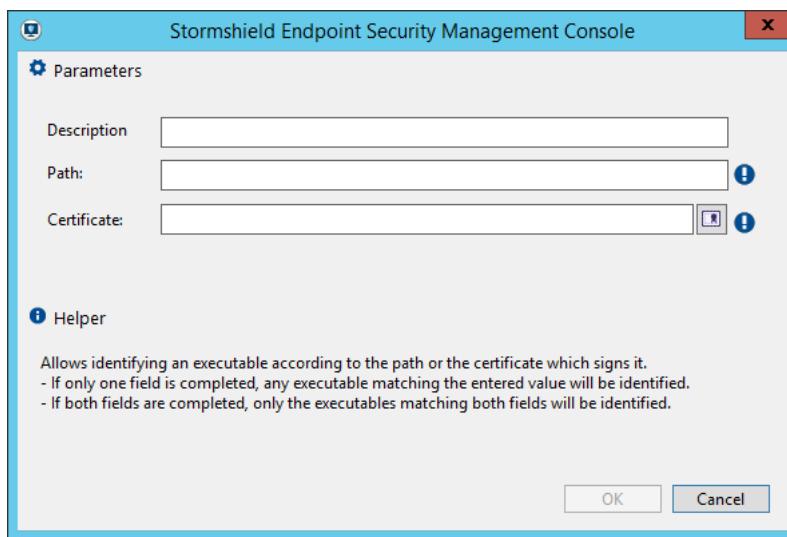
Before using the identifier in a security policy's rules, entries must first be added. Each identifier may contain an unlimited number of entries.

1. Select the identifier to edit in the upper panel.

2. Double-click it to edit it or use the **Edit** button at the top of the **App identifiers** panel.

3. Click Add in the **App identifier entries** panel.

4. Select identification by path/signature certificate or by MD5 and/or SHA-1 hash. Refer to the explanations in the paragraph Types of application identifiers regarding your choice.

Path and/or certificate

Applications can be identified either by the certificate that signed the executable file or by the executable file's partial or full path, or even a combination of both.

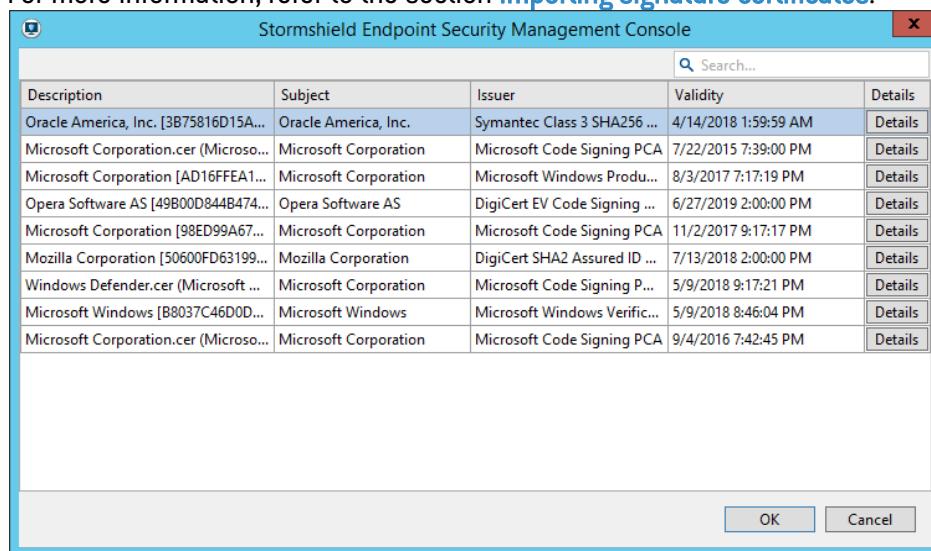1. In the window above, enter a path or select a certificate.

   - Path: This attribute defines the name of the application to which the rule applies. Using a wildcard at the end of the path lets you set a rule that covers all executable files in a given path and its subfolders.
     Example: |programfiles|\Internet Explorer*
     To apply a rule to a folder and not to its subfolder, you have to create two identifiers and replace * by ** in the second identifier. Add a rule for each of these identifiers and specify rights for each rules. The rule ** must have priority over the rule * so that both rules will be taken into account.

   - Certificate: click **Select a certificate** and select the one that will be used to identify the application in the window that opens. The list of certificates displayed in this window sets out the certificates imported in the **Certificates** panel in the security policy.
     SHA-1 certificates are supported by Windows from Windows XP. SHA-256 certificates are supported from Windows 7. When a application is signed by a certificate chain, SES only uses the more specific certificate at the end of the chain.
     For more information, refer to the section Importing signature certificates.

   When an application is signed with more than one certificate, you can choose the certificate which will be used to identify the application.

2. Click **Finish** to finalize the creation of the entry and repeat the operation each time you need to add new entries.

3. To assign application identifiers to applicative rules, refer to the section Identifer: in the security policy

Certain specificities apply when certificates are used in Stormshield Endpoint Security to identify applications. Two situations need to be considered:

- When the executable file of an application subject to an applicative rule embeds signature information, it will be extracted in order to be verified.

- When the executable file of an application subject to an applicative rule does not provide signature information, all security catalogs on the workstation will be verified (those relating to the user will be ignored). If any signature information for the executable file is found there, it will be extracted in order to be verified.
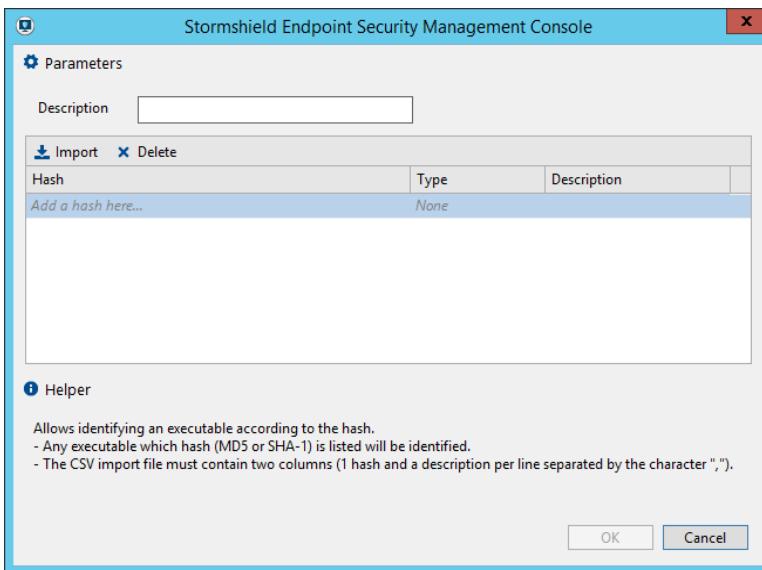
Several rules apply regardless of the type of application signature (embedded in the executable file or through the catalog):

- Neither the console nor the agent will check the CRL (Certificate Revocation List) used in application control rules.

- Neither the console nor the agent will prevent the use of expired certificates in applicative rules. The console will display a simple warning message.

- The agent's verification of a program's signature includes the cryptographic operation on the public key to check that it matches the private key on the certificate found.

- If a certificate has been added in the console, all applications signed by this certificate or any of its child certificates, without depth restrictions, will be taken into account. This relationship search is based only on the store of the local machine. Certificates in users' stores will be ignored.

- The agent will always establish the certificate's parent-child relationship up to its root. It will then check whether any of the certificates in this chain exists in its store, starting with the signer certificate of the executed application. It will stop at the first certificate in the chain that exists in its store and apply the associated applicative rules.

Hash

Applications can be identified either by an MD5 hash or by an SHA-1 hash.

1. In the window above, enter an MD5 and SHA-1 hash directly and a description. The type of hash will be automatically recognized according to its length.

   A list of hashes may also be imported from a CSV or text file. To do so, click **Import** and select the file in the Windows Explorer screen that opens.

2. Click **Finish** to finalize the creation of the entry and repeat the operation each time you need to add new entries.

   > **ℹ NOTE**
   > For the sake of workstation performance, the maximum number of synchronized hashes to Stormshield Endpoint Security agents is 50,000 per directory (Active Directory or internal directory). In other words, the number of hashes stored in the database is unlimited, but only 50,000 hashes can be applied simultaneously by an agent. When this limit is exceeded, an error message will appear in the console.

3. To assign application identifiers to applicative rules, refer to the section **Identifer:** in the security policy

The lines below can be imported as hash lists in the console:

0123456789ABCDEF0123456789ABCDEF;

FEDCBA9876543210FEDCBA9876543210;Firefox

0123456789ABCDEF0123456789ABCDEF01234567;Internet Explorer

FEDCBA9876543210FEDCBA9876543210FEDCBA98;Chrome.exe

9.2 Importing signature certificates

To enforce application control in a security policy, you must first create application identifiers as explained in the section Application identifiers

In order to identify an application by its digital signature instead of its name, certificates can be imported in the SES management console.

To find out how to use certificates for the purpose of identifying applications, please refer to the sections Signature certificate and Path and/or certificate.

To add certificates:

1. Expand the **Security** folder in the **Policies** panel's tree and select **Certificates.**
2. Click on **Import** at the top of the **Certificates** panel.
3. In the window that opens, select the various certificates to import.
4. Confirm your changes by right-clicking on **Certificates** in the tree on the left, and then by clicking on **OK**. You may also click on **OK** at the top of the panel in which certificates are imported.

This feature supports X509 certificates.

In the **Certificates** panel, each certificate has various attributes:

- Description: name of the imported file
- Object: common name (CN) of the imported certificate
- Issuer: issuer of the imported certificate
- Validity: expiry date of the certificate. Do note however that the Stormshield Endpoint Security agent will not block applications with expired certificates. This date is indicated for information only. The **Validity** field will therefore be shown in italics with "Expired" in brackets once the certificate has expired.
- Details: button that opens a window summarizing all information about the imported certificate.
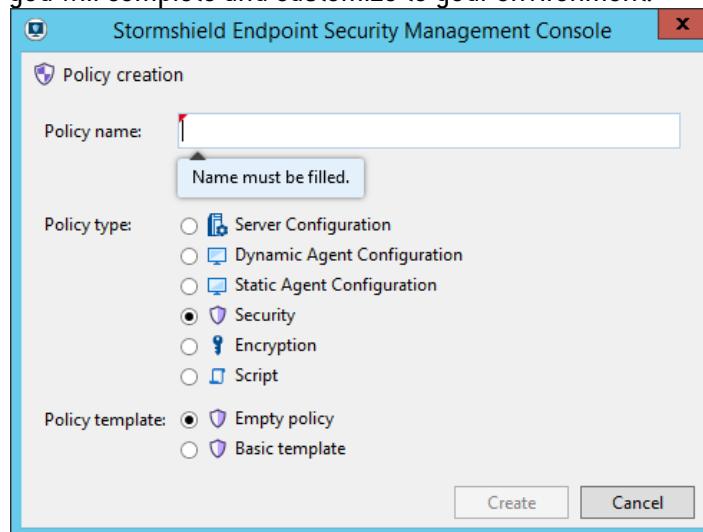
Once they are validated, certificates will be saved in the database of the SES management console. There is therefore no need to save files on the disk.

9.3 Creating a security policy

1. Click **Policies** and the ＋ button. The window **Policy creation** opens.
2. Enter a policy name and select the **Security** type.

3. Select a template. The policy templates are:
   - **Empty policy**: no blocking is set up.
   - **Basic template**: includes system and network basic security rules required for standard Windows services to work properly on workstations. This policy provides a basis which you will complete and customize to your environment.

4. Click on **OK**. The policy edition window opens.

You can also import policies. For more information, refer to the section Importing security policies.

9.4 Importing security policies

9.4.1 Import a new policy

1. Click on **Policies** in the **Environment Manager** menu, and then on the ⬇ button.
2. In the files selection window, select one or more files to import (*.sczp* or *.scep* files).
3. Edit the names if necessary.
4. Click on **Import**.
5. If application identifiers used in the imported policies are already listed in the console, select an option between:
   - **Duplicate the app identifier**: allows creating a new identifier from the imported resources. The new identifier will have an automatically generated name to avoid name collisions.
   - **Replace the app identifier**: allows replacing the existing identifier. This option allows guaranteeing that the behavior of the imported policy will be exactly the same as its behavior prior to the import. Warning: selecting this option may modify the behavior of other policies using the same identifier.
   - **Keep the app identifier**: allows using the identifier as it currently is in the console. Warning: selecting this option may modify the behavior of the security policy if the identifier was modified between the export and import.

9.4.2 Importing a policy from an existing policy

If you wish to keep the links to the environment elements in an existing policy, you can duplicate this policy and edit or replace the content. To do so, open and edit the policy, and click on the button **Import** at the top of the policy edition panel.

Importing a full policy

The first tab of the window allows importing a full policy (.sczp or .scep files) or a full policy template. The content of the current policy will be fully replaced by the imported policy. If application identifiers used in the imported policy are already listed in the console, choose between **Duplicate**, **Replace** or **Keep**.

Importing rules groups

On the contrary, in the **Rules groups** tab, you can choose to import some rules groups related to application control or network security control. This import does not override the rules existing in the policy.

9.5 Editing a security policy

The security policy edition window is divided into four tabs corresponding to different categories of settings: *System Behavior*, *Device Control*, *Network security control* and *Applicative rules*.

The **Links** tab lists the organizational units and Stormshield Endpoint Security groups on which the policy is applied with the corresponding application condition.

9.5.1 System Behavior

General settings of the *System Behavior* tab allow defining system behavior control and application behavior control.

Select **Kernel Components** in the **System Behavior** panel to control driver loading and detect suspect drivers.

System Behavior Control

The System behavior control settings are the following:

- **Enabled/Disabled**.
- **High/Low/Critical/Advanced**.

- **Executable file creation**:

  Possible settings are the following:

  ○ **Disabled**:

    By default, this parameter is set to **Disabled**.

◦ **High**:

This parameter prevents the creation of the following executable files:

com	dll	exe	msi	mst	scr	cpl

◦ **Critical**:

This parameter prevents the creation of the following executable files:

bat	com	exe	mst	scr	vbs
cmd	dll	inf	pif	sys	ws
chm	drv	msi	reg	vbe	wsm
cpl					

It is possible to authorize or ban the creation of executable files with a specific extension for a specific application. To do so, go to the applicative rules in the *Application control* tab of the security policy. Add an applicative rule for one or more identifiers and specify the extension (*.ext*) and the access right in the **Files** column. For more information, see section Files.

- **Protection against privilege escalation**:

This parameter enables or prevents applications from letting a process gain administrator or system rights.

Possible values are the following:

◦ **Disabled**:

Default setting.

◦ **High**:

The following privilege escalation attempts are blocked:

- Attempt to obtain the privilege to load a driver
- Attempt to elevate kernel privileges
- Theft or manipulation of a process security context

◦ **Critical**:

In addition to mechanisms blocked by the **High** level, the **Critical** level blocks the attempt to obtain the debug privilege (may generate false positives).

The privileges requested by applications are saved in system logs.

- **Protection against spontaneous reboots**:

Possible settings are **Enabled** or **Disabled**.

It is usually the user who restarts the system but malicious software can trigger spontaneous reboots in order to:

◦ Cause a denial of service.

◦ Prevent patches from being downloaded.

◦ Prevent antivirus signatures from being downloaded.

This parameter prevents or allows applications to access privileges which permit system reboot.

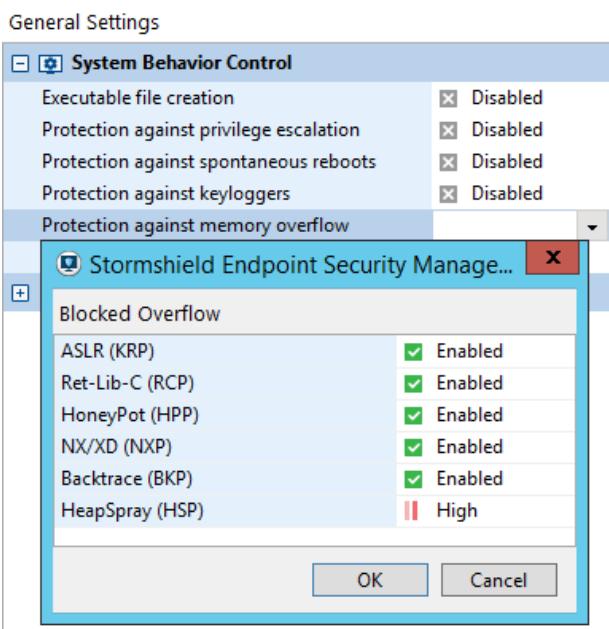The privileges requested by applications are saved in system logs.

- **Protection against keyloggers**:

Keylogging is used to capture keyboard events in order to steal passwords, confidential information, etc.

Possible settings are the following:

- **Disabled**:

  No blocking, no log. Default setting.

- **High**:

  Keylogging is blocked.

- **Critical**:

  Best defense against graphical interface hooking (any event related to the graphical user interface is captured).

- **Protection against memory overflow**:

Memory overflow occurs when programs attempt to write data beyond the allocated memory.

These extra bytes replace valid data, and are executed as a program code.

Possible settings are the following:

- **Disabled**:

  No protection. Default setting.

- **Low**:

  This is a combination of the options KRP+RCP+HPP+HSP (Low).

- **High**:

  Low+HSP (high)+NXP or BKP applied to network processes.

- **Critical**:

  This is a combination of the following options:

  - High+BKP applied to network processes if NXP is already enabled

  or

  - High+BKP applied to all processes if NXP is disabled.

- **Advanced**:

  The administrator can disable one or several protection techniques in case of incompatibility.

  Possible options for **Advanced** are the following:

- **ASLR (KRP)**:

  This option is used to randomize the base address of `kernel32.dll` when it is mapped into memory (under XP) on each reboot.

  Restart the computer for ASLR (KRP) activation/deactivation to be taken into account.

- **Ret-Lib-C (RCP)**:

  This option blocks `return-into-lib(c)` attacks.

- **HoneyPot (HPP)**:

  This option generates decoys which will be used by malicious code to find `kernel32.dll`.

- **NX/XD (NXP)**:

  First of all, you will have to enable this feature in the BIOS (Basic Input/ Output System) of your machine as well as the DEP (Data Execution Prevention) feature in Windows.
  This option in Stormshield Endpoint Security blocks the execution of processes based on memory addresses but does not kill the process in progress. There is a high risk of false positives, though.

  You can disable this option so as not to block the process in progress. It can prove useful when a legitimate process executes code in the memory addressing space.

- **Backtrace (BKP)**:

  This option is used to track the operations which led to the execution of untrusted code.

  This option can slow down the performance of your machine. If necessary, you can disable it.

- **HeapSpray (HSP)**:

  This option allows blocking HeapSpray attacks. In most cases, such attacks are executed from web browsers or even from the Microsoft Office suite. There are three levels of protection: Disabled (grayed-out cross), High (red arrow) and Low (yellow arrow).

ℹ️ **NOTE**
Some applications legitimately use mechanisms targeted by automatic protections.
For instance, the debugging function in a software development tool can legitimately use process injections whereas a remote control tool will perform keyboard event captures.
This is why Stormshield Endpoint Security has the ability to trust these applications, at each category level.
This feature is described in:

- **Trusted applications**.

- **Attributes**

Protection	ASLR	RET-LIB-C	Honeypot	NX/XD	Backtrace	HSP
Disabled	off	off	off	off	off	off
Low	on	on	on	off	off	low
High	on	on	on	on	off	high
Critical	on	on	on	on	on	high
Advanced	on/off	on/off	on/off	on/off	on/off	high/low/off

⚠️ **WARNING**
In case of incompatibility between an application and the memory overflow protection, it is recommended to check that the application is running properly by disabling only protection options NX/XP (**NXP**) and Backtrace (**BKP**).
Should the problem persist, add a rule in **Trusted Rules** from the *Applicative rules* tab.

ℹ️ **NOTE**
NX/XD and Backtrace:

- When the **NX/XD** option is disabled or not present on your computer, the Backtrace option will then be enabled.

- The **Backtrace** option is always enabled when Protection against memory overflow is set to **Critical**.

• **Kernel component protection**

This parameter enables the administrator to activate or deactivate the detection of driver downloads (only for 32-bit operating systems).

Possible settings are the following:

◦ **Disabled**:

Kernel driver detection is disabled. No log event has been created on the Stormshield Endpoint Securityserver.

◦ **Low**:

New drivers and suspect drivers will not be blocked. They will only be detected. If the security policy prohibits certain drivers from being downloaded, these drivers will be blocked.

◦ **High**:

New drivers and suspect drivers are blocked on next boot. The drivers installed by Windows Update are automatically trusted.

◦ **Critical**:

Unknown drivers and suspect drivers are blocked on next boot. The drivers installed by Windows Update are automatically trusted.

ⓘ NOTE
Blocking of new drivers can be temporarily suspended with the challenge **Install drivers**.

ⓘ NOTE
After enabling kernel component protection, workstations equipped with agents need to be restarted to take the change into account.

Application Behavior Control

Application Behavior Control parameters can be set to:

- Enabled/Disabled
- Critical/High/Disabled

- **Applications access**:

    The application injection mechanism is used by malicious code in order to:

    ◦ Block another application from operating.

    ◦ Corrupt the application.

    ◦ Take control over the application.

    Possible settings are the following:

    ◦ **Disabled**:

        No blocking, no log.

    ◦ **High**:

        All attachments are blocked.

    ◦ **Critical**:

        All attachments are blocked and the access to the system specific information is blocked by default.

        If this protection is enabled and if stopping the agent is allowed in the dynamic configuration, verify a trust rule for the *|systemroot|\system32\consent.exe* user account control exists (rule included in the policy basic template). If this rule does not exist:

1. Add the rule in the trusted rules in the **Application Control** tab.
2. When the rule is created, check the **Advanced mode** box.
   The column **Access to this application** displays.
3. Check the box in this column.

For more information on this option, see section Trusted domains.

Some applications legitimately use mechanisms targeted by automatic protections.

For example, the UAC (User Account Control) under Windows 7 and upwards, as well as the debugger of a software development tool, may legitimately perform process injections. Stormshield Endpoint Security allows trusting these applications. For more information, see section Trusted applications.

- **Execution Control**:

  This mechanism monitors the execution of applications installed on the workstation. Malicious code may actually be hidden within authorized applications.

  Possible settings are the following:

  - **Disabled**:

    No blocking.

  - **Enabled**:

    Allows the execution of the binary files which are listed in the Windows system directory.

- **Execution control on removable devices**

  This control mechanism allows requesting a confirmation from the user when an application starts from a removable device connected to the agent.

  Possible settings are the following:

  - **Enabled**:

    A confirmation from the user is requested when an executable file is launched from a removable device.

  - **Disabled**:

    No confirmation from the user is requested when an application tries to start from a removable device and the application can start.

  When this mechanism is used, a log message is created.

  The confirmation message directed at the user can be customized. In **Log Manager**, choose the type **System Logs** and edit the notification message of the lines (#.)?EXE_ON_USB BLKEXECUTE and (#.)?EXE_ON_USB WARN. The message will display in a confirmation window on the agent.

- **Socket access**:

  Possible settings are the following:

  - **Disabled**: Blacklist policy.

    No network blockage except when explicitly banned.

  - **High**: Whitelist policy.

    Most accesses are allowed.

  - **Critical**: Whitelist policy in which no network access is allowed unless it has been explicitly declared. This level may generate false positives.

- **File access**:

  This parameter is used to prevent the corruption and modification of executable file names.

  Possible settings are the following:

  - **Disabled**:

    No blocking, no log.

  - **Enabled**:

Any attempt to rename a file will be verified. Any attempt to edit an executable is blocked.

⚠️ WARNING

This protection is a very powerful but also very restrictive tool.
Updating an application requires that you first disable the protection.
It is highly recommended to use the Warning mode in order to adjust a policy.

Kernel Components

This category enables control over driver loading and detects suspect drivers.

The Kernel Components attributes are the following:

- **Status**:

  This attribute can be set to Enabled or Disabled.

- **Name**:

  This attribute is the driver name.

- **CheckSum**:

  This attribute is the driver hash.

  The list cannot include the same hash twice but different drivers can have the same name with a different hash.

- **Loading**:

  This attribute can be set to Allowed or Denied.
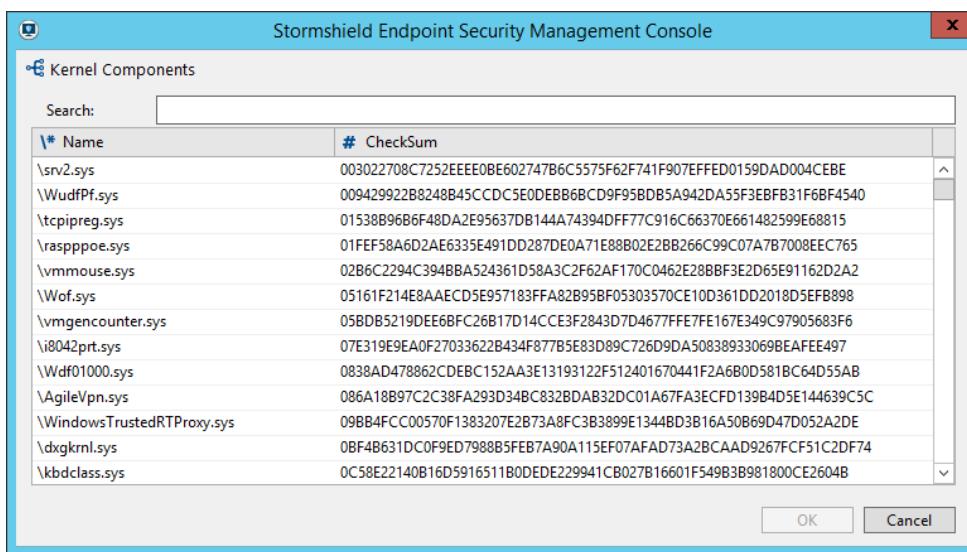
- **Log**:

  This attribute defines the settings for saving and viewing log files.

- **Description**:

  This attribute is a freeform comment.

To add a driver to the list of kernel components, click ➕ in the toolbar.
The following window is displayed:

The list of kernel components is automatically generated from the drivers loaded on the workstations on which the agent has been installed. The protection must be set at least to Low in order for the loaded drivers to be listed.

> **ℹ NOTE**
> The list of kernel components is only generated from 32-bit workstations.

You can use the Search field to make sure that a driver or its hash is not already present in the list.

9.5.2 Device Control

General settings

Device control can be set to **Allowed** or **Denied**.

Device Control covers the following items:

- Modems (examples: RTC, 3G).
- Bluetooth.
- IrDA (Infrared Data Association) ports.
- LPT (parallel) ports.
- Comm ports.
- USB smart cards.
- Floppy disk drives (internal or external).
- CD/DVD/Blu-Ray.
- CD/DVD/Blu-Ray Writer.
- PCMCIA cards.
- USB audio cards.
- USB HID (Human Interface Device) keyboards or pointing peripherals (examples: mouse, graphics tablet, etc.).
- USB still imaging (examples: cameras, scanners, etc.).
- USB printers.
- U3 feature: It blocks autorun execution on U3 USB keys and CD-ROM readers.
- USB/FW mass storage: It consists of devices such as USB keys and hard disks, FireWire, etc.
- Group management: enables or disables removable device groups.

> ⚠️ **WARNING**
> If the **Group management** parameter is modified in the policy, we strongly recommend that you restart your workstations so that SES agents may correctly apply the latest security policy. Likewise, we advise against applying two security policies with different **Group management** values either by script or by condition.

- Mass storage recovery: Allows the user to decrypt mass storage devices that have been encrypted with Stormshield Endpoint Security.
- Mandatory password strength (Standard by default): It is used to encrypt mass storage devices with Stormshield Endpoint Security.

> ℹ️ **NOTE**
> The administrator can create policies applied to agent groups using removable devices. Settings will be more accurate. See Creating an encryption policy to be applied to a group of devices.
> For more information, please refer to Removable Device Encryption.

Devices with access set to **Denied** are blocked. This information is stored in Device Logs and the user receives an alert. For more information, see section Device Logs.

Removable devices

Using groups of removable devices strengthens data security.

You can tailor each group of removable devices to ensure compliance with the company's usage guidelines relating to devices. For example, you can create separate groups of devices based on employees' job requirements, their hierarchical position in the company, etc.

A group of removable devices for R&D engineers might contain fewer restrictions than an administrative group.

Overview

Under **Removable Devices**, click on **Default Group** or create a new device group.

1. To create a new device group, right-click **Removable Devices** and click **Add Group**.
2. To change the group name:
   - Select the name.
   - Press **F2**.
   - Enter the new name.
     You cannot rename the **Default Group**.

The group settings panel on the right changes according to the device type selected in the **Group Settings** area. The following areas are available:

- **Area A: Group Settings.**

  These settings are applicable to all removable devices in the group.

- **Area B: USB Settings**

  These settings allow changing the enrollment status of removable devices in the group.

- **Area C: Individual device settings**

  This is the list of devices that make up the group.

- **Area D:** Exceptions by file extension

  For removable storage devices and CD/DVD/Blu-Ray, you can specify exceptions to default access rules according to file extension.

  Example: You can set the default access rule to **Denied** for a given device or device type but allow Read access to Excel or Word files.

Group Settings

Group settings apply to **all** removable devices in the group.

SES - ADMINISTRATION GUIDE - V 7.2
9. SECURITY POLICIES

The **Group Settings** can include the **six** following items according to the device type selected:

- Device type.
- Default access rights.
- Audit.
- File encryption.
- Access right if encryption is cancelled.
- Stand-alone decryption tool (SURT).

Device Type

This parameter defines the device type. It can assume the following values:

- **Mass storage**.
- **ActiveSync (USB)**:

  It is used to synchronize with mobile phones (Windows).

- **Other USB devices**:

  It is used for all other types of USB devices.

- **PCMCIA** :

  It enables the user to insert PCMCIA cards.

- **CD/DVD/Blu-Ray**.

After selecting a device type, the data related to this value is updated and set as default.

Default access rights

This parameter can assume the following values:

- **Denied**:

  By default, the user has no access rights to the devices in the list.

  If default access for the device group is set to **Denied**, when the user tries to read or write to a device pertaining to this group, the action will be blocked and the event entered into the Device Logs.

- **Read**:

  By default, the user has read access rights to the devices in the list.

  If the user tries to write to any device listed, the action will be blocked and the event entered into the Device Logs.

- **Read/Write**:

  By default, the user has both read and write access rights to all devices in the list.

Page 152/393   *ses-en-administration_guide-v7.2 - 06/22/2023*

> **ⓘ NOTE**
> You can add a list of files that will be excluded from the **Default access rights** settings.
> This list is defined in Area C called **Exceptions by file extension**.

<u>Difference between Access Denied from General Settings and from Removable Devices</u>

When access to a removable device is denied from the security policy under **Device Control > General Settings**, the volume appears on your workstation but not its content.

When access to a removable device is denied from **Device Control > Removable Devices**, the volume appears on your workstation.
However, you can list the volume files and folders even if access is denied. Creating empty folders is also possible but not new files.

Audit

This parameter is used to enable the audit of a specific group of mass storage devices.

This parameter allows you to track device use without blocking device actions. You can gather information on how devices are being used. Whenever an audit is enabled, it is recorded in Device Logs.

The Stormshield Endpoint Security agent does not notify the user when an audit is triggered. However, the user can view auditing activity in the **Monitoring > Device Logs** panel.

It can assume the following values:

- **Disabled**:

  Auditing is disabled.

- **Plug/Unplug**:

  An audit entry is written into Device Logs when a device in the list is plugged into or unplugged from the computer. This entry includes the device size and storage capacity.

- **File access**:

  An audit entry is generated into Device Logs when:

  - A device in the list is plugged into or unplugged from the computer.
  - A file on the device is either created, renamed or deleted.

- **Write access**:

  An audit entry is generated into Device Logs when:

  - A device in the list is plugged into or unplugged from the computer.
  - A file on the device is either created, renamed, modified or deleted.

- **Read-only access**:

  An audit entry is generated into Device Logs when:

  - A device in the list is plugged into or unplugged from the computer.
  - A file on the device can either be created, renamed, open for reading, modified or deleted.

🛑 **WARNING**

Auditing **records** actions in Device Logs. It does not block unauthorized use.
Blocking unauthorized use is controlled by the **Default access rights** settings and the list of exceptions under the **Removable Devices** panel.

File encryption

This parameter and the two following parameters enable the encryption of the files stored on a USB or FireWire device. It can be set to **Enabled** or **Disabled**.

For more information, see chapter SURT.

Access right if encryption is cancelled

The values of this parameter may be:

- Read (only).
- Read/Write.
- Denied.

if the user chooses not to encrypt the device when prompted to create an encryption password.
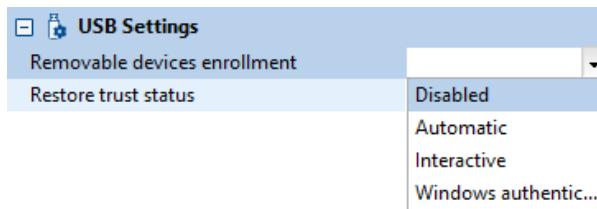
Stand-alone decryption tool (SURT)

This parameter allows or denies the use of the SURT decryption tool to enable file decryption on removable devices, for systems not running Stormshield Endpoint Security.

If this option is enabled, the SURT application will be copied onto the removable devices encrypted by Stormshield Endpoint Security.

USB settings

USB settings apply to USB devices of the group and include the following options:

Enrollment of removable devices

This option allows to enroll removable devices listed in the group and not already enrolled, directly from a Stormshield Endpoint Security agent.

This parameter can assume the following values:

- **Disabled**: Default setting. The removable device is not automatically enrolled.
- **Automatic**: The removable device is automatically enrolled. A window notifies the user.
- **Interactive**: A window asks the user to confirm the removable device enrollment. When the device is enrolled, a window notifies the user.
- **Windows authentication**: A window asks the Windows credentials of the user. When the device is enrolled, a window notifies the user. The device is enrolled for the user previously specified in the window.

ⓘ NOTE

When plugging the removable device, a user of the Active Directory must be authenticated in Windows for the automatic or interactive enrollment to work.
This user becomes owner of the removable device and a log is sent to Device Logs.
Automatic and interactive enrollments are displayed in the enrolled devices list in the console after these logs have been processed.

ⓘ NOTE

When the enrollment status of the removable device is invalid (corrupted enrollment or device enrolled for another organization) and automatic or interactive enrollment is enabled, the user is asked whether he wishes to enroll his device again in order to use it in the new environment. If the user accepts, the trust status is lost. To restore the trust status, it is thus necessary to run the device on a station dedicated to checking incoming media.

Restore trust status

When a file is added or modified on the removable device outside the Stormshield Endpoint Security controlled area, it loses its trust status but remains enrolled. When this option is enabled, the antivirus installed on the workstation checks the file as soon as the device is plugged in, in order to restore the trust status.

Restore trust status only applies to enrolled devices.

⚠ WARNING

All files of the removable device must at least be accessible in Read mode so that trust status enforcement works.

For more information about removable device enrollment, see chapter Removable Device Administration.

Individual device settings

Overview

You can create a group of devices by adding individual devices and their parameters.

Removable Devices

	Device Type	Vendor ID	Product ID	Serial ID	Enrollment	Description
☑	usb	3034	89654	569xk63	All	
☑	firewire	4569	456789	oi65599kk56	All	

Individual devices include specific details (device type, vendor ID, etc.).

The individual devices added to the list must include part or all of the following information:

- **Status**:

  It indicates whether the rule status is enabled or disabled (mandatory field).

- **Device type**:

  It can assume the values USB or FireWire.

- **Vendor ID**:

  This is the identification number of the device vendor.

- **Product ID**:

  This the product code of the device.

- **Serial ID**:

This is the serial number of the device. Enter this number if you want to assign parameters to an individual device, otherwise leave the field blank.

- **Enrollment**:

  This parameter is specific to USB devices. The following values are available:

  - All: the rule applies to all devices.

  - Enrolled: the rule only applies to enrolled devices.

  - Trusted: the rule only applies to enrolled devices that have not been modified from a workstation not protected by Stormshield Endpoint Security.

For more information about this setting, refer to section Delegation of the removable device administration.

- **Description**:

  You can add a comment about the device (optional).

  ### ⓘ NOTE
  You can use a wildcard to create a rule to include any USB or FireWire device.
  To do this, set all fields to * except for the **Serial ID** which should be left blank.

This information can be added manually, by automatic device detection or by copying/pasting from the device enrollment panel. For more information, see Procedure (Step 4).

Procedure

To add a new removable device to a group, follow the steps below:

1. Click ➕ . The **Device** window is displayed:

2. Add a device to the list manually or automatically. To do so, click on the **Manual mode** or **Automatic detection** radio button. Repeat the operation with each device.

   If you select automatic detection, you will need to plug in each device to be added.

   ### ⓘ NOTE
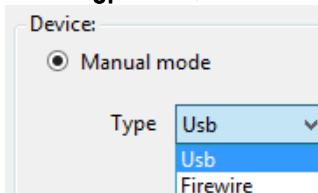   Depending on how you want to use the device group, you may not want to provide specific information for each category.
   For example, you may want to include all the devices from one vendor.
   In this case, you would not include the Serial and Product IDs.

   - If you click on the **Manual mode** radio button, follow the steps below:

- In the **Type** field, select **usb** or **firewire** from the drop-down menu.

- Enter the following information as appropriate:

- Vendor ID.
- Product ID.
- Serial ID.
- Description.
- Enrollment.

  ○ If you click on the **Automatic detection** radio button, in the **Type** field, select **usb** or **firewire** from the drop-down menu.

  Stormshield Endpoint Security will detect any device currently plugged into the USB port and add them to the group.

  The Device window automatically refreshes and displays the new information.

  The new device is automatically selected. You can deselect it by clicking on its line.

  If necessary, you can delete any unwanted device from the group.

3. Enter a **Description** (optional).

4. Click **OK**.

   The removable device is added to the device group.

5. Edit device information as needed.

6. Create a list of exceptions by file extension (optional).
   For more information, see section Procedure.

You can also copy a selection of devices from the **Enrollment** panel and paste them directly in the **Removable Devices** panel by clicking right > **Paste**.

Exceptions by file extension

Overview

You can specify exceptions to the default group settings. These exceptions are based on file extensions.

For example, **Group Settings** Default access rights can be set to Denied but you can allow `txt`, `rtf`, `jpg`, etc. files to be read in **Exceptions by file extension** (area D) by setting the Rights field to Read.

This parameter can assume the following values:

- **Denied**:

  If a user tries to read from or write to a denied file (which is stored on a device pertaining to the group), the action will be blocked even if **Group Settings** default access rights are set to **Read/Write** or **Read**.

- **Read**:

  The user can read from "excepted" files on devices even if **Group Settings** default access rights are set to **Denied**.

Even if **Group Settings** default access rights are set to **Read/Write**, the user can read but not write into these "excepted" files.

- **Read/Write**:

  The user can read from and write to an "excepted" file on listed devices even if **Group Settings** default access rights are set to **Denied**.

  🛑 **WARNING**
  Exceptions by file extension apply to all devices in the device group.

Procedure

To create a list of exceptions by file extension, follow the steps below:

1. Above the **Extension** column, click ➕ to add a rule.

   By default, rights are set to **Denied**.

	Extension	Rights	≡ Description
✅	doc	Read/Write	Word files
✅	exe	Denied	Executable

2. Double-click the **Extension** column field.

3. Enter a file extension (example: `doc`).

   ℹ️ **NOTE**
   To add an extension, you only need to enter the letters that indicate the extension. No wildcard is needed. For example, you do not need to enter *.doc, doc is enough.

4. In the **Rights** column, enter the access rights assigned to the file extension.

5. Enter a **Description** (optional).

Examples

The following three examples illustrate how you might use device group policies to reinforce your company's usage standards.

Example 1

In this example, a device group rule called "Minimal Access" is created to handle any device not specified in any other rule.
Example 1 is the most restrictive example.

To create this example, follow the steps below:

1. Set **Default access rights** in **Group Settings** to **Denied**.

2. Click ➕ to add a rule.

3. In the **Device** window:

   - Select **Manual mode**.

   - Set Type to usb.

   - Enter 0 in the **Vendor ID** and **Product ID** fields.

   - Leave the **Serial ID** blank. This acts as a wildcard.

     The result is that all devices are blocked by default.

   - Enter a **Description** (optional).

   - Click **OK**.

4. Repeat Step 3 to block all **FireWire** type devices.

5. Set the access rights for the "excepted" files (`doc`, `xls` and `ppt`).

6. The result should look similar to this example:

Removable Devices / Default Group

Group Settings	
Device Type	Mass storage
Default access rights	Denied
Audit	☒ Deactivated
File encryption	Disabled
Access right if encryption is cancelled	Read
Stand-alone decryption tool (SURT)	☒ Denied
USB Settings	
Removable devices enrollment	Interactive
Restore trust status	Disabled

Removable Devices

Device Type	Vendor ID	Product ID
☑ usb	0	0
☑ firewire	0	0

Extension	Rights	☰ Description
☑ docx	Read/Write	
☑ xlsx	Read/Write	
☑ pptx	Read/Write	

Example 2

In this example, a "VIP" group is created to handle specific devices used by highranking company officials.
Access is unrestricted but devices are listed individually.
Vendor, product and serial IDs are included so that only individually-identified devices can be used. The serial ID is especially important in specifying a unique device.

ℹ️ **NOTE**
An unidentified device would be treated under the "Minimal Access" group rule created in Example 1.

To create this example, follow the steps below:

1. Set **Default access rights** in **Group Settings** to **Read/Write**.

2. Click ➕ to add a USB device.
   - Define the usb settings:
     - Type.
     - Vendor ID.
     - Product ID.
     - Serial ID.

Description (optional).
   - Click **OK**.

3. Repeat Step 2 to add a rule for all USB and FireWire devices belonging to company directors.

ℹ️ **NOTE**
In this example, we grant read/write rights on all devices.
That is the reason why it is highly recommended to fill in the information fields – in particular the serial number field – available for each device.

4. The result should look similar to this example:

Removable Devices / Default Group

Group Settings	
Device Type	Mass storage
Default access rights	Read/Write
Audit	☒ Deactivated
File encryption	Disabled
Access right if encryption is cancelled	Read
Stand-alone decryption tool (SURT)	☒ Denied
USB Settings	
Removable devices enrollment	Interactive
Restore trust status	Disabled

Removable Devices

	Device Type	Vendor ID	Product ID	Serial ID	Enrollment	Description
✓	usb	79534	58665	56924xk63	All	
✓	firewire	123456789	65989	oi65599kk56	All	

Example 3

In this example, an "Employee" group is created.

Access is:

- Less restricted than in the "Minimum Access" group of example 1.
- More restricted than in the "VIP" group of example 2.

The "Employee" group does not list individual devices but lists groups of devices.

This is useful for restricting devices to company-issued devices that use particular vendor and product IDs.

Default access and audit settings, and file exceptions will then apply to any device that matches both the vendor and product IDs of one of the devices listed.

To create this example, follow the steps below:

1. Set **Default access rights** in **Group Settings** to **Read/Write**.

2. Click ✚ to add a device type.

3. In the **Device** window, create a device group:
   - Select detection mode: **Manual mode** or **Automatic detection**.
   - Set the device type. **usb** or **firewire**.
   - Define the following parameters:
     - Device Type.
     - Vendor ID.
     - Product ID.
     - Description (optional).
   - Leave the **Serial ID** blank.
   - Click **OK**.

4. The result should look similar to this example:

Removable Devices / Default Group

Group Settings	
Device Type	Mass storage
Default access rights	Read
Audit	☒ Deactivated
File encryption	Disabled
Access right if encryption is cancelled	Read
Stand-alone decryption tool (SURT)	☒ Denied
USB Settings	
Removable devices enrollment	Interactive
Restore trust status	Disabled

Removable Devices

Device Type	Vendor ID	Product ID
☑ usb	79534	58665
☑ firewire	123456789	65989

Extension	Rights	☰ Description
☑ docx	Read/Write	
☑ xlsx	Read/Write	
☑ pptx	Read/Write	

9.5.3 Network security control

General settings

Network Activity Control

Stormshield Endpoint Security protects network activity through an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS).

The interest of the IDS is multiple:

- The embedded IDS provides the client workstation with standalone attack detection capabilities, even when roaming away from the company's network protection systems.
- The IDS returns alerts that precisely identify recognized attacks.

The **IDS** is integrated with the firewall built into Stormshield Endpoint Security to form an Intrusion Prevention System (IPS).

The **IPS** alerts the administrator and blocks in real time attacks detected in incoming traffic. Depending on the IDS sensitivity defined by the administrator, the alerts generated may trigger the dynamic application of a filtering rule by the firewall in order to temporarily cut off network access at affected port and protocol levels.

Network Activity Control settings are used to block network communications depending on the seriousness of the alert.

The **Network Activity Control** parameters are the following:

- **Firewall State**:

  This setting can be set to **Enabled** or **Disabled** and allows enabling or disabling all the Stormshield Endpoint Security network protections.

  ⚠️ **WARNING**
  If the setting is disabled, all the firewall, wifi and network rules defined in the applicative rules are disabled.

- **IDS sensitivity**:

  Possible settings are the following:

  ◦ **Low**:

    Any suspect network activity is logged.

  ◦ **High**:

    Any illegal network activity is blocked.

  ◦ **Critical**:

    Any illegal network activity is blocked. When enabled, this option is used during ARP cache analysis to block identity theft.

Correlation between IDS and IPS

The IDS sensitivity setting enables/disables the following IPS features:

- Protection against flooding.

- Protection against port scan.

- Protection against ARP cache poisoning.

Protection against flooding

It protects connections using the TCP protocol against flooding.

It monitors incoming connections and removes connections which remain too long in `SYN_RCVD` or `FIN_WAIT` state (~ 10 seconds).

If the IDS is set to **High**, and more than 20 connections are blocked in `SYN_RCVD` or `FIN_WAIT` state, these connections are removed.

Log excerpts:

```
[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(SYN_RCVD;16006;1533)]ÿ[192.168.42.121]ÿ
[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME1]ÿ[20]ÿ[0]
```

```
[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(FIN_WAIT1;80;6218)]ÿ[192.168.42.122]ÿ
[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[20]ÿ[0]
```

If the IDS is set to **Critical**, and more than 10 connections are blocked in `SYN_RCVD` or `FIN_WAIT` state, these connections are removed and the firewall generates a rule to block the connections coming from the source IP address.

Log excerpt:

```
[FLOOD]ÿ[IP_BLOCKED]ÿ[0]ÿ[192.168.42.122]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ
[20]ÿ[0]
```

The number of connections in `SYN_RCVD` state per service is limited (port).

IDS level	Protection against flooding
Low	Disabled
High	Connections are removed when exceeding 20 in number
Critical	◦ Connections are removed when exceeding 10 in number ◦ Source IP address is blocked

Protection against incoming port scan

⚠ **WARNING**
To use this protection, you must have enabled **Protection against port scan** in **General Settings > Network Activity Control**.

⚠ **WARNING**
The workstation must be restarted if this protection is disabled.

It consists in filtering:

- The `RST_ACK` packets of closed TCP ports.
- The `ICMP` packets of closed UDP ports.

An IP address is recognized as a scanner when a number of filtered packets is reached:

- Approximately 3 packets for rapid scans.
- Approximately 5 packets for slow scans.

If the IDS is set to **Low**, the agent detects port scans but no action is taken to block the IP address associated with the detected scanner.

Log excerpt indicating that incoming scans are blocked, when the IDS is set to **High**:

```
[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;49154) (TCP;49157) (TCP;34313) (TCP;37792) ( Blocked until
20h06m33s)]ÿ[192.168.42.117]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[777]ÿ[0]
```

Log excerpt when the IDS is set to **Low**:

```
[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.117]ÿ[0]ÿ[0]ÿ
[0]ÿ[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]
```

IDS level	Protection against incoming port scan
Low	Filter
High	∘ Filter ∘ Block
Critical	∘ Filter ∘ Block

Protection against outcoming port scan

⚠ **WARNING**

To use this protection, you must have enabled **Protection against port scan** in **General Settings > Network Activity Control**.

⚠ **WARNING**

The workstation must be restarted if this protection is disabled.

The workstation equipped with the agent is recognized as a scanner when a number of filtered packets is reached:

- Approximately 3 packets for rapid scans.

- Approximately 5 packets for slow scans.

`SCAN_OUT` logs are displayed if the host running the agent acts as a scanner:

```
[PORTSCAN]ÿ[SCAN_OUT]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.1]ÿ[0]ÿ[0]ÿ[0]ÿ
[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]
```

IDS level	Protection against outcoming port scan
Low	Filter
High	∘ Filter
Critical	∘ Filter

Protection against ARP cache poisoning

This protection detects:

- When the host running the agent attempts to steal the identity of another machine on the network.

- When any machine on the network attempts to steal the identity of another machine.

This protection includes:

- An ARP stateful inspection to filter the ARP replies which match no ARP request.

- A protection for gratuitous requests which are sent when the agent detects a machine which has stolen the identity of the agent's host. Gratuitous requests are used to correct entries in the ARP cache of the machines which are not equipped with Stormshield Endpoint Security.

IDS level	Protection against ARP cache poisoning.
Low	Stateful inspection
High	◦ Stateful inspection ◦ Gratuitous ARP blocked
Critical	◦ Stateful inspection ◦ Gratuitous ARP blocked ◦ Protection against identity theft

Log excerpt:

```
[ARP_DELETE 00000005]ÿ[IN]ÿ[Request EthSrc=00:20:20:20:20:20
EthDst=00:16:17:2d:26:99 ArpHwSrc=00:20:20:20:20:20
ArpIpSrc=192.168.42.254 ArpHwDst=00:00:00:00:00:00
ArpIpDst=192.168.42.254]ÿ[192.168.42.254]ÿ[PORTSRC]ÿ[PORTDST]ÿ
[PROTO1]ÿ[PROTO2]ÿ[]ÿ[0]ÿ[61710]
```

	IDS	IPS	
	Protection against flooding	Protection against port scan	Protection against ARP cache poisoning
Low	Disabled	Filter	Stateful inspection
High	Connections are removed when exceeding 20 in number	◦ Filter ◦ Block	◦ Stateful inspection ◦ Gratuitous ARP blocked
Critical	◦ Connections are removed when exceeding 10 in number ◦ Source IP address is blocked	◦ Filter ◦ Block	◦ Stateful inspection ◦ Gratuitous ARP blocked ◦ Protection against identity theft

- **TCP stateful integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 793.

- **ICMP stateful integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 792.

- **Integrity check of Ethernet frames**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 894.

- **IPv4 integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 791.

- **TCP integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 793.

- **UDP integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

It verifies compliance with protocol RFC 768.

- **ICMP integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 792.

- **Protection against fragmented headers**:

  This parameter can be set to **Enabled** or **Disabled**.

  It protects against network attacks using header fragmentation as a way to bypass network firewall filtering rules.

- **Protection against port scan**:

  This parameter can be set to **Enabled** or **Disabled**.

  It blocks incoming packets from the source address if a port scan is detected.

- **IPv6 communications:**

  This parameter can be set to **Enabled** or **Denied**.

  Allows or denies all IPv6 communications.

  It is only supported from Microsoft Windows 7 onwards. It is not supported in Windows Server 2003 and Windows XP.

- **Compatibility with local network proxies:**

  This parameter can be set to **Enabled** or **Disabled**.

  Saves outgoing UDP sessions on the CONNECT instead of IPPACKET layer, allowing it to be compatible with local network proxies.

  It is only supported from Microsoft Windows 7 onwards. It is not supported in Windows Server 2003 and Windows XP.

WiFi Encryption and Authentication

WiFi Encryption and Authentication can be set to **Allowed** or **Denied**.

WiFi Encryption and Authentication parameters are the following:

- **WiFi connections**:

  This parameter enables or disables the use of WiFi connections. The network interface remains active but communications are blocked.

- **WiFi adhoc connections:**

This parameter allows or denies the use of WiFi adhoc connections. This type of connection requires no base workstation and is limited to the duration of the session.

- **Open authentication mode**:

When set to Allowed, no checks are performed during IEEE 802.11 OpenSystem authentication.

- **WEP authentication mode**:

When set to Allowed, this mode uses specified IEEE 802.11 Shared Key authentication. This mode requires the use of a pre-shared *Wired Equivalent Privacy* (WEP) key for 802.11 authentication.

- **Open or WEP authentication mode**:

When set to Allowed, this mode enables auto-switch mode. When using autoswitch mode, the device tries to use IEEE 802.11 *Shared Key* authentication. If Shared Key authentication fails, the device tries to use IEEE 802.11 OpenSystem authentication.

- **WPA authentication mode**:

When set to Allowed, this mode enables the use of WPA version 1 *Security for Infrastructure* mode. Authentication is performed between the supplicant, authenticator and authentication servers via IEEE 802.1X.

Encryption keys are dynamic and derived through the authentication process. While in authentication mode, the device will only associate with an access point whose beacon or probe response contains an (802.1X) authentication suite of type 1 within the WPA information element.

- **WPA (PSK) authentication mode**:

When set to Allowed, this mode enables the use of WPA version 1 *Security for Infrastructure* mode. Authentication is performed between the supplicant, authenticator and authentication servers via IEEE 802.1X.

Encryption keys are dynamic and derived through a pre-shared key used both by the supplicant and the authenticator.

In this mode, the device only associates with an access point whose beacon or probe response contains the authentication suite of type 2 (pre-shared key) within the WPA information element.

- **WPA (ADHOC) authentication mode**:

When set to Allowed, this mode enables the use of WPA version 1 *Security for adhoc* mode. This setting specifies the use of a pre-shared key without IEEE 802.1X authentication. Encryption keys are static and derived through the pre-shared key. This mode is no longer supported by Windows. It remains for the compatibility with old access points.

- **WPA2 authentication mode**:

When set to Allowed, this mode enables the use of WPA version 2 *Security for Infrastructure* mode. Authentication is performed between the supplicant, authenticator and the authentication server via IEEE 802.1X.

Encryption keys are dynamic and derived through the authentication process.

In this mode, the device only associates with an access point whose beacon or probe response contains the authentication suite of type 1 (802.1X) within the RSN information element.

- **WPA2 (PSK) authentication mode**:

When set to Allowed, this mode enables the use of WPA version 2 Security for Infrastructure mode. Authentication is made between the supplicant and the authenticator via IEEE 802.1X.

Encryption keys are dynamic and derived through a pre-shared key used both by the supplicant and the authenticator.

In this mode, the device only associates with an access point whose beacon or probe response contains the authentication suite of type 2 (pre-shared key) within the RSN information element.

- **Other authentication modes**:

  When set to Allowed, this mode enables the use of other authentication modes not mentioned above.

To read details about the authentication modes correspondence between Stormshield Endpoint Security and the Microsoft Windows operating systems, refer to the appendix WiFi authentication modes.

Network Firewall

Overview

Stormshield Endpoint Security integrates a network firewall that is controlled:

- Statically (by administrator rules).
- Dynamically (by reacting to embedded IDS alerts).

Static network firewall operation is defined by rules.

Dynamic network firewall operation is defined by IDS sensitivity and the seriousness of IDS alerts.

Rules are displayed in a tabular form:

Network Firewall / Base network

#	Status	Action	Direction	Remote IP	Over IP	Stateful
0	☑ Enabled	❌ Block	← Incoming	All	ICMP [1]	☑ On
1	☑ Enabled	❌ Block	← Incoming	All	ICMP [1]	☑ On
2	☑ Enabled	⭕ Accept	→ Outgoing	All	ICMP [1]	☒ Off

⚠️ **WARNING**
Network interfaces in bridge mode on virtual machines are not filtered by the firewall.

⚠️ **WARNING**
Windows 7 firewall is able to block incoming/outgoing connections explicitly authorized in Stormshield Endpoint Security by the administrator.

Attributes

The network rules attributes are the following:

- **#** :

  This attribute is used to define the order in which rules are evaluated so as to avoid conflicts between them.

  The network firewall uses the first rule which matches.

- **Status**:

  This attribute can be set to Enabled or Disabled.

A disabled rule is retained in the configuration but not evaluated when processing the network event.

The **Enabled** icon is . ✅ .

The **Disabled** icon is . ☒ .

- **Action**:

This attribute blocks or accepts the data flow.

The **Accept** icon is . ✅ .

The **Block** icon is . ❌ .

- **Direction**:

This attribute is used to define whether the data flow is filtered on the way **in** or on the way **out**.

Rules on TCP, ICMP and UDP traffic are stateful. This means that only the direction of the first packet needs to be defined. A rule to allow response data to flow will be dynamically generated by the firewall. In other cases (non-stateful), the administrator needs to define two rules: one rule for the way in and one rule for the way out.

- **Remote IP**:

This attribute is used to restrict the data flow's destination address.

This address can be:

  ◦ An IP address.
  ◦ An IP address list.
  ◦ An IP address range.

By default, no host is specified. This means that the rule applies to all addresses.

- **Over IP**:

This attribute defines to which IP protocol the rule is applied.

- **Stateful**:

This attribute activates/deactivates the stateful processing of TCP, UDP or ICMP flows.

Stateful rules retain the communication session status while the firewall automatically generates the rule required by the response data flow.

- **Local Port:**

This attribute defines the local host service port number (for TCP and UDP) or the local code (for ICMP).

The administrator can define:

  ◦ A port number.
  ◦ A port list.
  ◦ A port range.

- **Remote Port:**

This attribute defines the remote host port number (for TCP and UDP) or code (ICMP).

The administrator can define:

  ◦ A port number.
  ◦ A port list.

○ A port range.

- **Log**:

  This attribute defines the settings for saving and viewing log files.

- **Description**:

  This attribute is a freeform comment.

- **Group**:

  This attribute shows the group which the rule belongs to. (example: Base Network). This indication is only visible in the root overview mode of each category.

Additional attributes

The administrator has access to additional attributes by clicking [Expand] on the network firewall toolbar. Additional columns are displayed.

The additional rule attributes are the following:

- **Local MAC**:

  This attribute is used to restrict the data flow source address.

  This address can be:

  ○ A MAC address.

  ○ A MAC address list.

  ○ A MAC address range.

  By default, no host is specified. This means that the rule applies to all addresses.

- **Remote MAC**:

  This attribute is used to restrict the data flow's destination address.

  This address can be:

  ○ A MAC address.

  ○ A MAC address list.

  ○ A MAC address range.

  By default, no host is specified. This means that the rule applies to all addresses.

- **Over Ethernet**:

  This attribute defines the protocol over Ethernet to which the rule applies.

- **Local IP**:

  This attribute is used to restrict the data flow source address.

  This address can be an IP address or an IP address list.

  By default, no host is specified. This means that the rule applies to all addresses.

Changing attributes
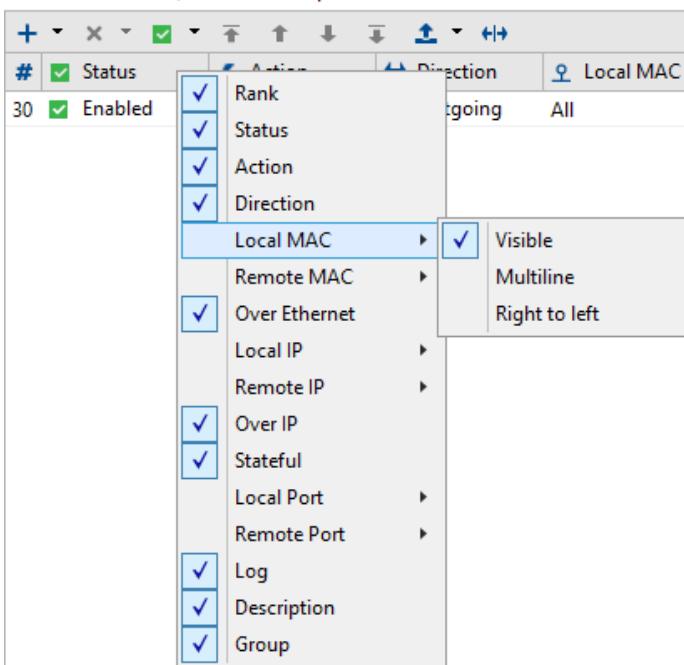
Graphical interface

By default, the network firewall settings are set to **All** and Status is set to **Accept**.

You can select the columns to be displayed by right-clicking any header.

Choose the headers you wish to display from the list.

The way of displaying some attributes can be customized to be read easily. For example select the option multiline to display information on several lines.
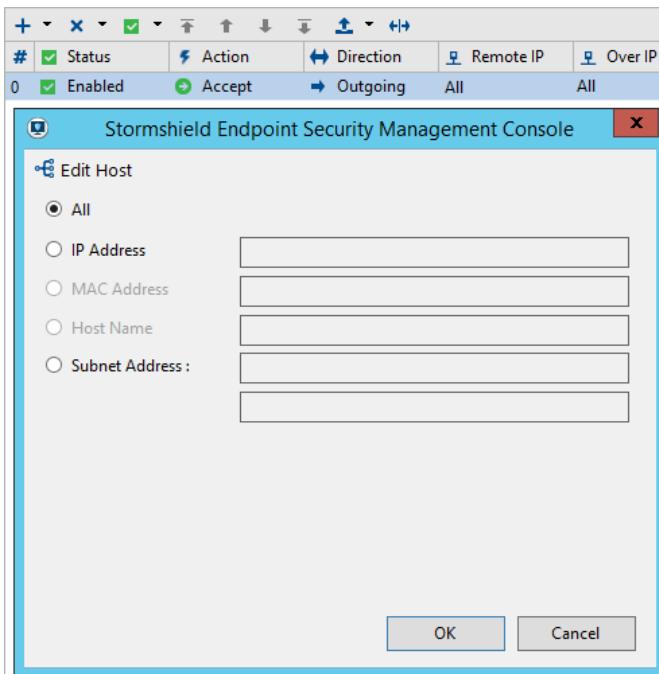
Network Firewall / Default Group

Remote IP
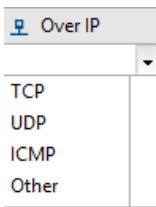
To modify settings, click ⊡ to display the following window and proceed with modifications:
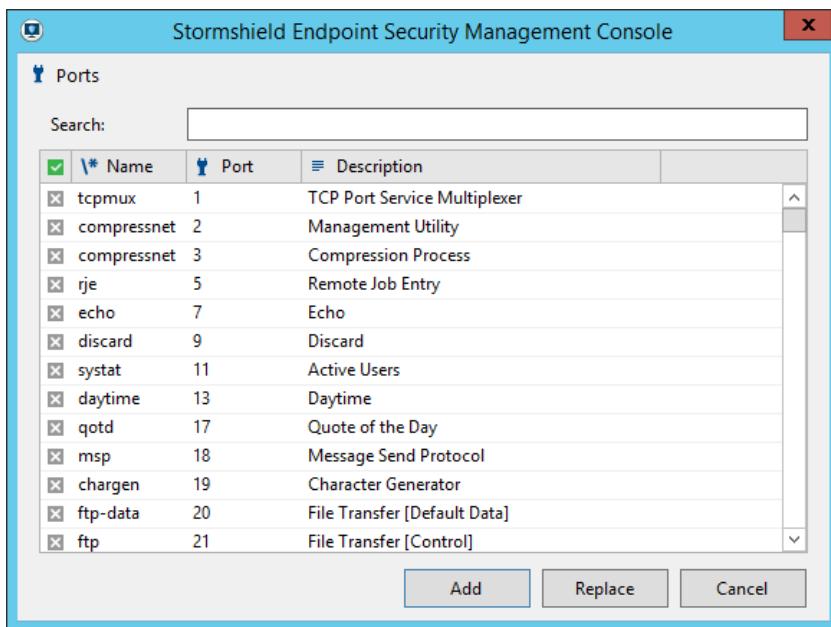
Over IP

To modify settings, click ⊡ to display the following window and proceed with modifications:

<u>Local Port</u>

To modify **TCP** and **UDP** settings, click ⊡ to display the following window and proceed with modifications:
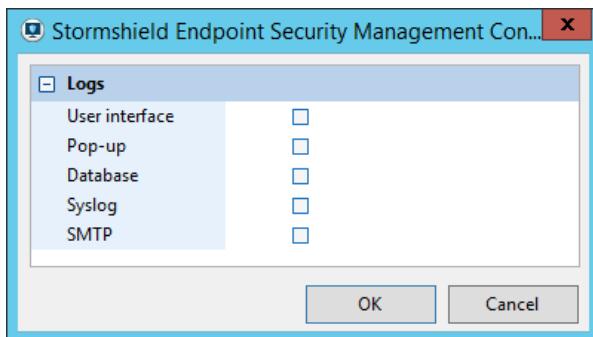
1. Select the required services by clicking in the check boxes.

2. Enter the characters in the **Search** field to reduce scrolling through the list.

3. Click **Add** after making your selection.

To modify **IMCP** settings, click ⊡ to display the following window and proceed with modifications:

Log
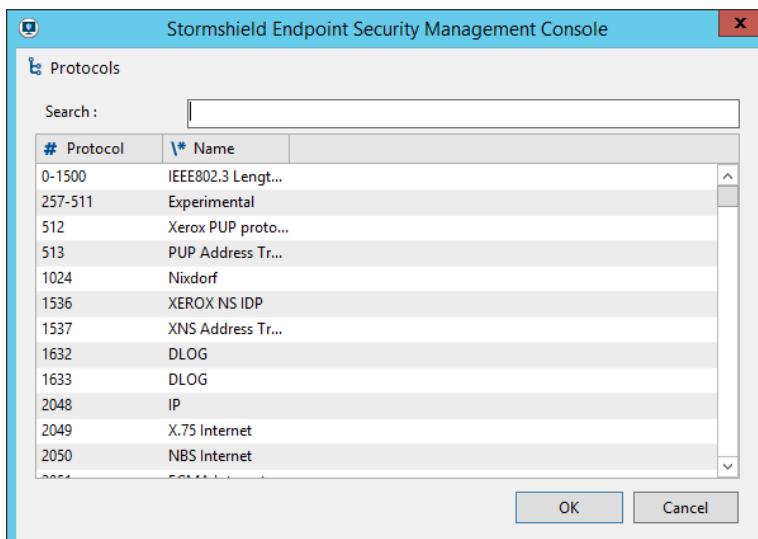
To modify settings, click ⊡ to display the following window and proceed with modifications:

Local MAC
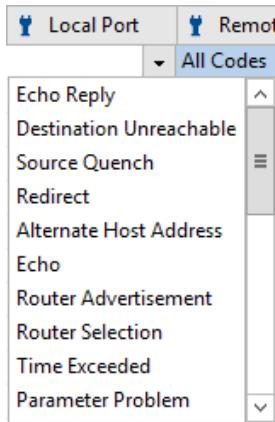
To modify settings, click ⊡ to display the following window and proceed with modifications:

Over Ethernet

To modify default settings, click ⊡ to display the following window and proceed with modifications:

1. Enter the characters in the **Search** field to reduce scrolling through the list.

2. Select the appropriate protocol.

3. Click on **OK**.

WiFi Access Points

Overview

The WiFi Access Points rules allow you to accept or block WiFi access points:

#	Status	Action	SSID	MAC Address	Log	Description	Group
0	Enabled	Accept	myssid	All	____	Company	Default Group
1	Enabled	Block	*	All	F___	Other	Default Group

> ℹ️ **NOTE**
> Blocked actions on WiFi Access Points are recorded into Device Logs.

WiFi Access Points rules define a **whitelist** of authorized access points to which workstations protected by Stormshield Endpoint Security can connect.

To create a whitelist, you must create or modify a policy so that it includes the following:

1. In **General Settings** > **WiFi Encryption and Authentication**, set **WiFi connections** to **Allowed**. Select the appropriate **WiFi Access Points** rules with allowed **SSID** names and set **Action** to **Accept**.

2. Add a final **WiFi Access Points** rule with **SSID** set to ***** and **Action** set to **Block** at the bottom of the list.

> ⚠️ **WARNING**
> WiFi Access Points rules must be ordered so that:
> - Rules with **Action** set to **Accept** are listed first.
> - A final rule with **Action** set to **Block** and **SSID** set to ***** is placed at the bottom of the list.

Attributes

The WiFi Access Points attributes are the following:

- **Status**:

  This is the rule status.

- **Action**:

  This option can assume the following values: Accept or Block.

- **SSID**:

  This stands for the Service Set IDentifier.

- **MAC address**:

  This is the MAC address of the access point.

- **Log**:

  This attribute defines the settings for saving and viewing log files.

- **Description**:

  This attribute is a freeform comment.

- **Group**:

  This is the group to which the rule applies.

Toolbar

The following toolbar is used to:

- Add
- Import
- Delete
- Change the status of several rules at a time
- Set the rule priority order
- Export

9.5.4 Application control

The *Application control* tab contains three types of rules:

- applicative rules.
- extension rules.
- trusted rules.

Application control relies on the concept of application identifiers. Before creating an applicative rule, an identifier must first be created corresponding to the target to which the rule must apply. The first step in generating an applicative rule is therefore to create at least an identifier in the **App identifier** panel of the security policy. Refer to the section **Application identifiers** for help on how to create identifiers.

General settings

Applicative rules operate in two ways: blacklisting and whitelisting.

The **Default behavior** option under **General Settings** allows selecting an operating mode.

- Prevent execution (whitelisting)
  The agent prevents the execution of all applications by default. The execution of
  applications may be allowed in two ways:

  ○ By adding the application to be authorized to the list of **Trusted applications** and
    selecting **Execution control**;

  ○ By adding an applicative rule that identifies the application to be authorized with the
    Execution attribute set to "Enabled".

  Warning: this operating mode may make the machine unstable if the list of authorized
  processes is not exhaustive - certain critical processes or services may be unable to
  execute and cause critical operating flaws.
  To facilitate the implementation of this operating mode, templates have been provided in
  order to allow the operating system's essential processes to start up, provided that
  Microsoft has digitally signed these binary files.
  Each template embeds the list of paths for trusted processes as well as the certificates
  containing the public key of the signatures expected for each process. These authorized
  processes are listed in the section White list.

  To update these templates:

  - contact the Stormshield Endpoint Security technical support to get an update file
    (*Templates.scwt*) or download it in your MyStormshield client area.

  - open the menu **Tools** > **Update whitelisting templates** and select the provided file. It is in
    the *Templates* directory of the SES administration console by default.

  Windows extension components that are not essential to the system loading process, such
  as Internet Explorer or Microsoft Paint, will not be allowed to execute.
  All templates are enabled by default. However, each template may be disabled individually.
  This involves reproducing equivalent behavior in the Trusted applications and Applicative
  rules in order to allow the relevant operating system to run properly.
  Note: For certain system processes that execute very early in the Windows startup phase,
  identification via certificate may fail. A mechanism allows subsequently checking that:

  ○ processes that had been executed during this critical period were legitimately executed
    (in compliance with the rules of the current security policy). If this is not the case, a
    specific log will be recorded (see System logs): [INVALID-EXECUTE]] ;

  ○ processes that had been blocked during this critical period were legitimately blocked (in
    compliance with the rules of the current security policy). If this is not the case, a specific
    log will be recorded (see System logs): [INVALID-BLKEXECUTE]].

  Logs of this type must warrant an update of rules. This technical limitation does not affect
  path or hash identification. The offending hash-based or path-based applications therefore
  need to be identified.
  Applications that have been blocked by the whitelist will be shown in the agent's logs. If a
  problem occurs, they must be checked directly on the agent or by monitoring the
  management console and the identifiers and the necessary corresponding rules must be
  created.

- Allow execution (blacklisting)
  The agent does not deny any access by default and as a result, allows the execution of all
  applications. For applications listed in the security policy, the applicative rule associated
  with them will then apply with its own restrictions and authorizations.

  ℹ️ **NOTE**
  In this operating mode, a combined whitelist/blacklist mode can be created with the
  appropriate rules.

The second option under **General Settings** makes it possible to **Force detailed logs**. By default, the agent calculates the hash and signature information of processes only when necessary as this has an impact on performance and the logs generated. Therefore:

- When the policy makes no reference to any hashes or certificates, the agent will then leave out the calculation of processes' hashes and certificates. In this case, performance will be optimal, but logs will not contain any hash/certificate information.
- When the policy only refers to hashes, the hashes of each process will then be calculated. In this case, performance will be slightly affected, and logs will contain the hash information of binary files.
- When the policy refers to certificates (with or without hashes), the agent will calculate the hashes and certificates of each process. In this case, the generated logs will be comprehensive.

In the event an administrator requires hash and certificate information in preparation of a switch to whitelist mode for example, and the security policy refers to neither hashes nor digital signatures, the agent can be forced to produce comprehensive logs by enabling the **Force detailed logs** option.

Applicative rules

Attributes

The Applicative rule attributes are the following:

- **Status**:

  This attribute can be set to Enabled, Disabled or Test.

  A disabled rule is retained in the configuration but not evaluated when processing the system event.

  A rule in Test mode enables an administrator to test the behavior of a new rule and to be aware of the impacts before activating the rule and deploying it. The rule is assessed when processing the system event: a log is generated as if the rule was enabled but the rule does not block anything.

  We recommend you to configure the backup of logs in the database or in an external application (Syslog or SMTP) to make the Test mode useful. For more information, refer to **Log Manager** and **Exporting logs to an external system (SMTP or Syslog)**.

- **Identifer**:

  Defines the list of selected identifiers to which the rule must apply.

A rule may have an unlimited number of identifiers. Once an identifier has been linked to an application rule, it cannot be deleted. Its assignment to executed applicative rules must first be removed. You cannot assign the same identifier to several applicative rules.

- **Execution**:

  This attribute allows or denies access to the application.

- **Files**:

  This attribute controls the application rights to access the files:

- **Network**:

  This attribute controls the application's right to access the network.

> ⚠️ **WARNING**
> If the **Firewall State** setting is disabled in the **Network security control** tab of the security policy, these rules will not apply.

- **Registry**:

This attribute controls the application rights to access the registry base.

- **Log**:

This attribute defines the settings for saving and viewing log files.

- **Description**:

This attribute is a freeform comment.

- **Group**:

This attribute shows the group to which the rule belongs.

Toolbar

The following toolbar is used to:

- Add
- Import
- Remove
- Change the status of several rules at a time
- Set the rule priority order
- Export

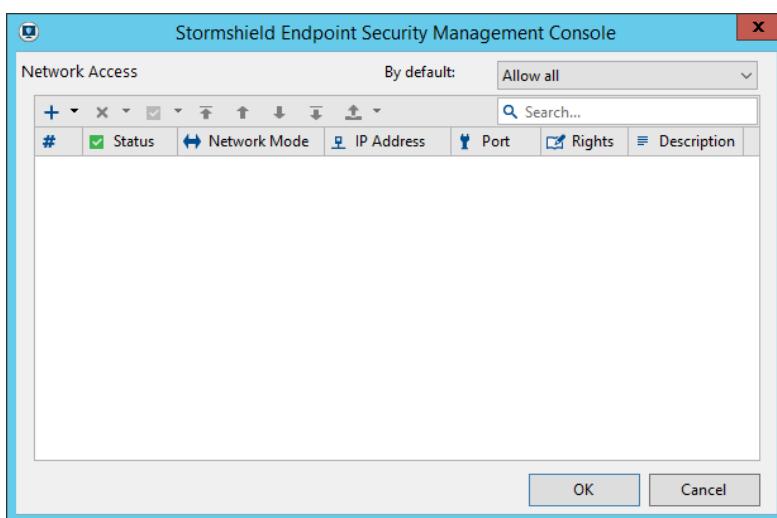The search field is used to reduce scrolling through the list of rules.

Modifying attributes

Graphical interface

All applicative rule attributes are displayed by default. You can customize the attributes to be displayed by right-clicking any column heading. The way of displaying some attributes can be changed to be read easily.

Network

Double-click in the **Network** column to open the Network Access window.

Overall management of access rights to the network

Access rights to an application are managed with an overall or detailed basis.

Overall access privileges are defined in the **By default** field. This field is used to restrict application communication.

Four options are available:

- **Deny Server Only**:

  The application cannot listen to a port. It can only operate in client mode, which means that only the application can initiate a connection to a given service.

- **Deny Client Only**:

  The application can only operate in server mode. It can only respond to connections initiated by client programs.

- **Deny All**:

  The application is not allowed to connect to the network.

- **Allow All**:

  Nothing is blocked by default. The behavior is the one defined by the global security level (High, Low or Critical) and associated rules.

  > **ℹ️ NOTE**
  > Network access control applicative rules involve TCP and UDP.

  > **ℹ️ NOTE**
  > Local sockets are not controlled by network access rules.

Detailed management of access rights to the network

The network access attributes are the following:

- **Status**:

  Possible values are Active, Inactive or Test.

  Just like other items that require activation:

  - an inactive access right is retained in the configuration but not evaluated when processing the system event.
  - the Test mode enables the administrator to try new rights and to test the impacts before putting them into production.

- **Network Mode**:

  Possible values are the following:

  - Client. This mode indicates that the rule applies to outgoing network flow.
  - Server. This mode indicates that the rule applies to incoming network flow.
  - Client and Server.

- **IP address**:

  This attribute is used to restrict the data flow's destination address.

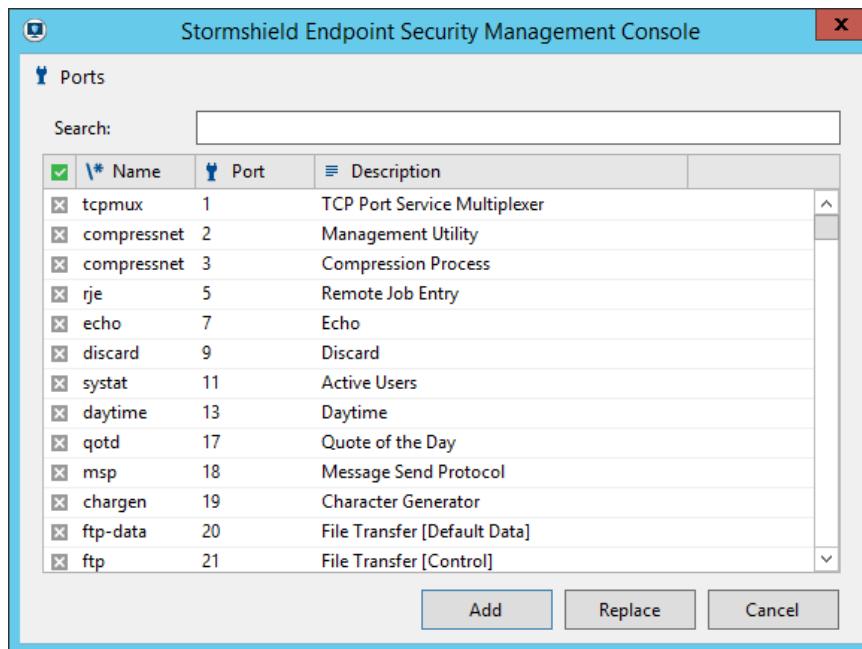 This list of addresses corresponds to:

  - A IP address.
  - A series of addresses (separated by semicolons ";").
  - An IP address range (separated by dashes "-").

- An IP address network in the form of "a.b.c.d/mask".

By default, no address has been specified. It means that the rule applies to all addresses.

- **Port**:

Use the selection button to choose from the list of predefined services. You can define port lists and ranges.

- **Rights**:

This attribute can be set to Allowed or Denied.

- **Description**:

This attribute is a freeform comment to facilitate identification.

Management of access to the network is fully operational on Windows 7 and partially operational on Windows XP:
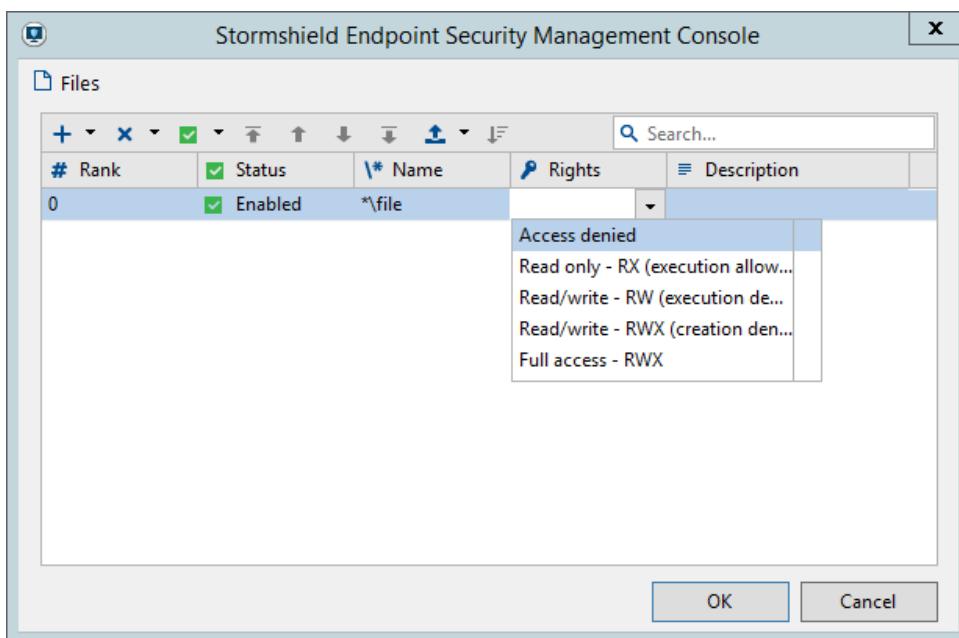
	XP	7 and upper.
TCP client application filtering	✓	✓
UDP client application filtering	✓	✓
TCP server application filtering	Partial (rules with one or several IPs are ignored)	✓
UDP server application filtering	Partial (rules with one or several IPs are ignored) Furthermore, the concept of traffic on UDP is not supported.	✓

ℹ️ **NOTE**
Conflicts may arise if client application filtering rules are applied on UDP server applications in Windows XP. Such applications will then be unable to respond to network packets received.

Files

Double-click the **Files** column to open the Files window:

The file access attributes are the following:

- **Status**:

  Possible values are Active, Inactive or Test.

  Just like other items that require activation:

  - an inactive access right is retained in the configuration but not evaluated when processing the system event.

  - the Test mode enables the administrator to try new rights and to test the impacts before putting them into production.

- **Name**:

  This attribute is the filename which may include one or several * wildcards.

- **Rights**:

  Possible values are the following:

  - Access denied

  - Read only - RX (execution allowed)

  - Read/Write - RW (execution denied)

  - Read/Write - RWX (creation denied)

  - Full access - RWX

- **Description**:

  This attribute is a freeform comment to facilitate identification.

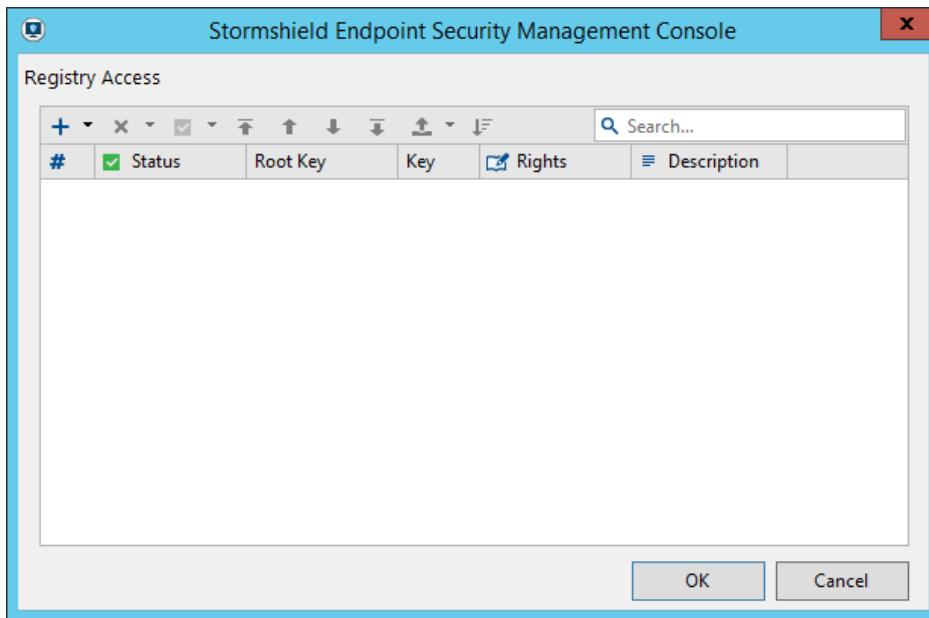The button ![sort icon] allows automatically sorting sub-rules according to the following criteria:

- Full path.

- Full path including environment variables.

- Full path without environment variables, ending with a *.

- Full path including environment variables, ending with a *.

- Path starting with a *.

Registry

<u>Management of access rights to the registry base</u>

Double-click the **Registry** column to open the Registry Access window:

The registry access attributes are the following:

- **Status**:

  Possible values are Active, Inactive or Test.

  Just like other items that require activation:

  ◦ an inactive access right is retained in the configuration but not evaluated when processing the system event.

  ◦ the Test mode enables the administrator to try new rights and to test the impacts before putting them into production.

- **Root Key**:

  Possible values are the following:

  ◦ Local Machine.

  ◦ Users.

  ◦ Current Config.

  ◦ Classes Root.

All Root Keys.

- **Key**:

  This attribute is the name of the key to be specified for registry access.

- **Rights**:

  Possible values are the following:

  ◦ Read Only.

  ◦ Access Denied.

  ◦ Access Allowed.

- **Description**:

This attribute describes the key type used for registry access so as to facilitate identification.

The button ⤓ allows automatically sorting sub-rules according to the length of the key (from the longest to the shortest).

Here are two examples showing how to protect a registry key and its values:

- To prevent from writing and deleting values on the key HKLM\Software\MySoft\MyKey, create a sub-rule with read-only rights on the whole key HKLM\Software\MySoft\MyKey*.
- To block the creation and modification of the registry key HKLM\Software\MySoft\MyKey and its content, create two sub-rules with denied access rights on:
  - HKLM\Software\MySoft\MyKey
  - HKLM\Software\MySoft\MyKey*

  In this example, the sub-rule with denied access rights on HKLM\Software\MySoft\MyKey* also blocks all MyKeyXXX keys.

Extension Rules

Extension rules are used to create a whitelist of extensions and specify the applications that can use them.

For each extension specified, you need to define the applications that are allowed to access this extension. By default, defining a rule for an extension will ban all applications from accessing the corresponding files.

Extension Rules are presented in a tabular form:

#	Status	Extension	Identifier	Log	Description	Group
0	✅ Enabled	WNCRYPT		____	...	WannaCry
1	✅ Enabled	WNRY		____	...	WannaCry
2	✅ Enabled	WCRY		____	...	WannaCry
3	✅ Enabled	WNCRY		____	...	WannaCry
4	✅ Enabled	WNCRYT		____	...	WannaCry
5	✅ Enabled	wab	Outlook	____	Microsoft Outlook Express	Default Group
6	✅ Enabled	pst	Outlook	____	Microsoft Outlook Express	Default Group
7	✅ Enabled	nfs	IBM Lotus Notes	____	IBM Lotus Notes	Default Group

> ℹ️ **NOTE**
> `.srx`, `.sro`, `.sra` or `.srn` files located only in the agent installation directory are protected by Stormshield Endpoint Security: no applications can access them.

The **Extension Rules** attributes are the following:

- **Status**:

  Possible values are Enabled, Disabled or Test.

  Just like other items that require activation:

  - an inactive access right is retained in the configuration but not evaluated when processing the system event.
  - the Test mode enables the administrator to try new rights and to test the impacts before putting them into production.

NOTE
Status has no effect on whether or not the application can access files with an extension specified in the Extension column.
When Status is set to Disabled, the application will not be treated as part of the whitelist until Status is re-enabled.

- **Extension**:

  This attribute defines the extension to which the rule applies. Only the extension is to be entered. There is no need to enter a dot . or a wildcard *.

- **Identifier**:

This is a list of identifiers to which the whitelist feature must apply, meaning the list of applications allowed to access files with this extension type (permission to read, write, run, but not create).

A rule may have an unlimited number of identifiers. Once an identifier has been linked to one or several extensions, it cannot be deleted. Its assignment to executed extensions must first be removed.

WARNING
If no identifiers have been defined, the whitelist feature will not be applied. Thus, no application will be able to access files with the specified extensions.

- **Log**:

  This attribute indicates the log where messages are saved when an application not specified in the whitelist tries to access a file covered by the extension rule.

- **Description**:

  This attribute is a freeform comment.

- **Group**:

  This attribute shows the group to which the rule belongs.

Trusted applications

Defining applications in the Trusted Rules category releases these applications from certain checks so that they can continue to execute actions banned by these checks.

Here are a few examples:

- A remote control application may legitimately use keylogging functions if the **Keylogging** box is checked.

- A debugging tool must be able to attach itself to processes if the **Access to this application** box is checked for the trusted domain.

Attributes

Trusted Rules attributes are displayed in a tabular form:

The **Trusted Rules** attributes are the following:

- **Status**:

  This attribute can be set to Enabled or Disabled.

  A disabled rule is retained in the configuration but not evaluated when processing the system event.

- **Identifer**:

  This is a list of identifiers to which the rule must apply, meaning the list of trusted applications for the specified trusted domain.

  A rule may have an unlimited number of identifiers. The same identifier may be applied to several trusted applications.

  Once an identifier has been linked to one or several trusted applications, it cannot be deleted. Its assignment to the trusted applications that have been run must first be removed.

- **Application scope** (advanced mode):

  This refers to the scope of the trusted rule. A trusted rule applies by default to all application identifiers assigned to the rule, but not to applications that were started via parent applications. If an application starts another application, the trusted domains of the parent application will automatically apply to the latter when you select the **Application and children** option.

- **Rules evaluation** (advanced mode):

  This parameter makes it possible to determine the mode for evaluating trust if the rule in question is applied. By default, the next rule that applies to the same application will be evaluated and applied accordingly. Conversely, if you select **Skip next rules**, as soon as the rule applies, the following rules that apply to the same application will be ignored. Therefore, whenever the application's trusted domains are evaluated, the various rules that apply to the application make it possible to accumulate trusted domains until you reach a rule with specific instructions to skip the next rules, or until the last rule is reached.

- **Trusted domains**:

  This attribute specifies the domains in which the application is trusted.

  The **checked** box means that the application can be trusted in the specified domain. All actions relating to this domain that are normally blocked or indicated by the automatic protections will, in this case, be considered legitimate.

  The **unchecked** box means that the application is not trusted in the assigned domain.

- **Description:**

  This attribute is a freeform comment.

- **Group:**

  This attribute shows the group to which the rule belongs.

  > ⚠️ **WARNING**
  > Two modes are available for this panel: the normal mode and the advanced mode. In normal mode, the **Application scope** and **Access to this application** columns are hidden.

Trusted domains

The trusted domains used are the following:

- **Access to this application**:

  If the box is checked, other applications are allowed to attach themselves to the application.

Applications access:

If the box is checked, the application is allowed to access and attach itself to one or more applications.

- **Execution Control:**

  If the box is checked, the application is allowed to execute any application.

- **Registry**:

  If the box is checked, the application is allowed to access the registry base.

- **Network:**

  If the box is checked, the application is allowed to use sockets.

  > ⚠️ WARNING
  > The level of trust assigned to an application in order to use network sockets does not exempt it from the firewall's rules. However, it will allow the application to bypass applicative rules.

- **Privileges:**

  If the box is checked, the application is allowed to do escalation of privileges.

- **Files:**

  If the box is checked, the application is allowed to access protected files.

- **Keyloggers:**

  If the box is checked, the application is allowed to capture keyboard events.

- **Overflow**:

  If the box is checked, the application is allowed to exceed memory.

  > ℹ️ NOTE
  > Data Execution Prevention (DEP) must be enabled to limit false positives.

- **Reboot:**

  If the box is checked, the application is allowed to reboot the workstation.

- **Exe on removable device:**

  If the box is checked and if the option **Execution control on removable device** in the application behavior control is enabled, the application can start from a removable device connected to an agent without confirmation from the user.

- **Attachment disabled** (advanced mode):

This trusted domain only applies to 64-bit systems and disables many SES security functions. Select the checkbox only to resolve compatibility issues for specific applications.

When the checkbox is selected, SES will not be attached to the application, and the SES protections listed below will stop functioning for the application in question.

The trusted domains correspond to the General Settings of the *System Behavior* tab.

Protections that do not function in the System behavior tab - General settings

- Executable file creation
- Protection against privilege escalation
- Protection against keyloggers
- Protection against memory overflow

- Applications access
- Execution control
- File access

Protections that do not function in the Device control tab

- General settings - Floppy disk drives
- Removable devices - All (only some file controls disabled)

Protections that do not function in the Application control tab

- General settings - Default behavior
- Application rules - Files
- Application rules - Registry
- Extensions - All

Internal protections that do not function

- SES auto-protection is significantly downgraded with regard to applications that use this trusted domain

Handling conflicts between applicative rules

Rule priority order

The order for evaluating rules depends on the rule order defined manually by the administrator, the rule category and its scope of action.

The check sequence for rule categories is the following:

1. Trusted Rules.
2. Applicative Rules (**Execution** column).
3. Extension Rules.
4. Application Rules (**Files**, **Network** and **Registry** columns).

Resolving conflicts

In applicative rules, several rules may apply to the same application. In this case, the order in which rules are checked follows the principles below:

1. Each type of sub-rule (files, registries and network) is independent. The rule engine will examine rules according to the action performed by the user (opening a file, registry key, network access).
2. Sub-rules with an "authorize" privilege will have priority over all others in the definition of privileges on the resource in question, regardless of its rank.
3. Rules are examined by rank. Rules with a lower rank will have priority if several rules identify the same application.
4. Rules that do not have certain types of sub-rules (files, registries and network) will be ignored during the resolution of privileges over such resources.
5. Rules with at least one sub-rule applying to the type of resource accessed will be considered active. As a result, higher ranking rules will not be examined. If the resource (file, registry key, network port) that the application is attempting to access has been indicated in a sub-rule, the specified privileges will be applied. Otherwise, the default privilege will be granted (allowed for files and registries, indicated in the panel for the network).

Examples

Here are four examples showing how applicative rule conflicts are handled.

Example 1

Let us consider the following situation:

- The first applicative rule associated with an identifier containing an entry corresponding to all applications (`*.exe`) does not allow access to text files (`*.txt`).
- The second applicative rule associated with an identifier containing only Windows Notepad (`*\notepad.exe`) allows access to text files (`*.txt`).

In this case, the second rule takes precedence, as its access privilege is "allowed".

Example 2

Let us consider the following situation:

- The first applicative rule associated with an identifier containing an entry corresponding to all applications (`*.exe`) does not allow access to text files (`*.txt`).
- The second applicative rule associated with an identifier containing only Windows Notepad (`*\notepad.exe`) denies access to CSV files (`*.csv`).

In this example, the application `notepad.exe` will not be able to access text files but will have no restrictions on CSV files.

The first rule contains privileges to access files. It will therefore be selected and the other rules will be ignored.

Example 3

Let us consider the following situation:

- The first applicative rule associated with an identifier containing an entry corresponding to all applications (`*.exe`) does not specify any privilege to access files.
- The second applicative rule associated with an identifier containing only Windows Notepad (`*\notepad.exe`) denies access to CSV files (`*.csv`).

In this example, the application `notepad.exe` will not be able to access CSV files.

The first rule does not contain any privileges to access files. It will therefore be ignored and the other rules will be examined. The second rule also identifies `notepad.exe`. Its access rules will therefore be used.

Example 4

Let us consider the following situation:

- The first applicative rule associated with an identifier containing an entry corresponding to all applications (`*.exe`) does not allow access to text files (`*.txt`).
- The second applicative rule associated with an identifier containing only Internet Explorer (`*\iexplore.exe`) explicitly allows Internet Explorer to access the network on certain ports.

The rule relating to Internet Explorer will be applied for network access. There is no conflict as the field of application of the two rules is different:

- The first rule applies to files.
- The second rule applies to network access.

Writing conventions

Application entry format

The full application path can be specified in the **Application** column of each applicative rule. One or several * wildcards can also be used.

Example 1

Here is an example of an application identified by its full path:

```
C:\program files\Internet Explorer\iexplore.exe
```

Example 2

This example shows how to identify an application regardless of the drive where it is located or its access path:

```
*:\program files\Internet Explorer\iexplore.exe
*\iexplore.exe
```

Environment variables

There are four environment variables used to specify rules independently of differences in naming and organization proper to Windows system directories.

These variables are defined using pipe separators (|), at the beginning or end of the string:

|programfiles|

On a 32-bit operating system, this variable matches the directory:

```
c:\program files
```

On a 64-bit operating system, this variable matches the directory:

```
C:\program files (x86)
```

|programfilesnative|

Regardless the architecture of the operating system, this variable matches the directory:

```
C:\program files
```

|systemdrive|

This is the root of the drive where the system is installed. It is usually:

```
C:\
```

|systemroot|

This is the primary directory for operating system files. For Windows XP, it is usually:

```
C:\windows
```

9.6 Applying a security policy to an object of the directory

1. When you have finished editing the security policy, click **Check In**.

2. In the directory tree view, select the object containing the computers on which the policy must be applied.

3. Select the policy in the **Security** part in the *Policies linked* tab.

4. Click **Deploy to the environment**. This action must be performed each time you edit the security policy.

> 🛈 NOTE
> When the agent receives the new security policy, an entry is added in the agent logs.

10. Scripts

10.1 Overview

10.1.1 Scripts feature

The Scripts feature allows creating scripts that control the automatic and autonomous reconfiguration of Stormshield Endpoint Security agents.

Dynamic policy enforcement makes it possible to modify security policies and agent dynamic configuration in real time and enforce workstation conformity.
The latter is highly important before allowing user workstation access the corporate network.

> **NOTE**
> Policies or configurations applied via script take the priority over those assigned in the policies linked tab of a group of agents. You are therefore advised to restore policies or configurations when their application is no longer needed.

10.1.2 Scripts

Scripts are configurable in a script policy. They are created and saved in the **Script** folder in the policies.

Scripts can include the following elements:
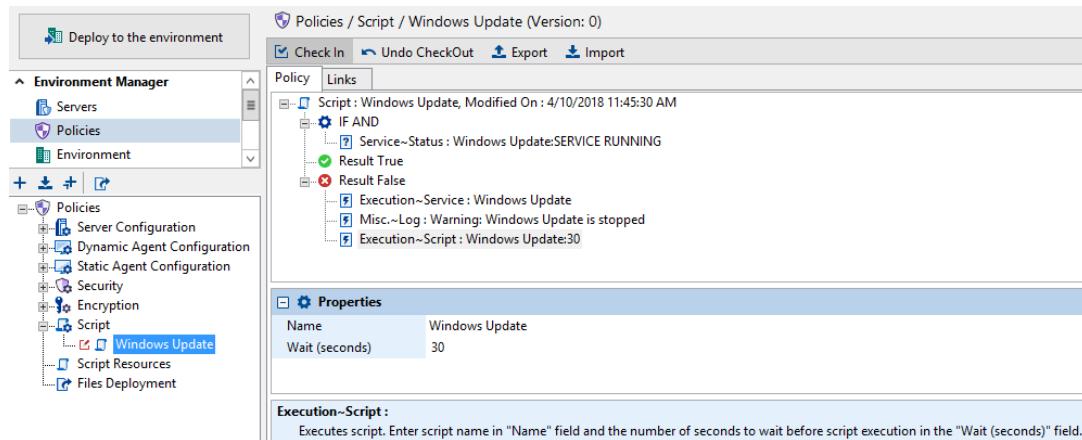
- Tests.

- Actions.

- Boolean logic operators.

- Results.

The Script icon is .

The TRUE result icon is .

The FALSE result icon is .

Here is an example of script based on the verification of the execution of Windows Update service. If the service is not active, it will be relaunched:

The script policy edition window includes the following elements:

- **Work area**:

  This area displays the contents of the selected script. This is where you actually build or edit your scripts.

- **Properties**:

  This area displays the properties associated with a test or an action.

  You can double-click the field next to the property to change it.

- **Message area**:

  This area displays a description of the selected test or action.

  > **NOTE**
  > When creating or modifying scripts, you can move items (examples: statements, built-in tests or user-defined tests) by a simple drag-and drop.

  For more information, see:

- [Tests](#).

- [Actions](#).

- [Scripts](#).

  > **NOTE**
  > This chapter contains a section dedicated to [Transferring files towards the agents](#).
  > It does not belong to the standard script category. These scripts fulfill a specific function upon user's request that is to run scripts on the Stormshield Endpoint Security agents on a temporary basis.

  > **NOTE**
  > SES scripts are run from the SES framework, which is a process which runs within a 32-bit context. Therefore, if you need to access system32 elements in a script (for example: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"), you are advised to replace system32 with the expression "sysnative" in order to maintain the compatibility between 32-bit and 64-bit Windows versions. For example: "C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe".

  These scripts are configured on the management console.

10.1.3 Script Resources

Two types of script resources are available from **Script Resources** under the **Policies** menu in the **Environment Manager** section:

1. Tests.

2. Actions.

Tests

Tests can include the following elements:

- Built-in (or predefined) tests.

- User-defined tests.

- Boolean logic operators.

The test icon is [? Tests] .

Here is an example of test including a built-in test based on a domain user group:

You can add tests by:

- Right-clicking on this area and selecting **Add** from the drop-down menu.

- Clicking directly .

You can also modify existing tests by clicking directly .

For more information, see section Tests.
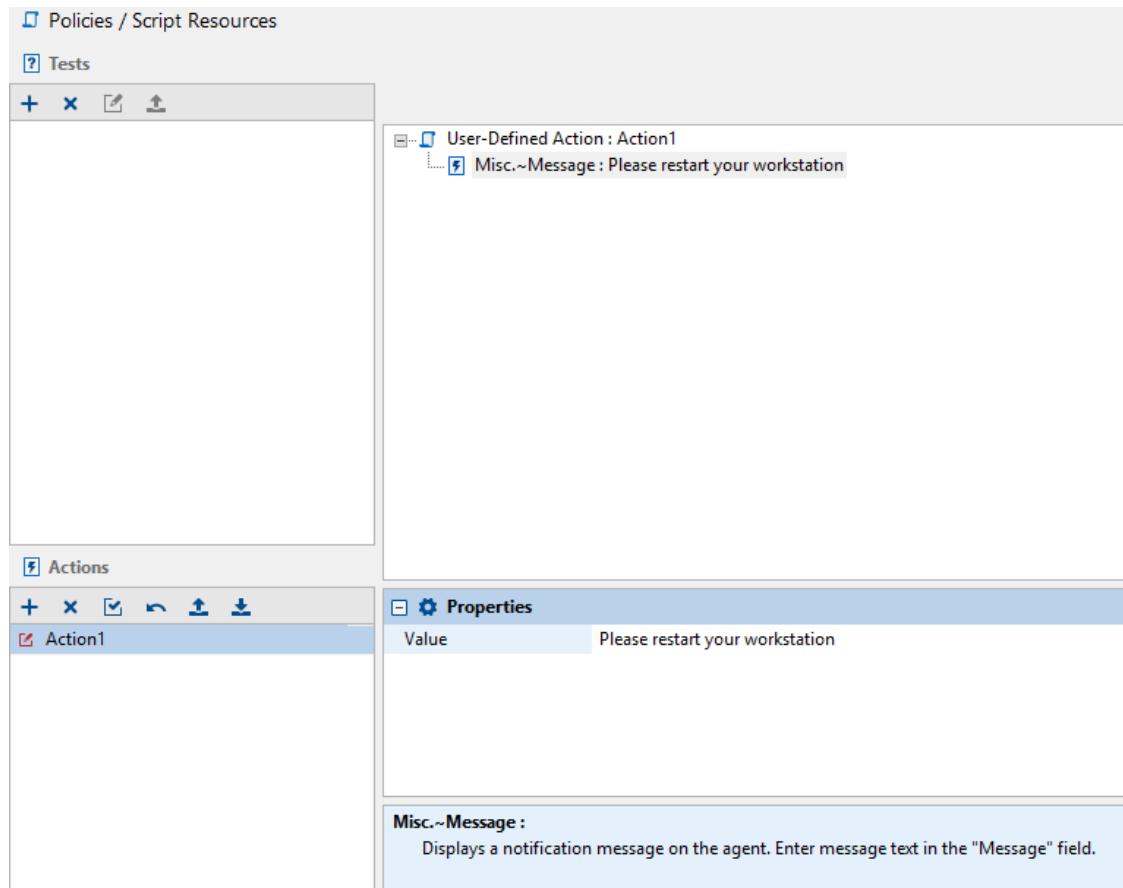
Actions

Actions can include the following elements:

- Built-in actions.

- User-defined actions.

The action icon is . .

Here is an example of action including a user-defined action based on a message display.

You can add actions by:

- Right-clicking on this area and selecting **Add** from the drop-down menu.

- Clicking directly ➕ .

You can also modify existing actions by clicking directly 🖉 .

For more information, see section Actions.

10.2 Tests
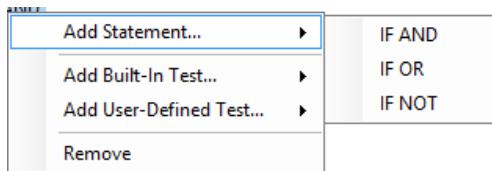
10.2.1 Overview

The test components are the following:

- **Statements**:

  Boolean logic operators (Example: IF AND).

- **Built-in tests**:

  Predefined tests (Example: used to check the execution of a process).

- **User-defined tests**:

  Tests that you or another administrator have previously created.

10.2.2 Statements

Statements use the Boolean logic operators IF AND, IF OR and IF NOT.

Statement definitions

Statements return **TRUE** or **FALSE** values depending on the statement and the test results.

Statement	returns...
IF AND	• TRUE if all tests return TRUE. • FALSE if any test returns FALSE.
IF OR	• TRUE if at least one test returns TRUE. • FALSE if all tests return FALSE.
IF NOT	• TRUE if all tests return FALSE. • FALSE if any test returns TRUE.

Example of tests using logic operators

Following is an example of the components that make up a simple test:

```
IF NOT
 \
 IF AND
 \
```

```
mytest1
|
mytest2
```

- If **mytest1** and **mytest2** both return **TRUE**:
  - ◦ Statement IF AND returns TRUE.
  - ◦ Statement IF NOT returns FALSE.
- If **mytest1** returns **TRUE** and **mytest2** returns **FALSE**:
  - ◦ Statement IF AND returns FALSE.
  - ◦ Statement IF NOT returns TRUE.
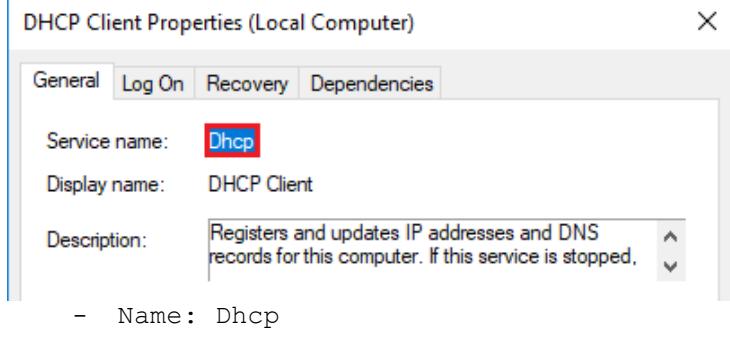
10.2.3 Built-in tests

A built-in test performs common operations and can be run in your own script.

Test	Description	Properties
File > Exist	Checks for named file on agent system. Returns **TRUE** if named file exists. Otherwise, returns **FALSE**.	Enter filename and path: ◦ `Name: c:\programs\acme software\acme software update.exe`
File > Date	Checks the modification date of the named file on agent system to determine its age. Returns **FALSE**: ◦ either if modification date and specified age are greater than or equal to the current date, ◦ or if named file does not exist. Otherwise, returns **TRUE**.	Enter filename and path: ◦ `Name: c:\Programs\antivirus\update.exe` Enter the duration that will be added to the file modification date to define the time basis for the test: ◦ `Time (sec.) : 120`

Test	Description	Properties
File > Size	Checks the size of a specific named file on agent system. Returns **FALSE**: ◦ either if the file size is different from the size specified, ◦ or if named file does not exist. Otherwise, returns **TRUE**.	Enter filename and path. ◦ `Name: c:\test\file.png` Specify the size of the filename in bytes: ◦ `Size (bytes): 20`
File > Content	Checks the content of the named file. Returns **TRUE** if file contains the character string specified. Returns **FALSE**: ◦ either if named file does not exist, ◦ or if the character string is not found, ◦ or if the file size exceeds 5 MB.	Enter filename and path: ◦ `Name: c:\test\file.txt` Define the character string to be searched: ◦ `Content: antivirus test log`
Registry key > Exist	Checks for registry key in registry database. Returns **TRUE** if the registry key exists. Otherwise, returns **FALSE**.	Choose registry path: ◦ `Root Key: HKEY_LOCAL_MACHINE` Enter the registry key path: ◦ `Key: Software\Microsoft Office\11.0` Enable or not the registry redirection. This parameter allows disabling the redirection of the registry to the 32-bit view for 32-bit applications on 64-bit systems. This parameter has no effect on 32-bit systems.

Test	Description	Properties
Registry key > Content	Checks the content of the named registry key in the registry database. Returns **TRUE** if the key contains the character string specified. Otherwise, returns **FALSE**.	Enter registry path: ◦ `Root Key: HKEY_CLASSES_ROOT` ◦ `Key: SYSTEM\CurrentControlSet\Services\TCPip\Parameters` ◦ `Name: [Hostname]` ◦ `Content type: REG_DWORD` ◦ `Content: COMPUTER1` Enable or not the registry redirection. This parameter allows disabling the redirection of the registry to the 32-bit view for 32-bit applications on 64-bit systems. This parameter has no effect on 32-bit systems.
Service > Exist	Checks for a service. Returns **TRUE** if the service exists. Otherwise, returns **FALSE**.	Follow the steps below: ◦ Enter `services.msc` in **Start > Run** or in a command prompt. ◦ Select the appropriate service. ◦ Right-click the service. ◦ Click **Properties** to view the service name. ◦ Conform to writing conventions when entering the service name in the built-in test (see frame): – `Name: Dhcp`
Service > Status	Checks the service status. Returns **TRUE** if the service status matches specified properties. Otherwise, returns **FALSE**.	Enter service name: ◦ `Name: Dhcp` Define the service status: ◦ `Status: SERVICE_RUNNING`
Service > Type	Checks the service type. Returns **TRUE** if the service type matches specified properties. Otherwise, returns **FALSE**.	Enter service name: ◦ `Name: Dhcp` Enter service type: ◦ `Type: SERVICE_AUTO_START`

Test	Description	Properties
Network > IP address	Checks the IP address of the host specified. Returns **TRUE** if the IP address is that configured on the host. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ∘ `IP/Netmask: 172.16.36.21/32`
Network > Default IP address	Checks the default IP address. Returns **TRUE** if the IP address is that configured on the host. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ∘ `IP/Netmask: 172.16.36.21/32`
Network > Default gateway IP address	Checks the default gateway IP address. Returns **TRUE** if the IP address is that configured on the host. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ∘ `IP/Netmask: 172.16.36.254/32`
Network > DNS IP address	Checks the main DNS server IP address that is configured on the host. Returns **TRUE** if the IP address matches the main DNS IP address. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ∘ `IP/Netmask: 172.16.36.254/32`

Test	Description	Properties
Network > Active Network Interface	Checks the network interface specified. Returns **TRUE** if the active network interface matches the one specified. Otherwise, returns **FALSE**.	After clicking in the **Value** field in the **Properties** area, make a selection from the dialog box to display the list of active network interfaces.
Network > Connected to server	Checks that the agent can connect to the Stormshield Endpoint Security server.	
Domain > Domain name	Checks the default domain name. Returns **TRUE** if the domain name on the host matches that of the DNS server. Otherwise, returns **FALSE**.	Enter domain name to be tested: ◦ `Name: domain.com`
Domain > Active Directory User	Checks the Active Directory user in the current interactive session. Returns **TRUE** if the user logged onto the current session corresponds to the one specified. Otherwise, returns **FALSE**.	Enter user Distinguished Name (DN): ◦ `Name: CN=john,OU=Users,DC=stormshield,DC=en` Remark: This built-in test only works in Connected mode.

Test	Description	Properties
Domain > Active Directory Group	Checks that a given user belongs to the Active Directory Group in the current interactive session. Returns **TRUE** if the user logged onto the current interactive session belongs to the group specified. Otherwise, returns **FALSE**.	Enter the domain name in NETBIOS format: ◦ `Domain: STORMSHIELD` Enter the Active Directory group name: ◦ `Name: users` Remark: This built-in test only works in Connected mode.
Process	Checks for a running process. Returns **TRUE** if the process is running. Otherwise, returns **FALSE**.	Enter process name: ◦ `Name: update.exe`
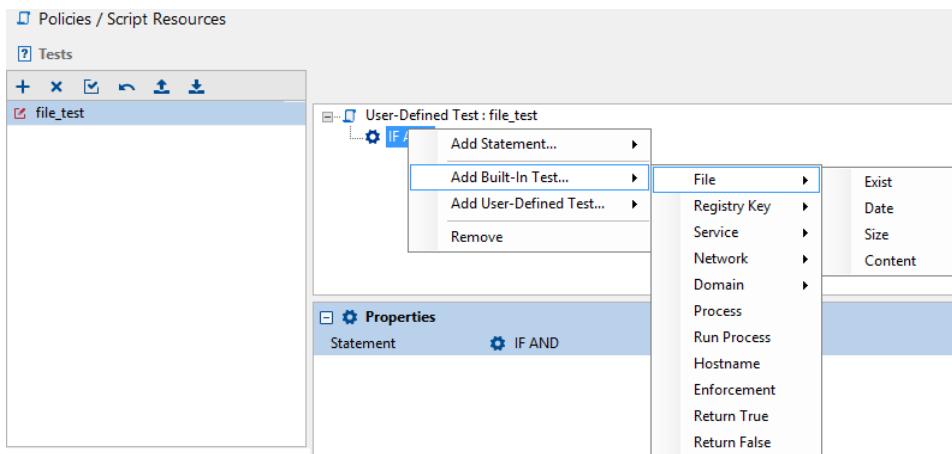
Test	Description	Properties
Run Process	Launches and checks the execution of a process. If **Wait for execution** is set to **TRUE**, the script will wait for the end of process execution before executing another action. If process execution exceeds 10 minutes, the script will be run in parallel. If **Wait for execution** is set to **FALSE**, the script continues in parallel. Returns **TRUE** if process terminates properly. Otherwise, returns **FALSE**.	Enter process name and path: ◦ `Name: c:\program files\antivirus\update.exe` Enable/Disable Wait for execution: ◦ `Wait for execution: False`
Hostname	Checks the hostname. Returns **TRUE** if hostnames correspond. Otherwise, returns **FALSE**.	Enter hostname: ◦ `Name: Computer1`
Recommendation	This action sets a status variable which can be used by TNC clients (Trusted Network Connect) such as Odyssey Access Clients on Juniper Networks (R).	Set **Status** to either of the following options: ◦ Allow, ◦ Isolate, ◦ No access, ◦ No recommendation.
	For more information on Juniper's UAC, see How to install Juniper's "Unified Access Control" module?	
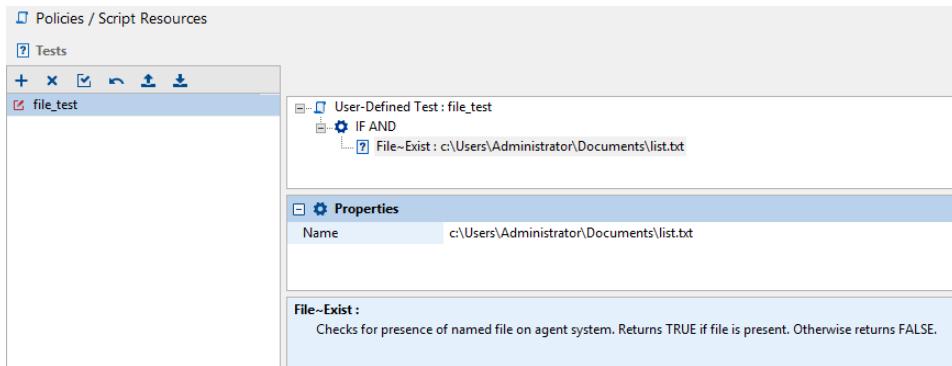
Test	Description	Properties
Return True	Always returns **TRUE**.	
Return False	Always returns **FALSE**.	

Example of built-in test

Here is an example of built-in test (**File > Exist**) that is designed to check for the `list.txt` file on the agent workstation:

You can also specify the file pathname. If the file exists, the test returns TRUE.

10.2.4 User-defined tests
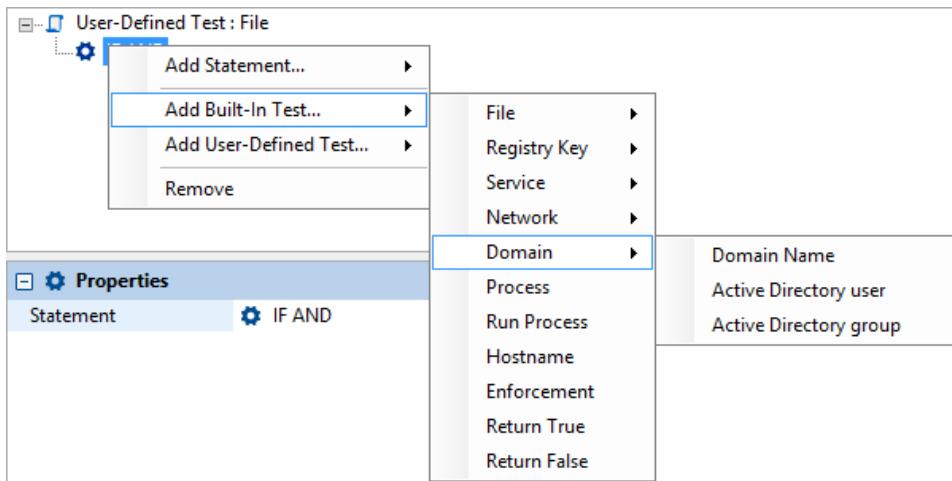
A user-defined test is a test that you or another administrator have created. You can include user-defined tests in scripts and tests.

10.2.5 Creating a test script

To create a test, follow the steps below:

1. In the **Tests** area of the **Script Resources** panel:

   ◦ Right-click in the area.

   ◦ Select **Add** from the drop-down menu or just click the icon ➕ in the toolbar.

   ◦ Name the user-defined test.

2. Right-click the statement **IF AND** displayed by default and click one of the following items:
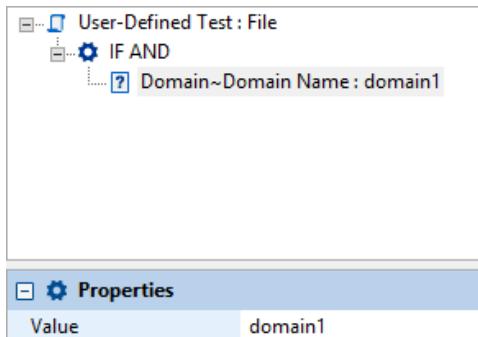
- Add Built-In Test
- Add User-Defined Test.
- Add Statement.

3. When adding a **test,** specify its properties.

    To display and fill in the **Properties** panel:
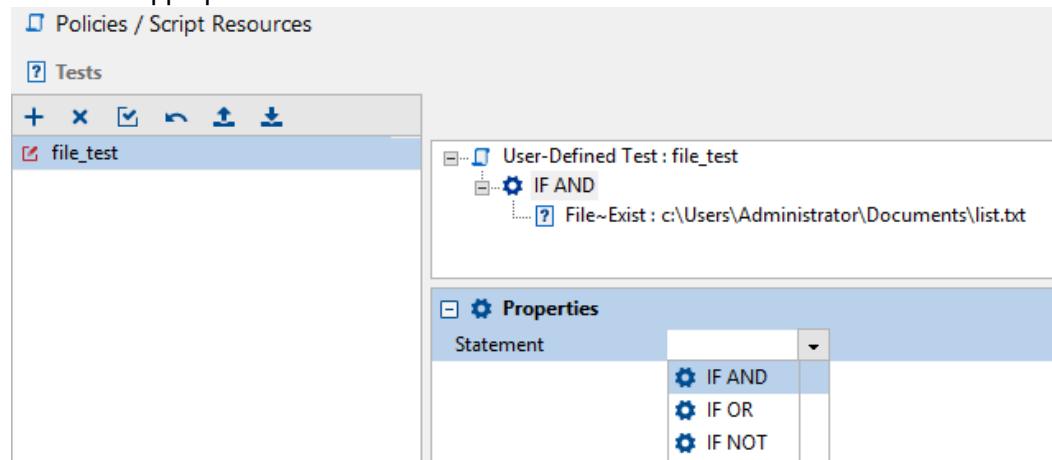
    - Click the newly created test.
    - Fill in the **Value** field to define the domain name.

4. To change the **statement** displayed by default (IF AND) or to add another statement:
    - Click the IF AND statement in the upper panel.
    - Click the statement in the **Properties** panel.
    - Click ⏷ to browse the statement list.
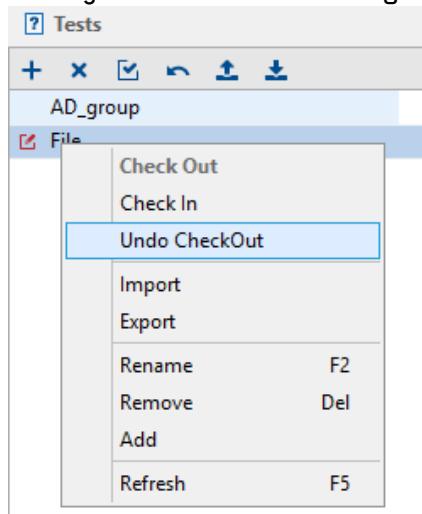
◦ Select the appropriate statement.

> **ℹ NOTE**
> If several tests are included in the test script, you have to enter and/or select required information using ▾ .

5. When you have finished creating the test script, validate by clicking **Check In**.

You can also modify existing actions by clicking directly [✎] .

For more information, see section Built-in tests.

10.3 Actions

10.3.1 Overview

There are two types of action:

- **Built-in actions**:

  These actions are standard actions supplied with Stormshield Endpoint Security .

- **User-defined actions**:

  These actions are the ones that you create or that are created by another administrator.

10.3.2 Built-in actions

A built-in action is a predefined action and performs common operations. You can add numerous built-in actions as part of your scripts.

Test	Description	Properties
Configuration > Apply Policy	Applies a security policy.	Enter a name for the security policy: ° `Name: Policy 1` - The policies applied in this case are temporary. They will be disabled when the agent receives a new configuration from the server or after the workstation restarts. - Furthermore they are applied according to a priority order depending on the script execution source (challenge, action based on the detection of events and then *Policies linked*).
Configuration > Restore previous policy	Restores the previous security policy applied the last time the status of the agent has been checked.	
Configuration > Review policies	Checks the status of the agent and applies a security policy depending on what is set up in the environment.	
Configuration > Apply configuration	Applies a configuration.	Enter a name for the configuration: ° `Name: Warning` - The configurations applied in this case are temporary. They will be disabled when the agent receives a new configuration from the server or after the workstation restarts. - Furthermore they are applied according to a priority order depending on the script execution source (challenge, action based on the detection of events and then *Policies linked*).
Warrning	Restores the configuration applied the last time the status of the agent has been checked.	
Configuration > Review configuration	Checks the status of the agent and applies a configuration depending on what is set up in the environment.	
Execution > Process	Launches applications or processes.	Enter process name and path, and the Wait for execution parameter (if any): ° `Name:` `c:\Programs\antivirus\update.exe` ° `Wait for execution:` - `True:` The rest of the script is not executed until process ends. - `False:` The script is running in background mode. The process is executed with SYSTEM user privileges.

Test	Description	Properties
Execution > Service	Launches a service.	Enter service name: ◦ `Name: wuauserv`
Execution > Script	Launches a script.	Enter script name: ◦ `Name: AntiVirus Check` Enter the number of seconds before launching the script: ◦ `Wait (seconds): 30`
File > Copy	Copies a file.	Enter name and path of the file to copy: ◦ `Name: c:\Account1` Enter name and path of the file copy: ◦ `New name: c:\Account2`
File > Rename	Renames a file.	Enter name and path of the original file: ◦ `Name: c:\Account1` Enter name and path of the new file: ◦ `New name: c:\Account_01`
File > Delete	Deletes a file.	Enter path and filename: ◦ `Name: Account1`
Misc. > Message	Displays a message popup to the user.	Enter the message text to be displayed in the **Value** field. ◦ `Message: You must update your antivirus signature database.`
Misc. > Log	Generates a new INFO log on the agent. This log is displayed in the **Software logs** in the console. The log filename on the agent is `software.sro`.	Enter the log message to be displayed in the **Value** field.
Misc. > Wait	Pauses the script execution.	Enter pause length in seconds.
Network > Disable Network Interface (s)	Disables an agent network interface.	Select how to disable network interfaces: ◦ `Type:` - `Whitelist:` All network interfaces are disabled except those mentioned in the list. This action remains active until the next full review of the scripts on the agent or an explicit call in a script file of the "Flush NIC Restrictions" action. - `Blacklist:` Only the listed network interfaces are disabled. ◦ `Values: network card hash.` To disable all network interfaces in the Whitelist, a value of the type 0:000000000 must be entered. After clicking **Values** in the **Properties** panel, make a select from the dialog box. Network interfaces can be added by the administrator or imported from the database.
Network > Flush NIC Restrictions	Cancels the "Disable network interface" action. Be careful, the network interface is not automatically re-enabled.	

Test	Description	Properties
Recommendation	This action sets a status variable which can be used by TNC clients (Trusted Network Connect) such as Odyssey Access Clients on Juniper Networks (R).	Set **Status** to either of the following options: ◦ Allow, ◦ Isolate, ◦ No access, ◦ No recommendation.
	For more information on Juniper's UAC, see How to install Juniper's "Unified Access Control" module?	
Encryption > Lock Down File	Enables/Disables encrypted file lockdown. When files are locked, no user (even authenticated) will access encrypted files.	
Encryption > Allow Automatic Restart	Enables/Disables automatic restart (without compulsory password entry) for full disk encryption.	

10.3.3 User-defined actions

User-defined actions are actions previously created by an administrator.

You can include user-defined actions in scripts.
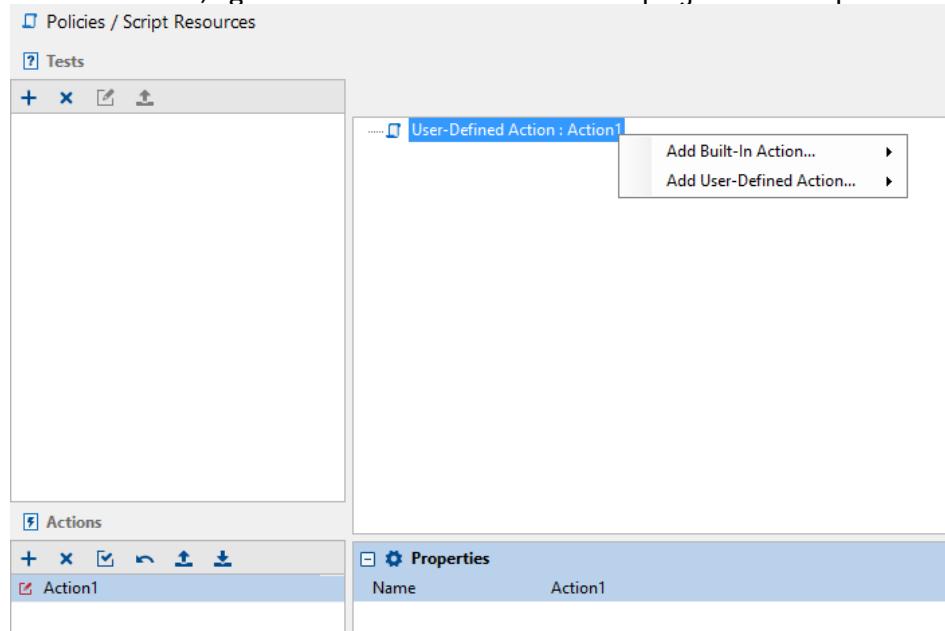
10.3.4 Creating an action

To create an action, follow the steps below:
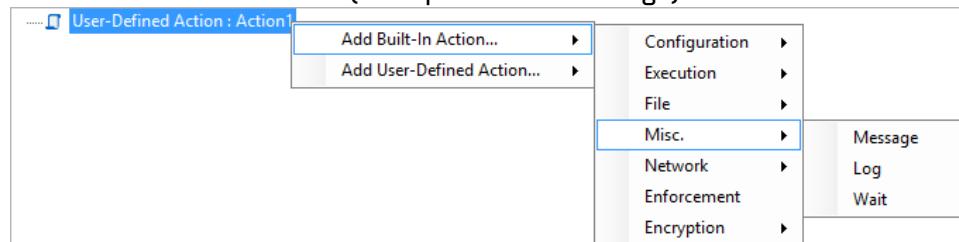
1. In the **Actions** area of the **Script Resources** panel:

   ◦ Right-click in the area and select **Add** from the drop-down menu or just click the icon ➕ in the toolbar.

   ◦ Name the action.

2. In the work area, right-click the Action icon ☑ to display the **Add** drop-down menu.
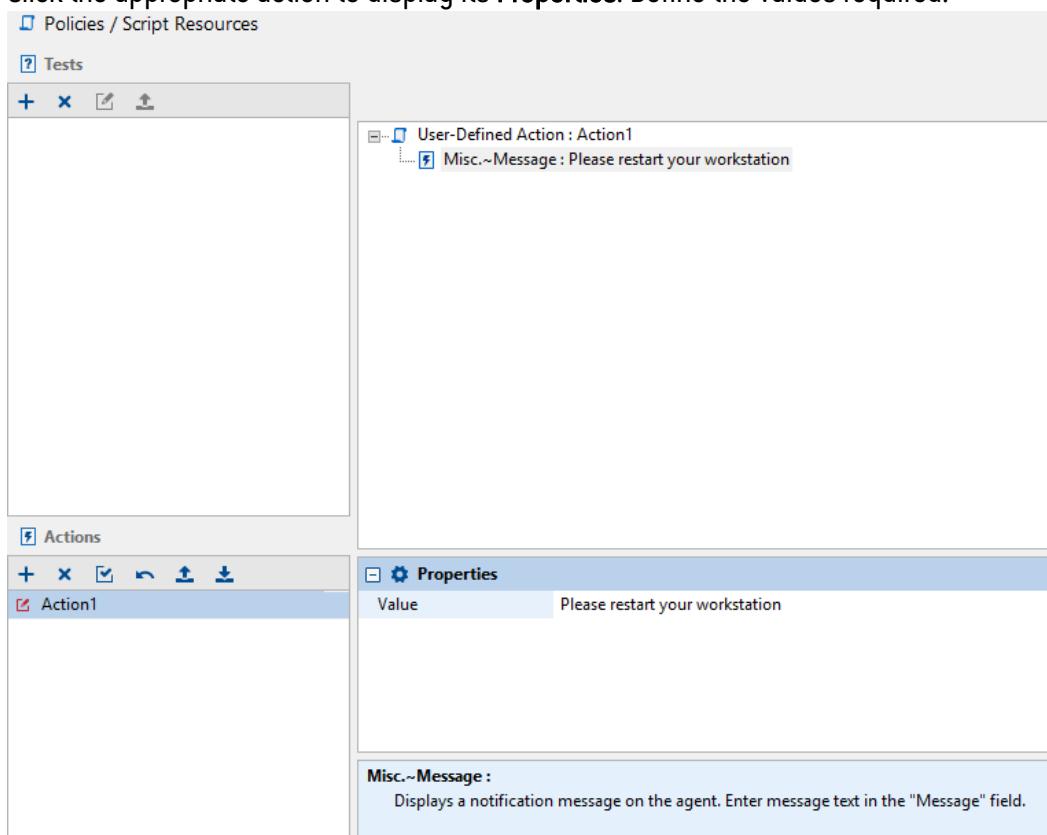
3. To display the first-level actions which are available, select either of the following:

    ◦ **Add Built-In Action**.

    ◦ **Add User-Defined Action**.

4. Select a second-level action (Example: Misc. > Message).
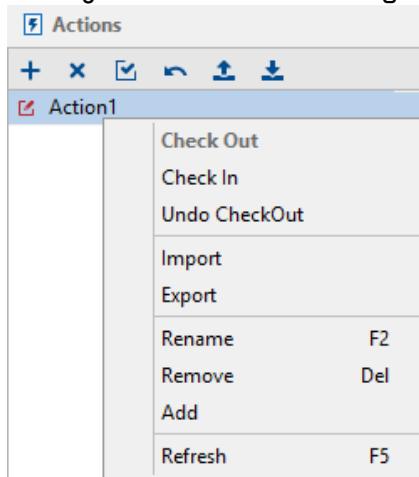
The action is added to the script. You now have to specify its properties.

5. Click the appropriate action to display its **Properties**. Define the values required.

6. When you have finished creating the action script, validate by clicking **Check In**.

You can also modify existing actions by clicking directly ⬚ .

10.4 Scripts

10.4.1 Overview

Scripts enable you to combine tests and actions in order to create more complex and powerful scripts that can be applied to network policies and configurations.

Scripts include the following:

- **Statements**

- **Built-in tests**
- **User-defined tests**
- **Built-in actions**
- **User-defined actions**

10.4.2 True/False results

When you add a new script, the **Result True** and **Result False** settings are automatically added. Add actions under Result True or Result False according to the result returned.

You can create a script to check that any workstation trying to log onto the network has antivirus software. If this is not the case, the script will be configured to refuse network access.

The script contains tests and actions to be executed based on the test results returned.
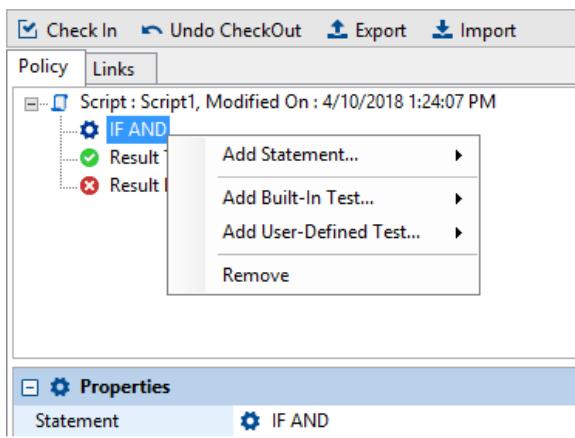
> 🛈 **NOTE**
> The administrator is not allowed to remove a script (test, action or script) used by another script.

10.4.3 Creating and applying a script to an object of the directory

To create a script, follow the steps below:

1. In the **Policies** menu in the **Environment Manager** section, create a new script policy. Name the script policy.

2. In the *Policy* tab, right-click the statement **IF AND** displayed by default and click one of the following items:
   - Add Statement.
   - Add Built-In Test.
   - Add User-Defined Test.

3. To change the **statement** displayed by default (IF AND) or to add another statement:
   - Click the IF AND statement in the upper panel.
   - Click the statement in the **Properties** panel.
   - Click ⬇ to browse the statement list.

Select the appropriate statement.

4. If you have added a **test**, specify its properties.
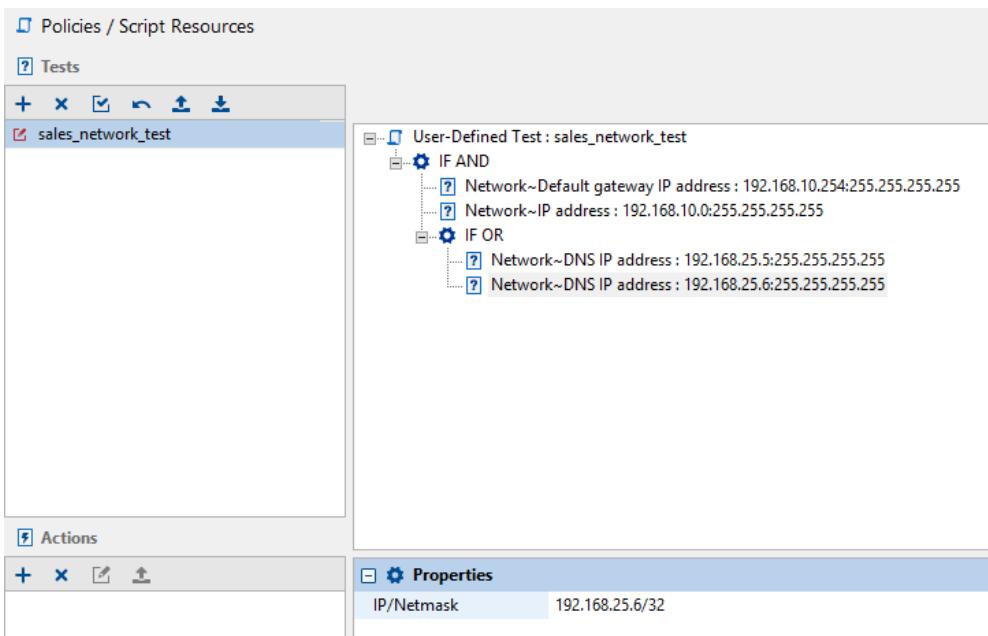
5. Right-click the **Result True** icon ❌ or the **Result False** icon ✅ to display the list of actions to be associated with the result returned.

   Both result icons are generated by default when creating the script.

6. Add required actions, tests and statements to your script.

7. To apply the script to an object of the directory:

   ◦ Select the *Policies linked* tab.

   ◦ In the **Script** part in the *Policies linked* tab, select the script to apply.

   ◦ Select the test to be run so as to apply the policy (`connected`, `disconnected` and `true` are present by default).

8. Click **Deploy to the environment**. This action must be performed each time you edit the script policy.

Example 1

Creating a test to check that a workstation is on the network

To check that a workstation is on the network, follow the steps below:

1. Create a test script called `test_sales_network` to check if the computer is on the network:

   ◦ Add an **IF AND** statement.

   ◦ Add the **Default Gateway IP Address** built-in test.

   ◦ In the Default Gateway IP Address properties, specify:

     - The gateway IP address of the Sales Network.

     - The network IP address.

   ◦ Add an **IF OR** statement.

   ◦ Add a **DNS IP Address** built-in test.

   ◦ Add another **DNS IP Address** built-in test.

   ◦ In the DNS server properties of each DNS server, specify:

     - The DNS IP address.

- The subnet mask.

Example 2
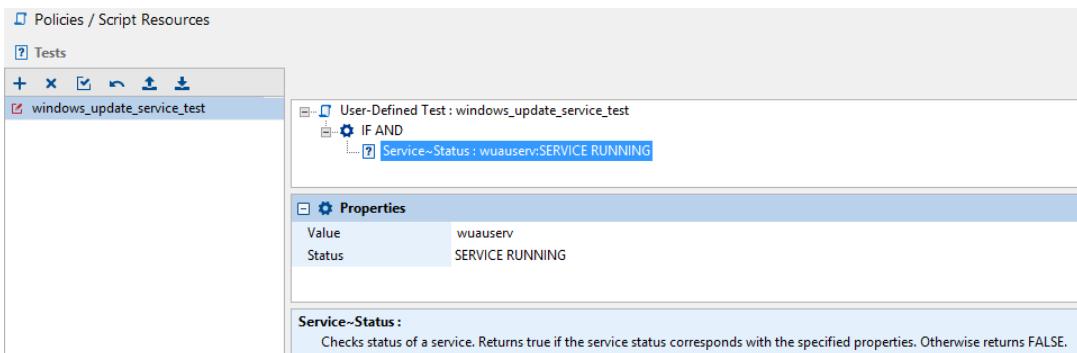
Checking that the Windows Update service is running

Your script should include the case when the service is not running and force Windows Update to restart.
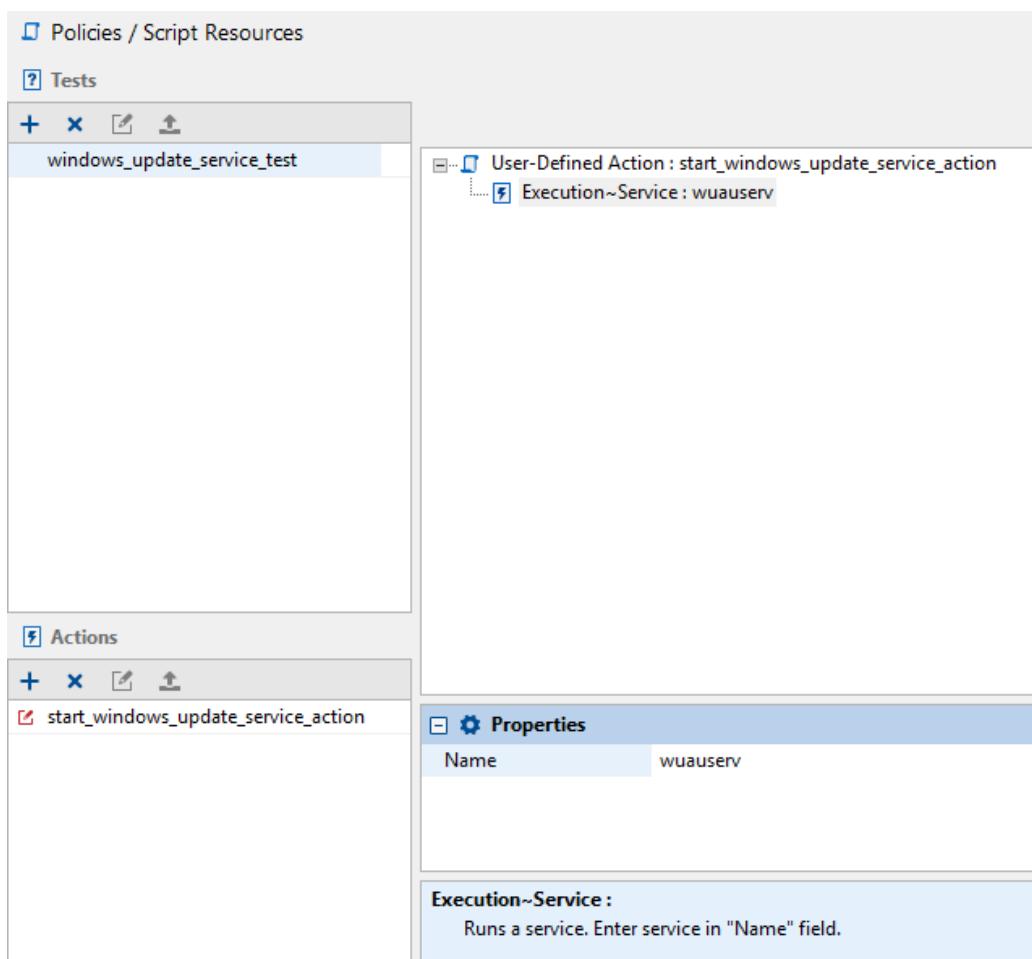
To check that the Windows Update service is running, follow the steps below:

1. Under **Environment Manager > Script Resources > Tests**, define a new test called `test_windows_update_service`.

   ○ Add an **IF AND** statement.

   ○ Within this statement:

     - Add the built-in test `Service (Status)`.

     - Enter the name of the Windows Update service: `wuauserv`.

   The test returns **FALSE** if the service has not started.
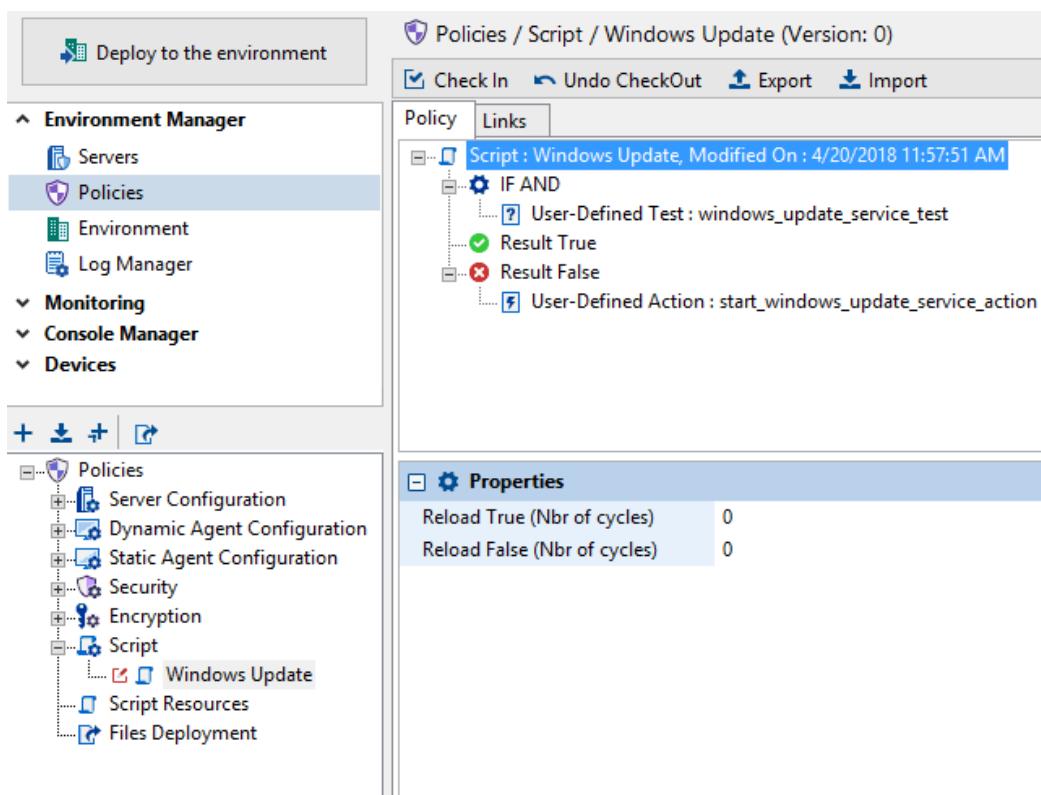
2. Under **Environment Manager > Script Resources > Actions**, define a new action called `action_start_windows_update_service`.

   ○ Add the built-in action **Execution > Service**.

   ○ Enter the name of the Windows Update service: `wuauserv.`
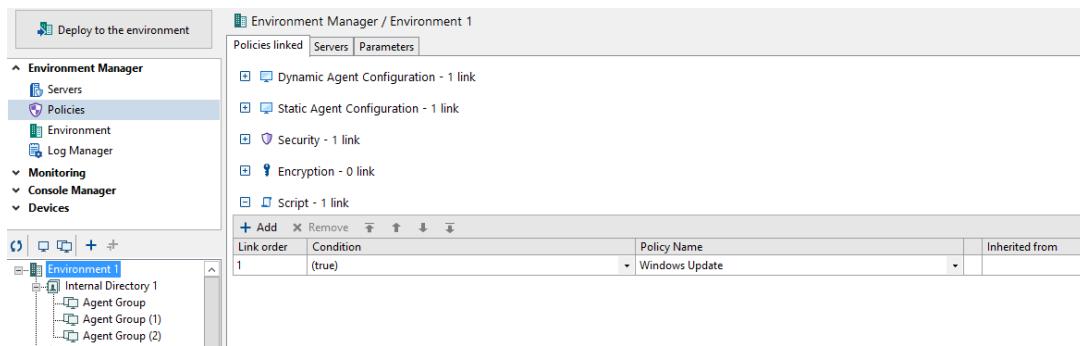
3. Under **Environment Manager > Policies > Scripts**, define a new script:

- Add an **IF AND** statement.

- Within the IF AND statement, add the user-defined test `test_windows_update_ service` that you have created in Step 1.

- In Result False, add the user-defined action `action_start_windows_update_ service` that you have created in Step 2.

4. To associate the script with an object of the directory:

   ◦ Select the object in **Environment Manager**.

   ◦ Select the *Policies linked* tab.

   ◦ In the **Script** part, select the script to apply.

   ◦ Select the test True so as to apply the policy.

10.5 Transferring files towards the agents

10.5.1 Overview

You can use the management console in order to:

• Transfer files from the console.

• Distribute these files to the agents via the servers.

For example, the administrator can upload and distribute a Script file to be applied to the agents.

Up to twenty files can be transferred and deployed on all agents.

Their characteristics are the following:

- The maximum size for the whole set of files to be transfered must not exceed 2MB.

- Transfered files are automatically renamed `name_file.srn` by Stormshield Endpoint Security.

- Files deployed on the agents will be copied in:
  `[Stormshield Agent install dir]\uploaded]`.

The extension of `name_file.srn` files implies that the applications:
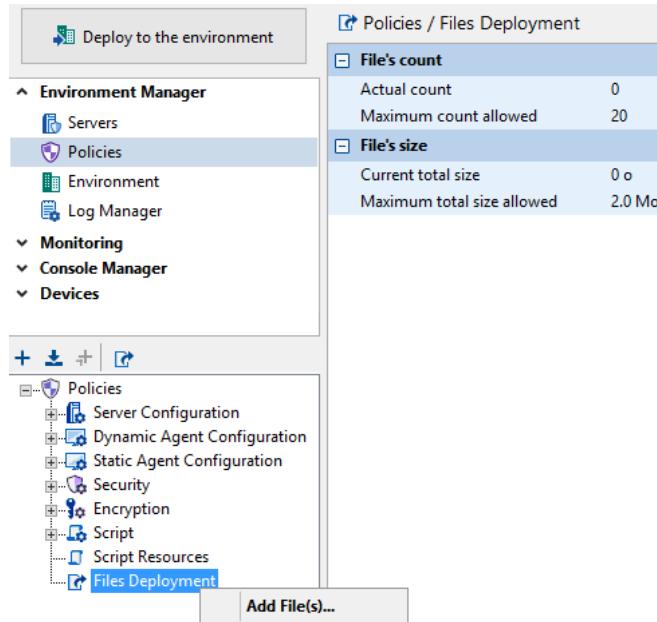
- Which checkbox – in the **Files** column in the **Trusted Rules** in the applicative rules of the security policy – is not checked will be denied access to this protected file.

- Which are not launched by a Stormshield Endpoint Security script will be denied access to this file.

10.5.2 Procedure

To transfer files from the console towards the agents, follow the steps below:

1. In the **Policies** menu under the **Environment Manager** section, right-click on the **Files Deployment** folder or click on .

   The following drop-down menu is displayed:

2. Click **Add File(s)**.

3. Select the file to be transfered. You can select several files by holding down the Ctrl key.

   If a file with the same name has been previously uploaded, an error message is displayed in the status bar.

> **ⓘ NOTE**
> If you try to upload a file exceeding 2 MB, upload will be refused. If the whole set of files exceeds 2 MB, a message displayed in the status bar indicates that you must remove some files before deploying changes to the environment.

4. Click **Deploy to the environment** to send files to the servers so that they are retrieved by the agents at the next connection to the server.

Example

You can deploy a script on agents to make a distinction between desktop and laptop workstations. This script will test the presence of batteries.

> **ⓘ NOTE**
> This test is not supplied with Stormshield Endpoint Security.

The script is written as follows:

- If a battery is detected, the script will return **TRUE** to the agent by sending value "1".
  This value is returned by the **vbscript** function "Wscript.quit(1)".

- Otherwise, the script will return **FALSE** to the agent by sending value "0".
  This value is returned by the **vbscript** function "Wscript.quit(0)".

To use this script in a test or another script, you will use the **Run** function and enter the following information:

```
Cscript.exe /E:vbscript "uploaded\file_name.srn"
```

`/E:vbscript` is used to indicate the file format (`name_file.srn`) if its extension is not `.VBS`.

> **⚠ WARNING**
> The administrator must not use the **Wscript** interpreter.

If the Vbs script allows the use of **arguments**, you will use the **Run** function and declare arguments as shown below:

```
Cscript.exe /E:vbscript "uploaded\file_name.srn" Argument1
```

or `Cscript.exe /E:vbscript "uploaded\file_name.srn" Argument1 Argument2`

11. Removable Device Administration

11.1 Overview

Stormshield Endpoint Security enables to enroll removable devices used on the organization's workstations in order to control them. It ensures the security of the workstation on which the device is connected and facilitates the management of devices.

An enrolled removable device is uniquely identified and configured by the device management tool. It must be associated to a single user who is the owner.

An enrolled device is trusted as long as its content has not been modified out of the perimeter of the organization. It can be used on any workstation of the secured perimeter. If a modification of the content is detected, it is possible to configure an antivirus check on the device to be trusted again.

A control agent installed on each workstation and server of the organization allows access only to enrolled removable devices complying with the controls defined in security policies.

Stormshield Endpoint Security supports all USB 2.0 device drivers. However it supports only 3.0 USB devices using the following drivers:

- usbhub (Microsoft Generic)
- usbhub20
- vusb3hub (Via)
- nusb3hub (Nec Electronics, Renesas Electronics)
- iusb3hub (Intel)
- asmthub3 (AS Media)
- usbhub3 (Microsoft Generic Window 8)
- amdhub30 (AMD)

11.2 Preparation of the removable device enrollment

To enroll removable devices, you must satisfy the following prerequisites:

- a unique identifier, specific to the organization.
- an access to the organization LDAP directory.

The organization identifier is automatically generated when installing Stormshield Endpoint Security. The value of the identifier can be manually modified, for example to reuse the identifier of a previous installation.

By default, the console uses the Active Directory set up for Stormshield Endpoint Security in the case of an environment based on an Active Directory. If the environment is based on an internal directory, Stormshield Endpoint Security automatically detects the LDAP directory to which the workstation belongs. This directory allows to identify the owners of the enrolled keys.

The removable device enrollment parameters are stored in the [db_environment] table of the Stormshield Endpoint Security configuration SQL base.

This table can include the following properties:

Key	Value
enrollment-organizationGuid	The value of this property must be specific to the organization. The identifier format is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx where x is a hexadecimal digit. It is initialized during the installation with a random value. This value can also be manually modified. In this case, follow the steps below for the identifier to be taken into account in your environment. 1. After having modified the value of the identifier, close and open all running instances of the management console. 2. Click **Deploy to the environment** to take the new parameter into account.
enrollment-LdapGuidAttribute	This property contains the name of the LDAP attribute including users GUID. The default value is `objectguid`. On other LDAP directories, it can be `entryuuid`.
enrollment-LdapBaseDN	This property defines the branch of the directory from which users are searched for. By default, it is the Active Directory root.
enrollment-LdapServer	This property contains the address and the port of the LDAP server. The current Active Directory is used by default.
enrollment-LdapUser	Login used to authenticate and search for users in the directory. This property can be empty when an anonymous or LDAP connection is used.
enrollment-LdapPwd	This property contains the connection password to the directory.
enrollment-LdapAuthType	The possible values of this property are `Anonymous` for an anonymous connection, `Basic` or `Digest` for a classic LDAP directory, and `Negotiate` for an Active Directory.
enrollment-LdapUserFilter	This property contains the LDAP filter listing the directory users. The default filter corresponds to the active users of the Active Directory: `(&(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(objectcategory=person))` For a classic LDAP directory, the filter can be `(objectclass=inetorgperson)`.
enrollment-LdapAutoCompleteFilter	LDAP filter used when automatically completing the name of a user. The default value is `(cn={0}*)`. The attribute used as users RDN must be used. This filter can be replaced by `(uid={0}*)` for example.
enrollment-LdapAdministratorFilter	This property contains the LDAP filter enabling to find the LDAP account of the administrator connected to the console from his/her Stormshield Endpoint Security identifier. The default value is `(&(userprincipalname={0}@*)(objectcategory=person))`. We recommend naming Stormshield Endpoint Security users with the same name as their account in the directory. On some LDAP directories, the value can be `(&(uid={0})(objectclass=inetorgperson))`.
enrollment-LdapSearchUserFilter	This property contains the LDAP filter used by the console for the advanced search of names. It can be applied to all attributes containing a part of the name of the searched user. The default value is `(l(cn=*{0}*)(displayname=*{0}*)(mail=*{0}*))`.

Key	Value
enrollment-LdapSearchDepartmentFilter	This property is used as LDAP filter by the console for the advanced search of names. It can be applied to all attributes containing a part of the service or the site of the searched user. The default value is `(l(ou=*{0}*)(department=*{0}*)(l=*{0}*))`.

To modify these properties, you must edit the [db_properties] table of the configuration SQL base thanks to an SQL Server client such as `sqlcmd` or SQL Management Studio.

11.3 Delegation of the removable device administration

11.3.1 Overview

If a security policy applies to several devices, it can be tedious to add new devices. You need to deploy a new configuration when modifying the list of devices.

In order to simplify these scenarios, the rules of the security policy rely on the enrollment status of the device. The status is one of the rule configuration settings.

The console enables to assign a status to a device. Agent configuration does not depend on the device status. The advantages are the following:

- Stormshield Endpoint Security administrators having access to the enrollment management features do not have to be the same as administrators able to modify agent configuration.

  The number of enrollment administrators can be much higher than the number of agent administrators.

- The status of a device can change over time. A device is considered as trusted if it is used only on the organization network. It can lose this status if it is modified on a workstation out of the network.

- The owner is known when enrolling the device. Logs generated by the agent mention the name of the owner.

To use this enrollment feature, the installation of Stormshield Endpoint Security may need to be customized as described in section Preparation of the removable device enrollment.

The device administration delegation features are detailed in the following sections.

11.3.2 Device administration permissions

The device administration is divided into two features. Each one is controlled by a specific permission in the roles management window.

The permission **View enrolled devices** is compulsory for all devices administrators. It enables to consult the current enrollment status of a device, to find devices associated to a person and to access the complete history of actions. It is a read-only access.

The permission **Enrolled devices management** allows administrators to enroll or revoke a device. The scope of the administrators includes all the devices and all the owners. It is not possible to limit the management of enrolled devices to a sub-set of the organization. However,

all the administration actions are traced and it is possible to audit each administrator's operations.

11.3.3 Enrolled devices display

All the devices administration functions are in the **Device enrollment** window.

The **Filter** panel enables to filter the list of devices in order to consult the enrollment status of a specific device, of a given person or to know the list of enrollment operations performed by a given console administrator.

The list of devices in the lower panel details enrollments and in particular the name of the administrator who enrolled or revoked the device. This list displays both devices enrolled or pre-enrolled by administrators and devices enrolled in an automatic or interactive way on workstations. In the two last cases, the values of the columns **Enrolled by** and **Owner** are the same.

You can copy a selection of devices from this list (right-click > **Copy**) and paste it in the **Device Control** tab in a security policy. For more information about device control, refer to the section **Device Control**.

Device selection

Administration screens automatically detect devices connected to the workstation.

Click the **Detect** button to display the device identifiers in the **Device** drop-down list.

Directory

In the **Owner** and **Performed by** fields, select the owner of a device or the administrator who performed the enrollment operation from the organization directory.

To select the owner or administrator, click the **Select** button to open the advanced search form. Enter the Windows connection name or the DNS name or any letter of the name, the location or the department of a person preceded or followed by the "*" character to filter the user list.

Events history

In the **Filter** panel, if the **History** checkbox is unchecked, the **Device** list only displays the current status of the device or of the person selected in the filters.

If it is checked, the list also displays past events.

11.3.4 Device enrollment and revocation

An administrator can enroll a device by clicking on **Enroll** in the **Devices** panel. The **Enroll a device** window displays:

- the device is plugged on the workstation hosting the administration console: the administrator clicks then on **Detect**. He/she can select the device, the owner and enter a comment.

- the device is not plugged on the workstation: the administrator manually types the serial number of the device in the **Device** field. Whenever the device is plugged into a workstation on which the SES agent has been installed, enrollment will be automatic.

When an enrolled or pre-enrolled device is listed in the main panel, you can revoke it by selecting it in the list and by clicking on **Revoke**. The **Revoke an enrolled device** window displays. You can then view the details of the device and add a **Comment** about the revocation.

The revocation operation is possible whether the device is plugged or not on the workstation hosting the administration console. If it is not plugged, the SES enrollment traces will be deleted the next time the device will be plugged on a workstation hosting a SES agent. It will then be unavailable.

It is also possible to enroll again a device previously revoked.

Administration events are systematically traced in the Stormshield Endpoint Security base and can be viewed in the history.

11.3.5 Pre-enrollment of removable devices

An administrator can also pre-enroll a batch of removable devices by importing a *.csv* file in the console. Enrollment will be thus pending for these devices and they will be automatically enrolled when they are plugged to a workstation with an SES agent for the first time.

A device is enrolled for the user specified by the administrator in the imported file. It is not enrolled for the user who plugged the device and who is connected to the Microsoft Windows session.

Pre-enrolling devices takes the priority over the other types of enrollment. For example, even if the automatic enrollment for a user connected to a workstation is allowed by the security policy, a pre-enrolled device which is plugged to this workstation will be enrolled for the user specified during pre-enrollment.

For more information about enrollment, refer to the section Device Control.

Preparing the file to import

The file must be in *.csv* format and encoded in UTF-8.

The columns must be arranged in the following order. The first line must directly contain the first device to import instead of column headings:

Vendor ID	Product ID	Serial number	Username	**Comment (optional)**

Example:

2385;5734;60A44CB1AE3DB030385A6390;DOMAIN\User0;comment1

2385;5734;60A44CB1AE3DB030385A6391;DOMAIN\User1

2385;5734;60A44CB1AE3DB030385A6392;DOMAIN\User2

SES requires the Vendor ID, Product ID and Serial number columns to identify the device. In the username column, you specify the user for who the device will be enrolled when it will be plugged for the first time. The username can be in two formats:

- NetBIOS domain name\User account name: DOMAIN\User1
- User account name@Domain name: User1@DOMAIN
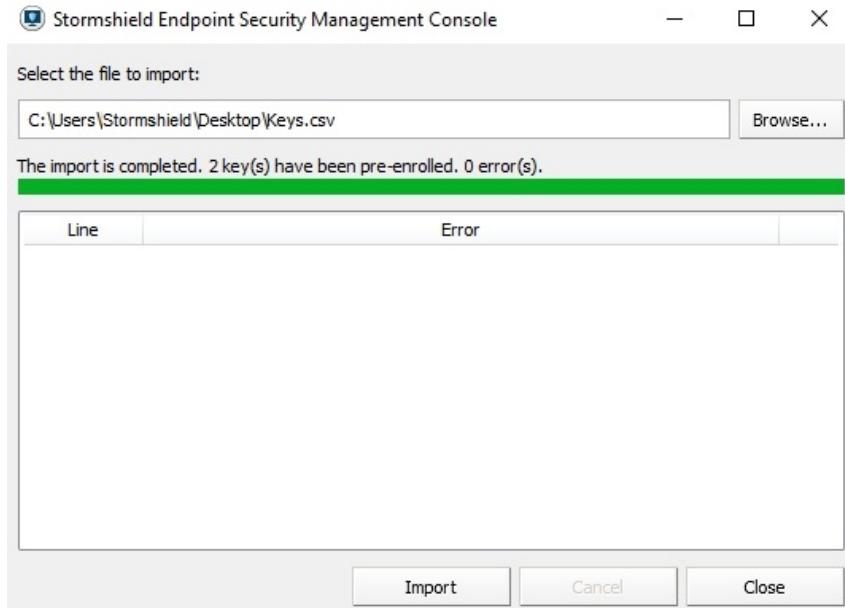
The column separator character must be the one you specified in the **Configuration** > **CSV separator** menu.

Each line displays a device to enroll.

Importing the *.csv* file

To import a list of removable devices:

1. Open the menu **Device Enrollment** in the left panel.
2. In the **Devices** panel, click on **Import**.
3. Select the file to import, then click on **Import**.
4. When the import is done, click on **Close**. The list of devices in the **Devices** panel is updated.

If the operation is canceled during processing, no device is enrolled.

12. Removable Device Encryption

12.1 Overview

12.1.1 Purpose

Removable Device Encryption provides an extra layer of protection by encrypting data stored on USB or FireWire devices with a password-protected key.

⚠ **WARNING**
Removable device encryption is **not** related to the Stormshield Endpoint Security encryption feature.

12.1.2 Characteristics

Advanced Encryption Standard

The Stormshield Endpoint Security encryption feature (for USB and FireWire devices) is based on the Advanced Encryption Standard (AES).
This system which has been approved by the U.S. Government for use with both classified and non-classified documents.

The size of device encryption keys is limited to 256 bits.

Password protection

By password-protecting the encrypted data stored on these devices, sensitive company data is further protected from theft.

Encryption password

The password used to open encrypted files is also encrypted. It is therefore as secure as the encryption applied on files.

Secure erasure

When encrypting a device already containing files, Stormshield Endpoint Security first generates an encrypted copy of old data before performing a secure erasure. When creating new files on a device encrypted by Stormshield Endpoint Security, this erasure operation is not required.

For this reason, the encryption of a device already containing files takes more time than the copy of the same amount of data on an already encrypted device. The number of passes required for a secure erasure depends on the device type: magnetic (external hard disk) or flash memory (USB key) type.

12.1.3 What can be encrypted

You can opt to automatically encrypt entire USB and FireWire devices.

For more information, see Creating an encryption policy to be applied to a group of devices.

⚠️ **WARNING**
The device encryption policy is applied to the entire device group.
The password strength used by the device encryption policy is defined in the **General Settings** panel.
For more information, see Removable Device Encryption and Access to the device without password.

12.1.4 Unencrypted partitions

For devices with partitions, such as external hard disks, you can omit a partition from the encryption policy after the first plug-in.

There is no password prompt for an unencrypted partition.

ℹ️ **NOTE**
Partitions must be created before the device is encrypted.

12.1.5 Encryption key

The encryption key is stored in a file called `sr_id.` in the key root directory.
There is one `sr_id.` file per partition. Each partition can be protected by a different password.

The Stormshield Endpoint Security server contains a copy of the data stored in the `sr_id.` file. If this file is **corrupted** on the removable mass storage device, a copy of the data is automatically downloaded from the server in order to restore the file. This is invisible to the user.

If however, the server is not available, the user will receive a message indicating that:

- `sr_id.` is corrupted.
- Encrypted files are inaccessible.

The user can either request a new encryption key from the administrator or replace the `sr_id.` file with a backup copy (if the user has previously made one).

ℹ️ **NOTE**
For added assurance, the user should also make a backup of the encryption key using the **Export** function in the Stormshield Endpoint Security Agent monitor menu.
For more information, see Agent side.

12.1.6 Synchronization

The first time a device is plugged in after a device encryption policy is applied, it goes through a synchronization process encrypting the entire device.

A progression bar is displayed throughout the process.

12.1.7 Symbology

A blue lock is displayed at "My Computer > Devices with Removable Storage" level to indicate that there is at least one encrypted file stored on the device.

12.2 Creating an encryption policy to be applied to a group of devices

12.2.1 Encryption settings

To set removable device encryption, fill in the following fields in the *Device Control* tab of the security policy:

- **General Settings**.
- **Removable Devices**.

For more information, see the section Device Control.

General settings

The device encryption settings under **Removable Devices > Device Control** of the security policy are the following:

- **Group management:**

  This option makes it possible to enable or disable the management of device groups. To enable device encryption, this option must be enabled.

- **Mass storage recovery:**

  This option allows or denies the user to decrypt the removable device.

- **Mandatory password strength**

  This option defines the password strength used for device encryption.

  The value is set to Standard by default.

  The administrator can define the minimum strength a password should have. As the user enters his password, Stormshield Endpoint Security performs a real-time evaluation of the strength of the password. If the strength is lower than that defined by the administrator, the password is rejected.

The criteria for password strengths are:

- **High**: the password must consist of at least 16 characters, and at least three out of the four following types of characters: lowercase letters, uppercase letters, special characters and numbers.
- **Standard**: the password must consist of at least 12 characters, and at least three out of the four following types of characters: lowercase letters, uppercase letters, special characters and numbers.
- **Low**: the password does not follow the criteria for High or Standard password strengths.

Removable devices

The device encryption settings under **Removable Devices** > **Device Use Control > Group Settings** are the following:

- **File encryption**
  - Disabled:

    No file encryption.
  - Enabled:

    This option encrypts the entire device or a device partition.
- **Access right if encryption is cancelled:**

  This option enables:

- Read-only access,
- Read/Write access,
- Denial of access,

to unencrypted files if the user chooses not to encrypt the device when prompted to create an encryption password.

- **Stand-alone decryption tool (SURT)**:

This option allows or denies use of the SURT encryption tool to enable file decryption on systems not running Stormshield Endpoint Security.

⚠️ **WARNING**
Encryption settings also apply to all devices in the device group.

ℹ️ **NOTE**
If **Default** access to the device group is set to **Denied**, the device will not be able to access the workstation on which the agent is installed.
Access will remain denied whatever the encryption policy applied to devices.

For more information about applying an encryption policy to a device group, see Applying a security policy to an object of the directory.

12.3 Connecting a removable device

12.3.1 Password

The first time a user plugs in a device with an encryption policy, a window:

- Opens.
- Prompts you to enter the new password.
- Prompts you to confirm the password.

If a USB or FireWire device uses an encryption policy, a pop-up window prompts for the password each time the device is plugged in.

The mandatory password strength is set by the administrator in **General Settings > Device Control**.

For more information, see Passwords.

12.3.2 Synchronization

The first time a device is plugged in after a device encryption policy is applied, it goes through a synchronization process encrypting the entire device.

A progression bar is displayed throughout the process.

⚠️ **WARNING**
During the synchronization process, the user should not leave the computer for a large period of time.
sIf the computer automatically locks or goes into standby mode after a period of time, the synchronization process will stop. The user will then have to enter the device encryption password to relaunch the process.
Default access control is bypassed. This means that all files on the device will be encrypted even if **Default** access is set to Denied or Read only.

12.3.3 Access to the device without password

If, when prompted to enter the password, the user clicks **Cancel**, the device is locked to prevent unencrypted data from being written to the device.

In this case, access rights depend on the **Access right if encryption is cancelled** in **Removable Devices > Device Control > Group Settings**.

Access rights can assume the following values:

- Read (only).
- Read/Write.
- Denied.

ℹ️ **NOTE**
It should be noted that **Default** access and **Exceptions by file extension** settings also apply to the device group.
Therefore, if default access to the device is set to **Denied**, the user cannot access the device.

If the user tries to access an encrypted file without setting the password, information contained in the file will be displayed as encrypted text.

ℹ️ **NOTE**
The Access right if encryption is cancelled option is valid only for this session. Next time the user plugs in the device, the password prompt will be displayed again.

12.3.4 Access to encrypted data

As long as the correct password is entered, there is no difference to the user between reading encrypted and unencrypted data.

Data is encrypted whenever it is written to a device with encryption enabled. If a file is copied, created or modified on the device, its data is encrypted.

12.3.5 Behavior when deactivating removable device encryption

When disabling the group parameter **File encryption** under **Device Control** of the security policy, the encrypted device remains encrypted and files added on the device are encrypted.

The user must manually decrypt the device. The device will remain unencrypted according to the new policy.

For more information about removable device decryption, see section Decrypting a removable device.

12.3.6 Using encrypted devices on other computers

Sharing encrypted files

Encrypted files on a device can be shared on condition that:

- The device is plugged into another computer running a Stormshield Endpoint Security agent.

- The encryption policy on the computer includes **Read** or **Read/Write** access.

- The user knows the encrypted device password.

Systems not running Stormshield Endpoint Security

If an encrypted device is plugged into a computer that is not running a Stormshield Endpoint Security agent:

- Encrypted files can be opened but their content will be displayed as encrypted text.
  If the device contains an unencrypted partition with files, these files can be used as normal.

- New files can be added onto the device. They will not be encrypted though.

- Files can be copied from the device but they will remain encrypted.

- If the SURT encryption tool is enabled in the device Group Settings of the security policy, the user can encrypt and decrypt files simply by dragging and dropping files to the Stormshield Endpoint Security Express Encryption icon .

  This standalone encryption tool can also be downloaded from MyStormshield website.

  For more information, see section SURT.

Other systems running Stormshield Endpoint Security

If an encrypted device is plugged into a computer that is running a Stormshield Endpoint Security agent:

- The encrypted device will be unaffected by the computer encryption policy.

- The user will need to enter the encrypted device password in order to access the files.

- The computer audit and access policies will be applied to the device.

12.3.7 Removing SD cards

When removing an SD card from the reader, Stormshield Endpoint Security is not notified.

If you remove an SD card from the reader, the system will not detect the action and the card volume label will still be displayed in Windows Explorer.
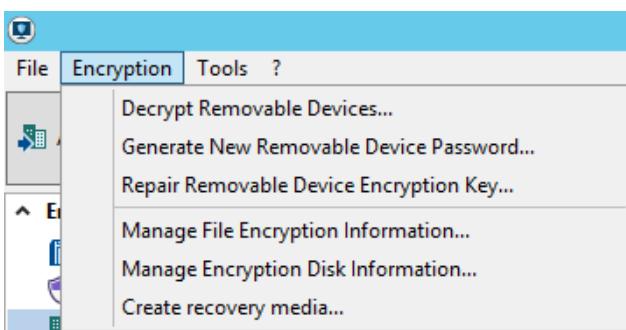
As a consequence, if you install a new SD card, Stormshield Endpoint Security will not prompt you to enter any password. Instead Stormshield Endpoint Security will use the password of the previous SD card. The user will not be able to access existing files because the key used to decrypt them is not correct and new files will be encrypted with the wrong key.

Before removing an SD card, it is imperative to use the eject function in Windows (right-click the reader and click **Eject**).
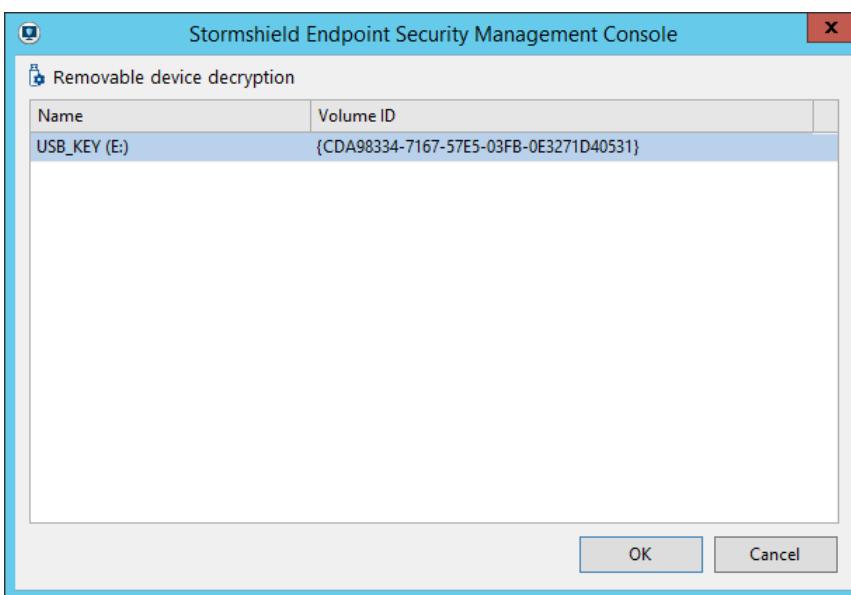
12.4 Decrypting a removable device

12.4.1 Administrator side

To decrypt a removable device, perform the following operations:

1. Connect the removable device to the computer where the management console is installed.

2. Click the **Encryption** menu.

3. Select **Decrypt Removable Devices**.

4. Enter the console certificate password.

5. Select a device from the list.

6. Click **OK**.

7. If the administrator's workstation has a Stormshield Endpoint Security agent, the removable device must be disconnected so that it can be used again later.

12.4.2 Agent side

Any Stormshield Endpoint Security agent user can decrypt a device on condition that **General Settings > Device Control > Mass storage recovery** is set to **Allowed** in the security policy.
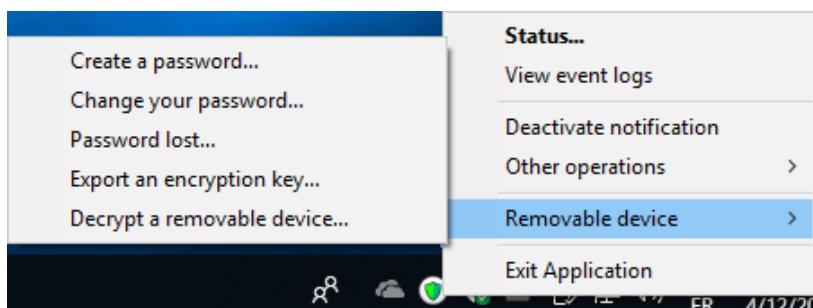
> ℹ **NOTE**
> During the decryption process, the user should not leave the computer for a large period of time even if the device has a large disk space.
> If the computer automatically locks or goes into standby mode after a period of time, the synchronization process will stop.
> The user will then have to enter the device encryption password to relaunch the process.
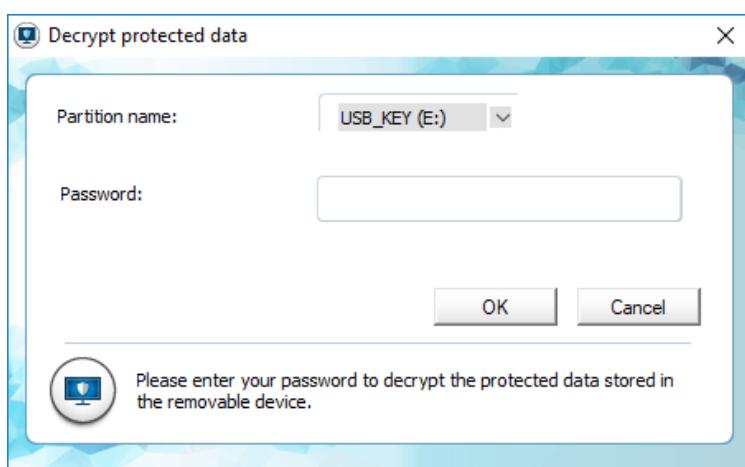
To decrypt a removable device, the user must follow the steps below:

1. Right-click the Stormshield Endpoint Security icon in the taskbar to display the menu below:

2. Click **Removable device** and **Decrypt a removable device**.

The Decrypt protected data window is displayed.

3. Select the device from the list.
4. Enter the device encryption password.
5. Click **OK**.

12.5 Passwords

If a user forgets the encryption password, a new one can be provided by the administrator.
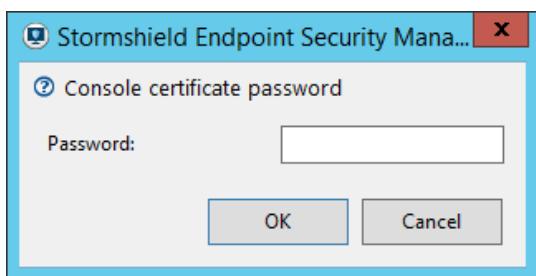
> ⚠️ **WARNING**
> The procedure requires action by both the user and the administrator.

12.5.1 Administrator side
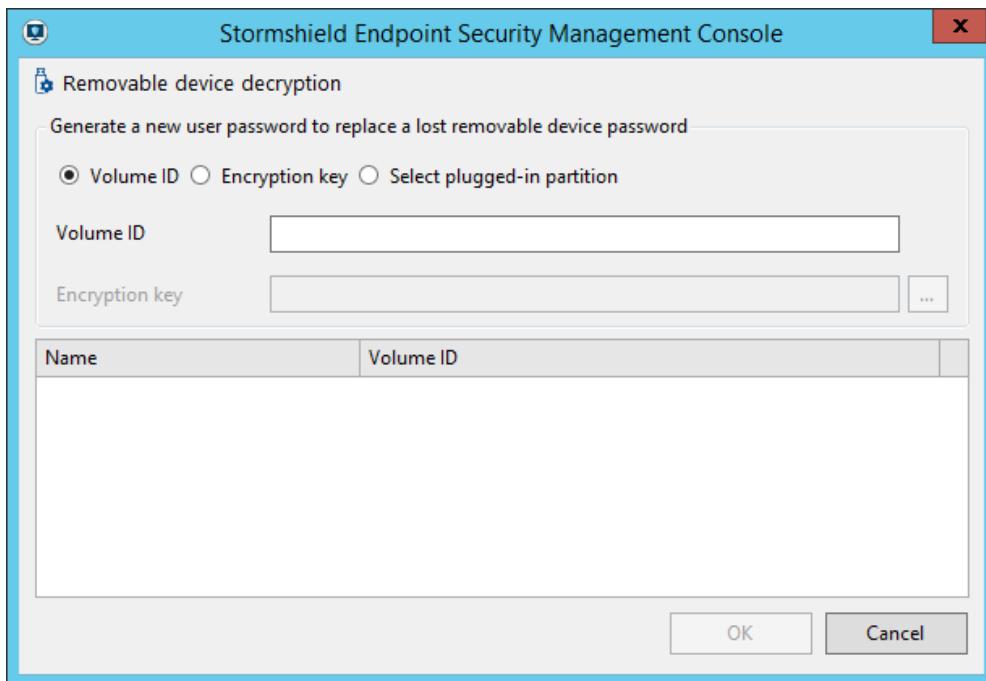
Replacing a lost password

To replace a lost password, perform the steps below:

1. Click **Encryption > Generate New Removable Device Password**.
2. Enter the console certificate password.
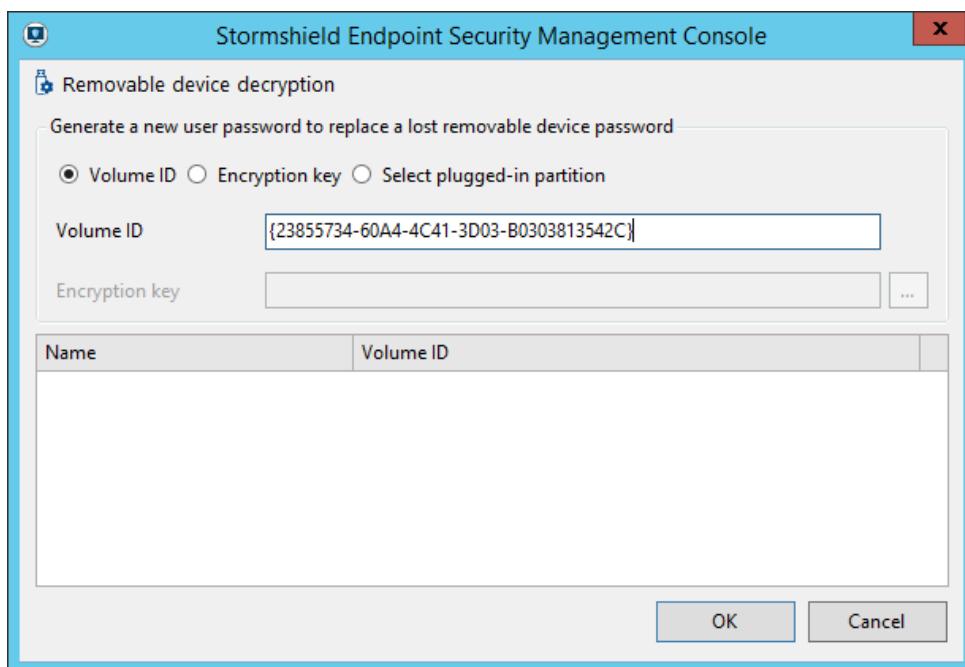
3. Select how to generate a new password:
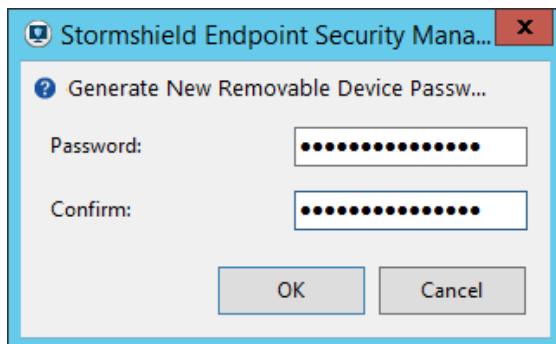
- By **Volume ID**:
  - Click the **Volume ID** radio button.
  - Enter the volume ID sent by the user and click **OK**.

    The **OK** button will be activated as soon as the volume ID is recognized.

- Enter the new password.
- Confirm the password.
- Click **OK**.

◦ By **encryption key**:

- Click the **Encryption key** radio button.

- Select the encryption key file from your system by clicking the Browse button .

- Click **OK**.

- Enter the new password.

- Confirm the password.

- Click **OK**.

◦ By **Select plugged-in partition**:

- Click the **Select plugged-in partition** radio button.

- Select the removable device partition.

- Enter the new password.

- Confirm the password.

- Click **OK**.

> ### 🛈 NOTE
> If the action selected fails to generate the key, try another option.

Exporting an encryption key

After generating a new password for the user, the administrator will export the encryption key. To do so, he must follow the steps below:
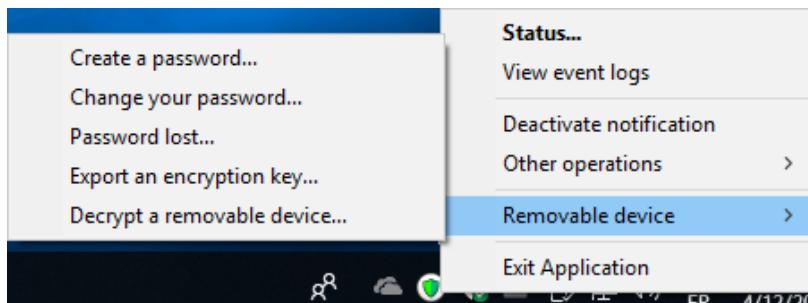
1. After entering the new encryption key password, save the `ExportKey.sxk` file.

   If you choose **Select plugged-in partition**, the encryption key file `ExportKey.sxk` will be directly exported to the connected device.

2. Notify the user of the new key location. The user can then import the new key.

12.5.2 Agent side
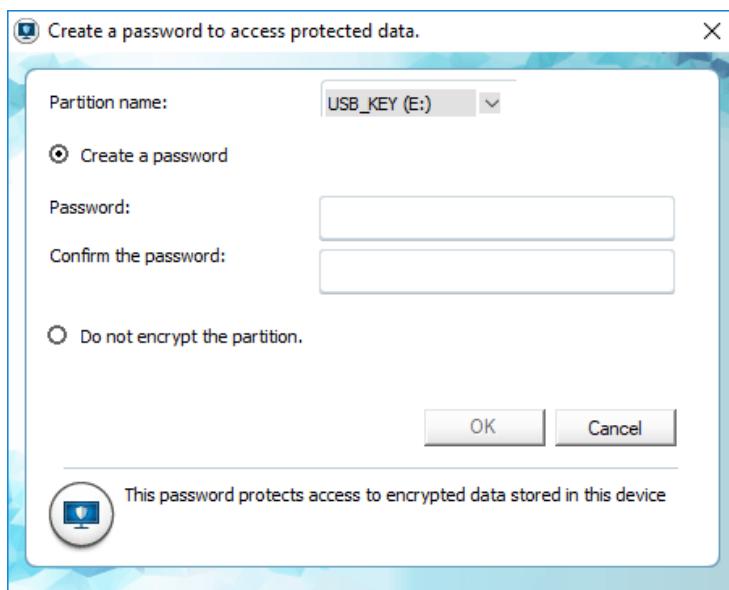
Creating a password

To create a password, the user must follow the steps below:

1. Right-click the Stormshield Endpoint Security 🛡 icon in the taskbar and click **Removable device > Create a password**.

   A window is displayed that prompts you to create your password to access protected data.

2. Select the volume from the list.

3. Enter the required information.

4. Click **OK**.

Changing a password
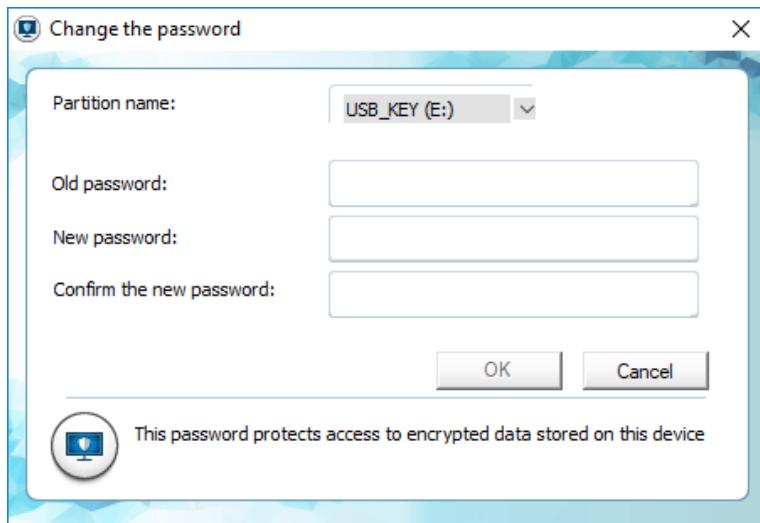
Users can change their own password in the Stormshield Endpoint Security menu.

The user must follow the steps below:

1. Right-click the Stormshield Endpoint Security 🛡 icon in the taskbar and click **Removable device > Change the password**.

A window is displayed that prompts you to change your password to access protected data.
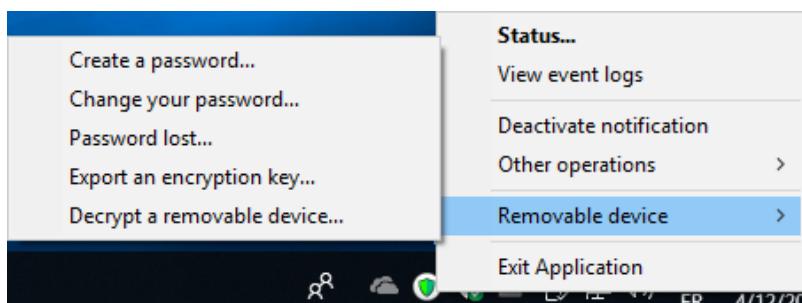
2. Select the volume from the list.

3. Enter the required information.

4. Click **OK**.
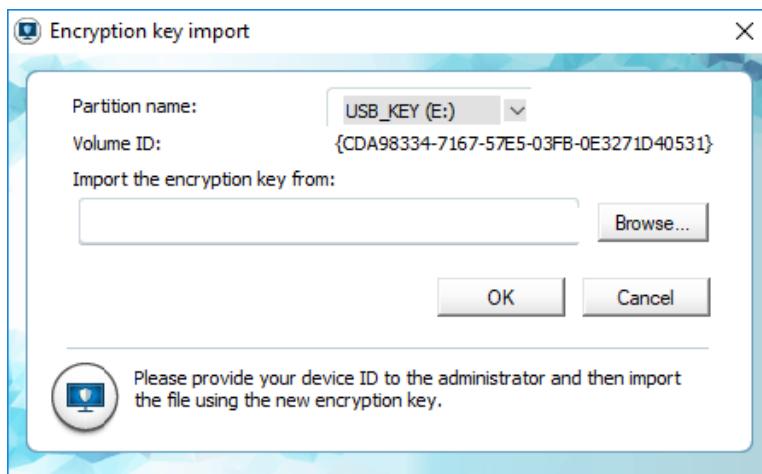
Lost password

To obtain a new password from the administrator, users must follow the steps below:
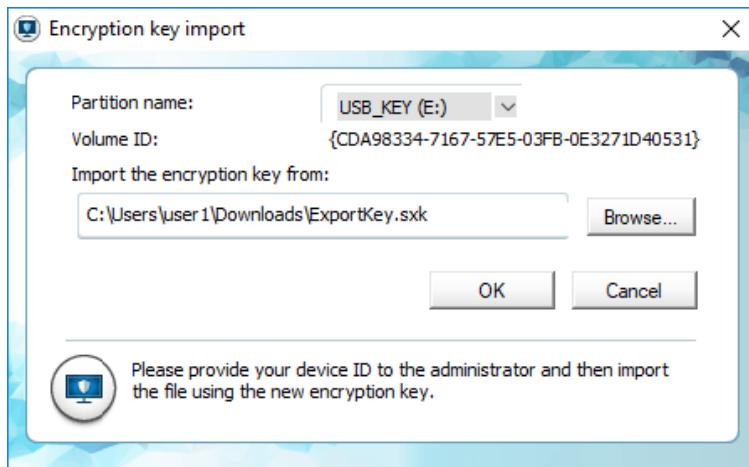
1. With the device plugged in, right-click the Stormshield Endpoint Security 🛡 icon in the taskbar and click **Removable device**.

2. Click **Password lost**.

Create a password...		Status...
Change your password...		View event logs
Password lost...		Deactivate notification
Export an encryption key...		Other operations
Decrypt a removable device...		Removable device
		Exit Application

A partition name and volume ID (key ID) are displayed.

Encryption key import

Partition name: USB_KEY (E:)
Volume ID: {CDA98334-7167-57E5-03FB-0E3271D40531}
Import the encryption key from:

[   ] Browse...

OK   Cancel

Please provide your device ID to the administrator and then import the file using the new encryption key.

3. Send the volume ID to the administrator (by email or by copying it to a server, etc.).

4. If the administrator sends you the encryption key, you must import it:

   ◦ Click **Import the encryption key from** field.

   ◦ Enter the path and filename (or click the **Browse** button to locate the encryption key).

   ◦ Click **OK** to import the replacement file.

Encryption key import

Partition name: USB_KEY (E:)
Volume ID: {CDA98334-7167-57E5-03FB-0E3271D40531}
Import the encryption key from:

[C:\Users\user1\Downloads\ExportKey.sxk] Browse...

OK   Cancel

Please provide your device ID to the administrator and then import the file using the new encryption key.
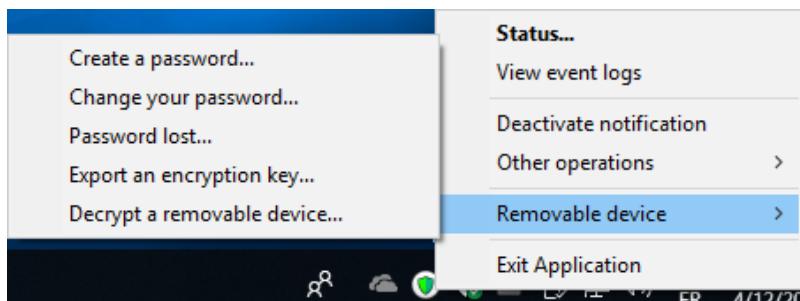
Exporting an encryption key
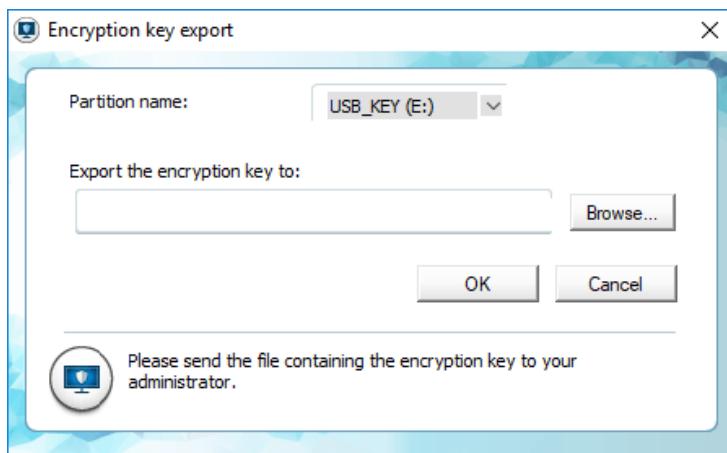
Stormshield Endpoint Security agent users can export a **copy** of the encryption key for backup purposes. Exporting an encryption key can be useful when there is no network access.

To export an encryption key, the user must follow the steps below:
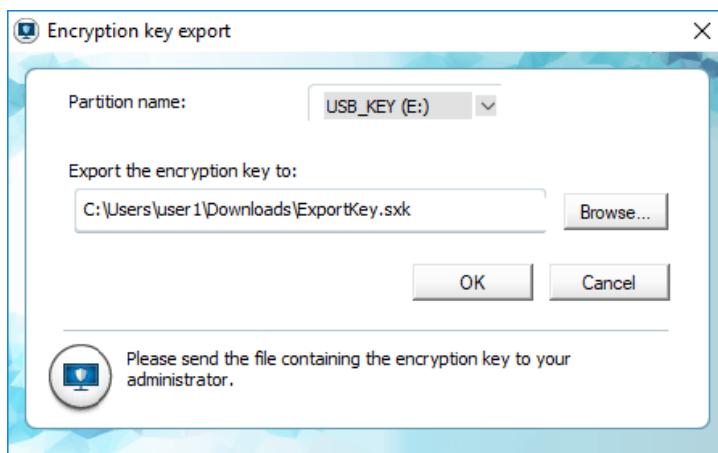
1. With the device plugged in, right-click the Stormshield Endpoint Security ⊙ icon in the taskbar and click **Removable device**.

2. Click **Export an encryption key**

The encryption key export window is displayed.
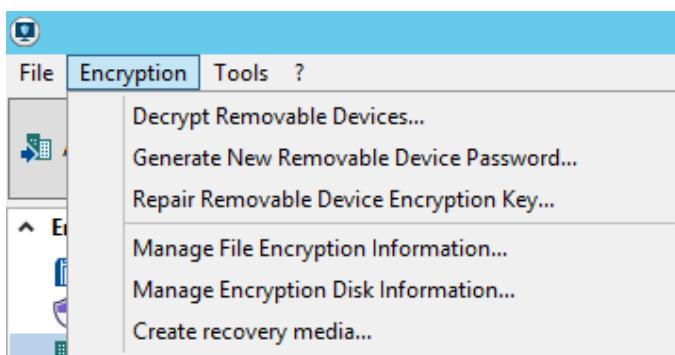
3. Click **Export the encryption key to** field.

4. Enter the path and filename (or click the **Browse** button to locate the encryption key).

5. Click **OK** to export the file.
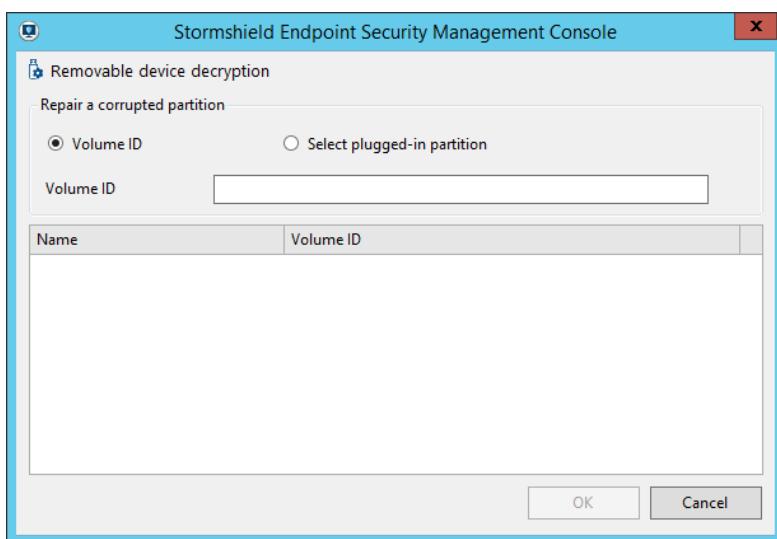
12.6 Repairing a corrupted encryption key

To repair a corrupted encryption key, you must follow the steps below:

1. Select **Encryption > Repair Removable Device Encryption Key**.

2. Select how to repair the encryption key.

- ◦ If you choose **Volume ID,** enter the volume ID in the text field.

- ◦ If you choose **Select Plugged-In Partition,** select the appropriate volume.

3. Click **OK.**

    The **OK** button will be activated only if the volume ID is correct or if the removable device is detected.

4. Save your new encryption key.

13. Encryption

13.1 Data encryption overview

13.1.1 Purpose

Data encryption provides an extra layer of data protection via encoding and password usage.

By password-protecting the encrypted data on your hard disks, sensitive data is protected in case of computer theft (**example**: laptops stolen during business trips).

Data encryption consists in:

- a full disk encryption used to encrypt everything on a specific disk partition, including computer configuration. New files saved on the computer are automatically encrypted.

- the encryption of file content located in folders defined by the administrator in the encryption policy.

13.1.2 Characteristics

Advanced Encryption Standard

The Stormshield Endpoint Security Encryption feature is based on the **Advanced Encryption Standard** (AES). This is a symmetric encryption system which offers the choice of a **128**, **192** or **256**-bit key length for encryption.

This system has been approved by the U.S. Government for use with both classified and non-classified documents.

Stormshield Endpoint Security 's Data Encryption has obtained the **Federal Information Processing Standard** (FIPS) **140-2** certification.

> **ℹ NOTE**
> Two **CBC** (Cipher Block Chaining) modes are available in Data Encryption.
> For more information, see Full Disk Encryption Parameters .

Invisibility

Once the administrator has configured the encryption policy, the computer launches the synchronization process. The agent's computer data is automatically encrypted by **file** or by **disk** (depending on the encryption policy applied).

> **ℹ NOTE**
> File encryption does not exclude the use of full disk encryption. Both options can be simultaneously enabled.

After the deployment of the encryption policy, Stormshield Endpoint Security users will not notice the encryption process in progress while working on their computer.

Nevertheless, some cases exist where a progress bar is visible during the encryption process (also called synchronization):

- Change of encryption policy.

- File transfer from unencrypted to encrypted paths.

- Recovery.

To prevent the display of encryption indicators, the administrator can enable **Stealth mode** under the file encryption parameters.

The lock 🔒 indicating that encryption has been applied to a file will not be displayed on encrypted files.

> ℹ️ **NOTE**
> If the stealth mode is enabled, the administrator needs to set authentication mode to **Windows**.

13.1.3 Supported system, hardware and software

Unsupported hardware and software are the following:

- Software RAID and dynamic disks.
- Partition management and disk cloning tools.
- Hard drives with sector size other than 512 bytes.
- Extended partitions are not supported by Full Disk Encryption. Only disks containing master partitions can be encrypted.
- Multiboot (several operating systems on the same partition or on two separated partitions) is not supported by disk encryption.
- Boot loaders other than Microsoft Windows boot loader are not supported by disk encryption.

To encrypt removable devices, you can use the **Removable Device Encryption** feature in Stormshield Endpoint Security.

For more information, please refer to Removable Device Encryption.

> ⚠️ **WARNING**
> Before using the data encryption feature, you must save all your data.

> ℹ️ **NOTE**
> If the encrypted hard disk includes one or several defective sectors, encryption will be interrupted and all data already encrypted will be decrypted again.
> It is recommended to perform a deep scandisk and repair defective sectors before applying Full Disk Encryption.

Just after applying a full disk encryption policy, downgraded performance can be observed when opening a session after startup.

This is absolutely normal due to the fact that encryption starts very early before the opening screen is actually displayed.

> ⚠️ **WARNING**
> The agent has to connect to the Stormshield Endpoint Security server in order to deploy full disk encryption.

Full disk encryption or decryption cannot be interrupted once started.

Once the disk is encrypted with full disk encryption, it is no longer possible to add, modify or remove anything on partitions. If you need to change something on partitions, first decrypt the disk by disabling full disk encryption in the management console and then, enable again the policy after changes.

13.1.4 Interoperability with versions previous to the certified 7.2.06 version

If you have a server in version 7.2.06 or higher, agents will have to be updated to the same versions to be able to use encryption.

Versions 7.2.06 and higher provide an enhanced authentication protocol with a strengthened identification step on the agent. They also provide new processes for exchanging data between servers and agents which are more secure.

When you update agents to version 7.2.06 or higher, users will have to reset their password in order to take advantage of the new authentication protocol.

If agents are not updated:

- users will not be able to modify their user password and recovery password and will therefore not take advantage of the enhanced authentication protocol.
- the server will not be able to exchange data related to encryption with these agents.

13.2 Encryption types

13.2.1 File encryption

File encryption characteristics are the following:

- Only file content is encrypted.
- The file list is defined by the administrator.
- The system and programs remain unencrypted.

The **advantages** of file encryption are the following:

- Each file is usually encrypted with a separate encryption key.
- Individual management of encrypted files.
- The Administrator can modify which files to encrypt.
- When a workstation is in multi-user mode, each user has a unique password for authentication.

The **disadvantages** of file encryption are the following:

- The administrator may forget to select important data that need to beencrypted.
- Users may save data in unencrypted folders.
- Less performance than full disk encryption.

13.2.2 Full disk encryption

Full Disk Encryption is used to encrypt everything on a specific disk partition. It is only compatible with the BIOS interface which supports the MBR partitioning scheme and it is not compatible UEFI (GPT partitioning).

🔴 IMPORTANT
When using **Full Disk Encryption,** NEVER choose a system restore point that is older than the encryption policy's application date.

In the event of a restoration, this operation would destroy the NEP driver (Stormshield Endpoint Security full disk encryption) and the encrypted disk would no longer be readable.

ℹ️ NOTE

When defining or typing the encryption password, follow these guidelines:

- do not use the Caps Lock key (use Shift).

- do not use the numeric keypad (use the numbers at the top of the keypad).

The **advantages** of full disk encryption are the following:

• Everything is encrypted even computer configuration.

   This is a major advantage when the administrator forgets to encrypt some files.

   This becomes even more important when the administrator wants to encrypt sensitive configuration files or data which are directly stored by software into program directories.

• Full disk encryption deployment is easier than File Encryption deployment.

The **disadvantages** of full disk encryption are the following:

• There is only one encryption password shared by all users of the computer.

• Full disk encryption deployment may take longer than file encryption deployment depending on disk size.

• Only the hard disk on which the system has been installed is encrypted. If you want to encrypt documents present on another hard disk, you have to use both full disk encryption and file encryption (under **General Settings** > **Protection mode**).

• Only file encryption will be applied to the second hard disk.

13.3 Creating an encryption policy

13.3.1 Graphical interface

Encryption policies are created and accessible from the **Policies** menu in the **Environment Manager** section.

13.3.2 Procedure

To create an encryption policy, follow the steps below:

1. Right-click the **Encryption** folder in the **Policies** menu from the **Environment Manager** section and select **New Policy** or click ➕ in the toolbar.

2. Name the policy and click **OK**.

3. Specify the encryption parameters.

    For more information, see:

    ◦ **Encryption parameters**.

    ◦ **File Encryption Parameters**

    ◦ Full Disk Encryption Parameters

4. Apply the encryption policy to a directory object.

    For more information, see **Applying an encryption policy to an object of the directory**.

5. Click **Deploy to the environment**.

> **ℹ NOTE**
> When you apply a new encryption policy to an agent group, the policy will not take effect until next reboot of the workstation.

> **ℹ NOTE**
> After applying an encryption policy, the password of the Stormshield Endpoint Security server's certificate files (*root.pem* and *rootcert.pem*) must not be modified.

To disable encryption on a workstation:

1. Modify the encryption policy currently in force or create a new policy.
2. Disable **Full disk encryption** and/or **File encryption** settings.
3. Apply this new policy to the workstation concerned.

Instead of that, if you just remove an encryption policy from an object of the directory, agents will keep applying the last encryption policy. This will avoid inadvertent decryption of a workstation.

13.4 File encryption features

13.4.1 Multi-user security

Stormshield Endpoint Security uses two types of encryption keys: a computer key and a user key.

Each computer has only one computer key but multiple user keys. This enables users to share computers and still maintain privacy and data confidentiality.

Computer encryption key

Folders and files which are encrypted with the computer encryption key can be opened by any authorized user.

User encryption key

After applying an encryption policy, folders and files which are encrypted with a user encryption key can only be opened by the first user who created or accessed the file/folder.

For more information, see:

- Computer encryption key.
- User encryption key.

13.4.2 Data erasure security

Providing secure file erasure implies overwriting deleted files to prevent data recovery (especially by unauthorized users). This is highly important when a laptop is stolen or left unattended.

You can select the number of overwrites to perform for data erasure.

> **ℹ NOTE**
> Professionals can retrieve information from almost any magnetic data carrier, even damaged ones.
> To delete a file permanently, the secure data erasure process performs several random data overwrites where the deleted file was stored.
> It is currently the only method which is valid to obliterate securely data on your disk. It makes it almost impossible to retrieve data via magnetic remanence.

13.4.3 File encryption options

To encrypt a file, you need to enter a path which can be a folder, a file or an extension with the help of the wildcard *****.

Here are some examples of wildcard use:

- c :*
- *\crypt*
- c :*.txt
- c :\file.txt
- |userprofile|*

You can also exempt files and/or folders from encryption.

For more information, see File Encryption Parameters and File Encryption Parameters .

13.4.4 Password creation and user logon

Password creation

The first time the user logs onto the computer after the encryption policy isapplied, he is prompted to create an authentication password or a PIN codedepending on the type of authentication selected (Windows, Secondary or Smart-Card).

This authentication password becomes the encryption password to accessprotected data on the workstation.

If a user is in the process of creating a new password and the Agent loses its connection to the server before the password is confirmed, the following error message is displayed:

```
You are not connected to the server
```

> **⚠ WARNING**
> If you apply a **file encryption** policy just after installing the Stormshield Endpoint Security agent, a popup window prompts the user to create his password.
> qAn error message is displayed if the agent computer was not rebooted before creating the user password.
> Reboot the computer in order to fix the problem and create the user password.

Create password prompt

The same password window is displayed to new users and users who already have passwords.

This is because a user may already have an existing encryption password on another computer.

Another situation may be that an encryption password already exists for the user and the Stormshield Endpoint Security agent has been uninstalled and re-installed on his computer.

> ⚠️ **WARNING**
> If the user already has an encryption password, this password should be entered in both the **New password** and **Confirm password** fields.

Connection

If a user tries to log on with an incorrect password, an error message is displayed.

After five unsuccessful logon attempts, the user will be blocked from logging on for 30 seconds. If the first logon attempt after the 30-second wait fails, the user will automatically be blocked from logging on for another 30 seconds.

13.4.5 Synchronizing

A synchronization with the hard disk is performed when a user logs on for the first time after an encryption policy has been applied.

Next time this user logs in, synchronization will occur only if the list of encrypted paths is modified.
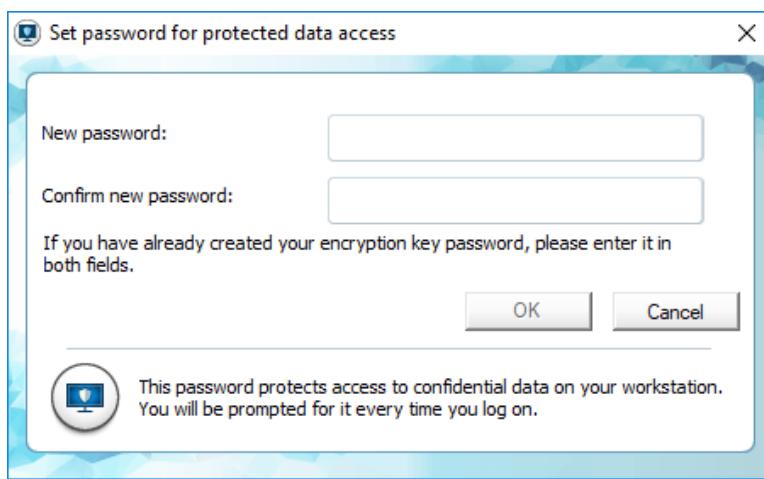
Synchronization occurs when a user moves a folder or several files from an unencrypted zone to an encrypted zone.

Desynchronization occurs when a user moves a folder or several files from an encrypted zone to an unencrypted zone.

If an unauthenticated user created files in an encrypted zone, the files will remain unencrypted until the user makes an encryption authentication or performs a manual synchronization of the encrypted zone.

To authenticate, the user must right-click the Stormshield Endpoint Security icon in the taskbar and select **Authentication > Access to Protected Data**.

The first time the user logs in, he will fill in the following fields:

Unencrypted files will be encrypted on next authenticated access or when performing a manual synchronization of the encrypted zone using **Resynchronize encryption policy**.

Desynchronization

During desynchronization, the hard disk is restored to its original state and all files are decrypted.

Desynchronization occurs when:

- A folder is removed from the list of encrypted paths.

- The encryption key type associated with a zone is modified.

- The Stormshield Endpoint Security agent is uninstalled and decrypting data at uninstallation is enabled. Only files encrypted with a computer key are unencrypted. Files encrypted with a user key must be decrypted manually.

> ### ⓘ NOTE
> When an encryption policy is modified, encrypted folders which no longer feature in the encrypted zone list are desynchronized whereas the folders which are defined in the new encryption policy are synchronized.
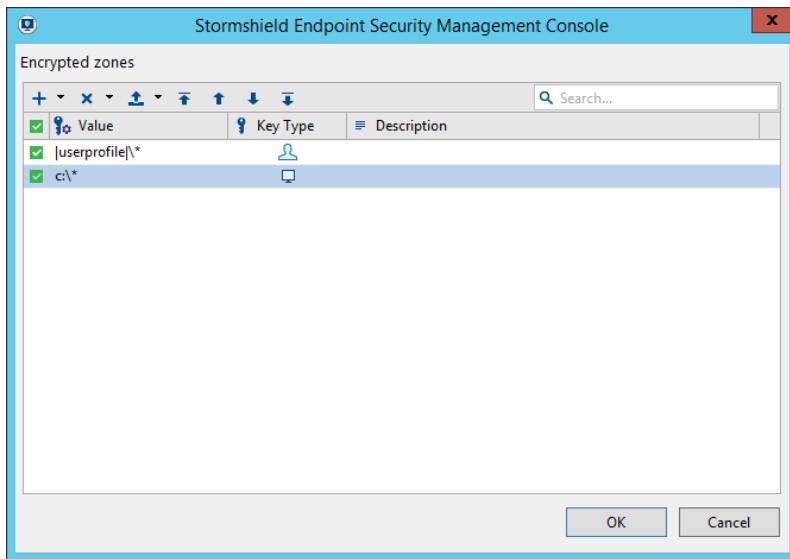
13.4.6 Synchronization with multiple users

If a computer has multiple users, encrypted files are resynchronized whenever a new user logs on for the first time.

Encrypted files are resynchronized with the encryption key type associated with each new user.

To illustrate this, consider the following example. Two users share the same computer. Each user has a specific user profile.

To display the window below, go to **Encryption Policies > File Encryption Parameters > Encrypted zones**.

The encryption policy is defined as follows:

- The user encryption key 🔏 is applied to folder
  `|userprofile|\*`

- The computer encryption key 🖥 is applied to `C:\*`

> ### ⚠ WARNING
> The encrypted zone with the most generic zone should always appear **last** in the encrypted zone list so that the more specific rules are applied **first**.
> Unencrypted zone rules have priority over other encryption rules.

First synchronization

For example, Craig is the first user to log on. His user profile is:

```
userprofile = c:\Documents and Settings\craig
```

The synchronization process encrypts:

- With Craig's **user key** all files stored in:

  `c:\Documents and Settings\craig`

- With the **computer key** all files stored on drive `C:\` except:

  - The folders defined in the Unencrypted zones option (if any).
  - `c:\Documents and Settings\craig`
  - Files exempted from encryption (see Appendix Files Exempted from Encryption).

Subsequent synchronizations

A new user, Lucy, logs on. Her user profile is:

`userprofile = c:\Documents and Settings\lucy`

A new synchronization process is now launched.

The files stored in `c:\Documents and Settings\lucy` were previously encrypted with the computer key on first synchronization.

This new synchronization process will remove the computer key and re-encrypt the files with Lucy's user key.

> ⚠️ **WARNING**
> Even if some users allow other users to access their files with ACL on the New Technology File System (NTFS), access to files encrypted with user keys will be denied to the latter.

13.5 Encryption parameters

13.5.1 General Settings

General Settings enable you to set a number of commands and options such as:

- Allow creation of encrypted archives.
- Allow secure file erasure.
- Number of secure erase cycles.
- Erase swap file when machine is stopped.
- Minimum characters required for second authentication password.
- Mandatory password strength.
- Encryption key size.
- Enforce encryption policy.
- Password change enforcement.
- Maximum password age (visible if the previous option is enabled).

Allow creation of encrypted archives

This option allows agent users to create their own encrypted files which they can safely send by email to other users, inside or outside the company network, without the risk of their contents being read in transit over the Internet.

In the encryption policy edition window, when Allow creation of encrypted archives is set to Allowed, the user can right-click on the file/folder to display the encryption options in the drop-down menu.

For more information about files and encrypted archives, see SURT.

Allow secure file erasure

When this option is enabled, agent users can erase their files securely.

Files are overwritten the number of times specified in **Number of secure erase cycles** in **General Settings**.

When this option is disabled, it is no longer displayed in the menu. The user cannot select the **Delete securely** option.

Number of secure erase cycles

This option indicates the number of erase cycles to be performed to securely delete files and folders.

The files marked deleted are overwritten the number of times specified in **Number of secure erase cycles** in General Settings.

By default, the value is **3**.

> **NOTE**
> You may increase this value. However, it will increase the time it takes to erase files/folders, which can be problematic with bulky files/folders.

Erase swap file when machine is stopped

This option ensures that the swap file is completely erased whenever the computer is stopped.

Minimum characters required for second authentication password

This is the minimum number of characters required to the user to create the password for protected data encryption and decryption.

By default, the value is **8**.

> **NOTE**
> This option can be modified only when the authentication type is set to **Secondary**.

Mandatory password strength

The administrator can define the minimum strength a password should have. The strength is measured according to three levels: High, Standard and Low.

As the user enters his password, Stormshield Endpoint Security performs a real-time evaluation of the strength of the password. If the strength is lower than that defined by the administrator, the password is rejected.

The criteria for password strengths are:

- **High**: the password must consist of at least 16 characters, and at least three out of the four following types of characters: lowercase letters, uppercase letters, special characters and numbers.
- **Standard**: the password must consist of at least 12 characters, and at least three out of the four following types of characters: lowercase letters, uppercase letters, special characters and numbers.
- **Low**: the password does not follow the criteria for High or Standard password strengths.

⚠️ **WARNING**

When using full disk encryption, the number of password entry attempts on computer startup is limited to 10. When exceeding 10 attempts, it is necessary to start the computer again.

ℹ️ **NOTE**

When specifying a password, the user is asked to restart the computer before starting disk encryption. Restarting the computer is required to validate the possibility to enter the password during startup. If the user cannot enter the password during startup, Microsoft Windows starts after the tenth invalid attempt and the user is asked to specify a new password.

Encryption key size

The administrator can set the encryption key size to:

- 128 bits.
- 192 bits.
- 256 bits.

Enforce encryption policy

The option is set by default to **Disabled**. If you enable this option, it will prevent the user from closing the password prompt window when opening the session.

Password change enforcement
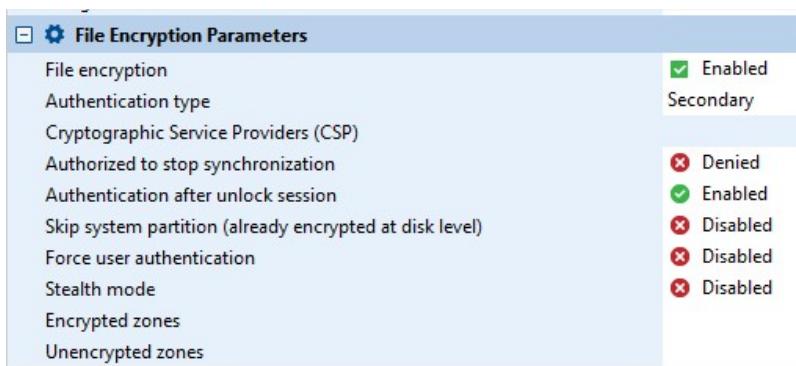
The option is set by default to **Disabled**. If you enable this option, it will advise the user to change his password. If he does not, the former password will remain valid.

If the option is enabled, the **Maximum password age** field is displayed.

13.5.2 File Encryption Parameters

File Encryption Parameters enable you to control the following parameters:

- Authentication type.
- Cryptographic Service Providers (CSP).
- Authorized to stop synchronization.
- Authentication after unlock session.
- Skip system partition (already encrypted at disk level).
- Force user authentication.
- Stealth mode.
- Encrypted zones.
- Unencrypted zones.

Authentication type

An authentication type is defined for each encryption policy. Different authentication types can be applied to different agents groups.

There is only one authentication type per encryption policy.
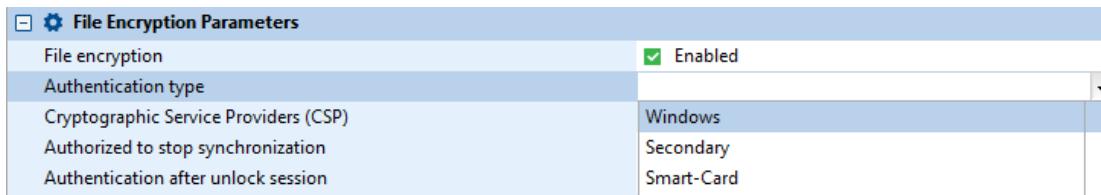
> ⚠ **WARNING**
> After agent deployment, authentication types cannot be modified.
> Modifications must be performed manually by the administrator for each user.
> For more information, refer to Recovery.

The three authentication types are the following:

- Windows.

- Secondary.

- Smart-Card.

Windows authentication type

This authentication type is based on Windows authentication. It is not as secure as Secondary or Smart-Card authentications.

The user can easily access encrypted files using this authentication type by simply logging into Windows using his Windows login ID and password.

> ⚠ **IMPORTANT**
> You cannot uninstall and then reinstall the Stormshield Endpoint Security agent on the same workstation. The encrypted data would be impossible to retrieve. Before uninstalling and reinstalling the agent, you must:

- Either revoke the already existing user key to generate a new one.

- Or change the authentication mode.

Secondary authentication type

When starting the computer for the first time after an encryption policy has been applied, the user is prompted to create a secondary authentication password.

In addition to entering the Windows login password during startup, the user must also enter another password to access encrypted data stored on the hard disk.

⚠ WARNING

It is highly recommended to create a secondary authentication password.

Smart-Card authentication type

The smart-card and the card reader must be connected to the computer in order to access encrypted data in the system.

After Windows startup, the user is prompted to enter a password to open encrypted files stored on the hard disk.

Usually, the password used for this authentication type is the PIN code supplied by the Smart-Card service provider.

Cryptographic Service Providers (CSP)

Cryptographic Service Providers are the Smart-Card manufacturers. The smartcards provided by the CSP include software that must be installed on the Stormshield Endpoint Security agent's computer to allow the use of Smart-Card authentication.

For user-friendly purposes, it is recommended to also install the CSP on the computer where the Stormshield Endpoint Security Management Console has been installed to configure smartcard administrative tasks (example: change user smart-cards by simply choosing from the drop-down menu of the CSP parameter in the Encryption Policy Editor).

⚙ File Encryption Parameters		
File encryption	✅ Enabled	
Authentication type	Smart-Card	
Cryptographic Service Providers (CSP)		▾
Authorized to stop synchronization	Microsoft Base Smart Card Crypto Provider	

If the CSP is not installed on the Stormshield Endpoint Security server but on the agent's computer, the administrator must enter the accurate name of the CSP by double-clicking the second column in the **Cryptographic Service Providers (CSP)** field.

ⓘ NOTE

This option can be set only when the authentication type is **Smart-Card**.
The names of the CSP installed are to be found in the registry under:

```
HKLM\Software\Microsoft\Cryptography\Defaults\Provider
```

The CSP name string must be exactly the same on the console and on the client workstations.

⚠ WARNING

The three folders below are added by default to the files/folders exempted from encryption:

- `|userprofile|\application data\microsoft\crypto\*`
- `|userprofile|\application data\microsoft\`
  `systemcertificates\*`
- `|userprofile|\application data\microsoft\protect\*`

Depending on the CSP used, these folders can include cache data for smart-card certificates which must be readable by the system.

Authorized to stop synchronization
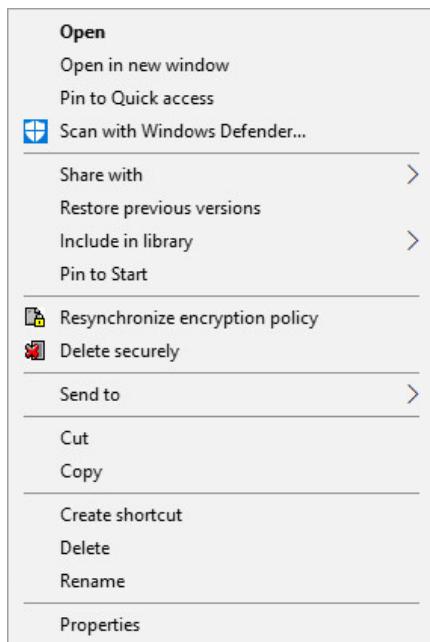
If data is updated in:

- Encrypted zones.

- Unencrypted zones.

then synchronization will be relaunched.

By default, this parameter is set to **Denied**. When set to **Allowed**, the user can stop the synchronization process.

To start resynchronization manually, use the right-click options on the folder to be resynchronized on the Stormshield Endpoint Security agent's computer.

Authentication after unlock session

When this option is set to **Enabled**, it prevents flushing the encryption keys when the user session is locked.

It is useful for software which could crash when accessing encrypted files, while the user session is locked.

On the other hand, if you intend to **disable** this option, think about it carefully. Indeed, there are some serious drawbacks to this action. For example, a hacker could steal the user encryption keys contained in the `hiberfil.sys` file by using the hibernate function in the operating system.

If a hacker breaks the session lock, encrypted files will be accessible without authentication (since encryption keys have not been flushed).

Skip system partition (already encrypted at disk level)

This option is enabled only when protection mode is set to **Full disk encryption and file encryption**.

If the option is set to **Enabled,** the path `|systemdrive|` will be encrypted by Full disk encryption but will not be protected by File encryption.

If the option is set to **Disabled,** the path `|systemdrive|` will be protected by Full disk encryption.
If the path is also included in **Encrypted zones,** then it will be encrypted twice: by File encryption and by Full disk encryption.

> ⚠️ **WARNING**
> Unencrypted zone rules have priority over other encryption rules.

Force user authentication

When this option is set to **Enabled**, the user is prompted to authenticate when opening a session so as to prevent him from creating unencrypted files.

Stealth mode

When this option is set to **Enabled**, file encryption is applied to the workstations but their users will not notice the encryption process in progress.

The agent will not display the following elements on the user's workstation:

- Right-click file encryption window.
- Encryption progress bar.
- Right-click menu (**Copy to an encrypted archive**).
- The lock icon 🔒 on encrypted files.

> ⚠️ **WARNING**
> You need to set the authentication mode to **Windows**.

Encrypted zones

This option is used to encrypt all the files in a specific folder.

You have to define the folders where users can store their files securely.

ℹ️ NOTE
The Administrator has to inform the users where they can store their files securely.
The encrypted zone with the most generic path should always appear last in the list of **Encrypted zones** so that the more specific rules are applied first.
Unencrypted zone rules have priority over other encryption rules.

ℹ️ NOTE
Zones that are considered vital for the proper running of the operating system cannot be encrypted. As a result, folders such as `C:\Windows\` and `C:\Program Files\` will be exempted from file encryption. The corresponding environment variables (`|systemroot|` and `|programfiles|` respectively) cannot be used in the file encryption policy. If you consider the data in these folders sensitive and require encryption, it may be preferable to encrypt the whole disk.

Environment variables

Environment variables make it easier to configure encrypted zones.

For example, you can enter `|userprofile|` to specify all individual user folders, rather than enter each individual folder one at a time.

Supported environment variables are the following:

- `|username|`
- `|systemdrive|`
- `|userprofile|`
- `|mydocuments|`

⚠️ WARNING
Environment variables, in particular `|username|` and `|userprofile|`, are dynamic. They change with each user session.
Let us consider the following situation:

- user1 logs on.
  The zone to be encrypted which is defined by the policy is:
  c :\documents and settings\utilisateur1
  (the environment variable is replaced by its value).

- user2 logs on after user1 on the same computer.
  The zone to be encrypted as defined in the policy is now:
  c :\documents and settings\user2
  and synchronization is launched.
  If user2 is allowed to access **c:\documents and settings\user1** (provided that file system permissions are granted and files are encrypted with a computer key), encryption will take place.

To prevent this, the administrator must define a user key for these types of folders.
For more information, see Environment variables.

Encryption key types

There are two encryption key types:

- The computer encryption key.
- The user encryption key.

Computer encryption key

The computer encryption key 🖥 is available to any user who has an encryption password for that particular computer.

This means that encrypted data is protected from theft and access by unauthorized users.

Each computer has only one computer key. The computer key is changed every time the Stormshield Endpoint Security Agent is installed so that each computer has a unique computer encryption key.

User encryption key

The user encryption key 👤 is unique to the user.

This means that if a file is encrypted by user "A", only user "A" can access the file.

When the user logs on for the first time with a password, Stormshield Endpoint Security creates a unique user key. The user key is a combination of the computer key and the user key with the user password.

Here are three typical situations:

- **Files encrypted by one key**:

    A file can be encrypted by only one key: a unique user key **or** the computer key.

- **User access to computer key**:

    Each user is able to access the computer key with his own password. Actually, the user password is used both for computer and user encryption keys. This is invisible to the user.

- **File access denied**:

    Access to encrypted files is denied when:

    ◦ The file has been encrypted with the user key of another user.

    ◦ No password authentication has been entered.

    ◦ There are several user sessions on a computer.

    ◦ The Stormshield Endpoint Security agent has been shut down.

    ◦ The administrator has disabled the encryption policy whereas files are still encrypted.

Unencrypted zones

You can use this option to prevent the encryption of unencryptable files.

Important applications that are initialized during computer start-up are not encrypted, namely:

- Windows Operating System files.
- System Volume Information.
- Stormshield Endpoint Security.

For more information on the list of applications exempted from encryption, see Files Exempted from Encryption.

⚠ **WARNING**

The following must also be exempted from encryption:

- **Any system file loaded during Windows startup**
Since files can be decrypted only after the user logs on, all files used during the boot-up sequence by services, drivers or the operating system must not be encrypted. This includes the desktop manager file currently selected.

- **Roaming profiles**
Access to encrypted files is denied until after encryption password authentication. Since Windows synchronization occurs before authentication, the roaming profile would still be encrypted and Windows synchronization would fail.

13.5.3 Full Disk Encryption Parameters

Full Disk Encryption Parameters enable you to control the following parameters:

- Partition encryption.
- Block-cipher mode of operation.
- Secure shredding before encryption.
- Number of secure erase cycles (before first encryption).
- Allow automatic restart.
- Single Sign-On (SSO).
- One-time recovery password.
- Use guest account.

🔑 **Full Disk Encryption Parameters**	
Full Disk Encryption	✅ Enabled
Partition encryption	System partition
Block-cipher mode of operation	CBC-Advanced
Secure shredding before encryption	❌ Disabled
Number of secure erase cycles	3
Allow automatic restart	❌ Disabled
Single Sign-On (SSO)	❌ Disabled
One-time recovery password	✅ Enabled
Use guest account	✅ Use challenge

Partition encryption

This option includes the following:

- **Partition system**

Only the system partition where the operating system of the computer is installed is encrypted.

- **All partitions**

All the partitions on the hard disk on which Stormshield Endpoint Security is installed are encrypted. Only master partitions are supported.

Block-cipher mode of operation

This option runs on blocks with a fixed length of 128 bits.

Since messages may be of any length and encrypting the same plain text by the same key usually generates the same output, various operating modes have been created.

These operating modes permit block ciphering to ensure confidentiality for messages whatever their length.

This option can be set to:

- **CBC** (Cipher Block Chaining)

  CBC is the most frequently used mode. Its main drawback is that encryption is sequential (the encrypted output of previous block is transmitted to next block) with no capability for parallel processing. Therefore the message must be stretched to a multiple of the cipher block size.

  Stormshield Endpoint Security uses CBC with 128-bit blocks for each 512-bit sector of the disk.

- **CBC Advanced**

Same as CBC mode except for including certain algorithmic rules such as complexity levels. For each encrypted block, an AES key is dynamically generated to prevent cryptanalysis.

Secure erasure

When this option is enabled, the disk is securely erased before the encryption process.

Secure erasure implies overwriting disk blocks to prevent data retrieval by unauthorized users. This is highly important when a laptop is stolen or left unattended.

Number of secure erase cycles

This option indicates the number of erase cycles to be performed to securely delete files and folders. The blocks on the disk are overwritten by the number of times set, with random data before encryption.

The more the number of erase cycles, the longer the synchronization.

> **ℹ️ NOTE**
> Professionals can retrieve information from almost any magnetic data carrier, even damaged ones.
> To delete a file permanently, the secure data erasure process performs several random data overwrites where the deleted file was stored.
> It is currently the only method which is valid to obliterate securely data on your disk. It makes it almost impossible to retrieve data via magnetic remanence.

Allow automatic restart

Console

This option allows automatic restart for remote maintenance without using encryption passwords.
After disabling Stormshield Endpoint Security's bootloader, you will reboot manually or via a script.
See table Built-in actions, line Encryption > Allow Automatic Restart.
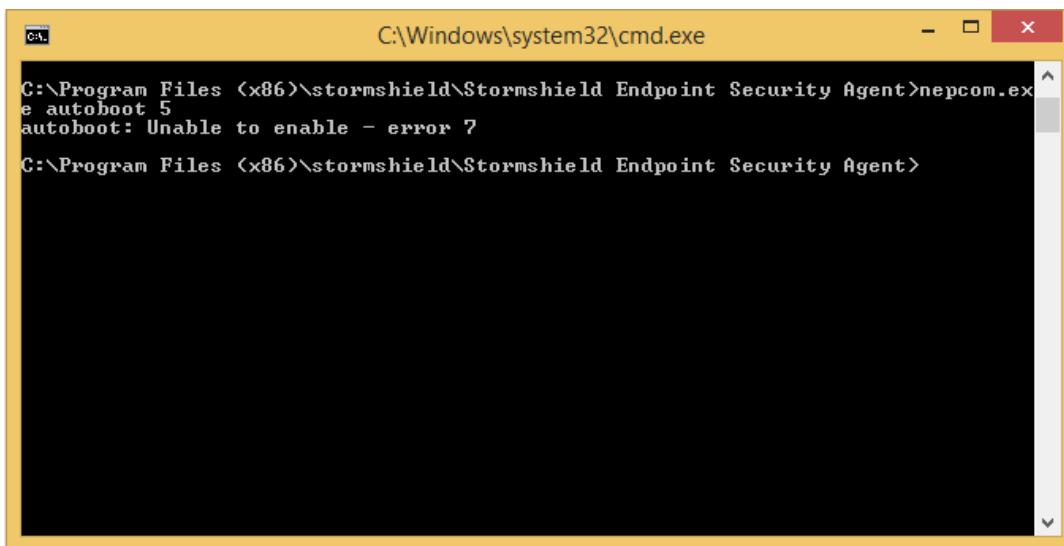
Agent

On the agent, the administrator may allow a predefined number of automatic restarts via `nepcom.exe`.

Prerequisites

To allow automatic restarts on the agent, you should enable **Allow automatic restart** on the console.

Otherwise, you will not be able to use `nepcom.exe` and the `Unable to enable` message will be displayed.
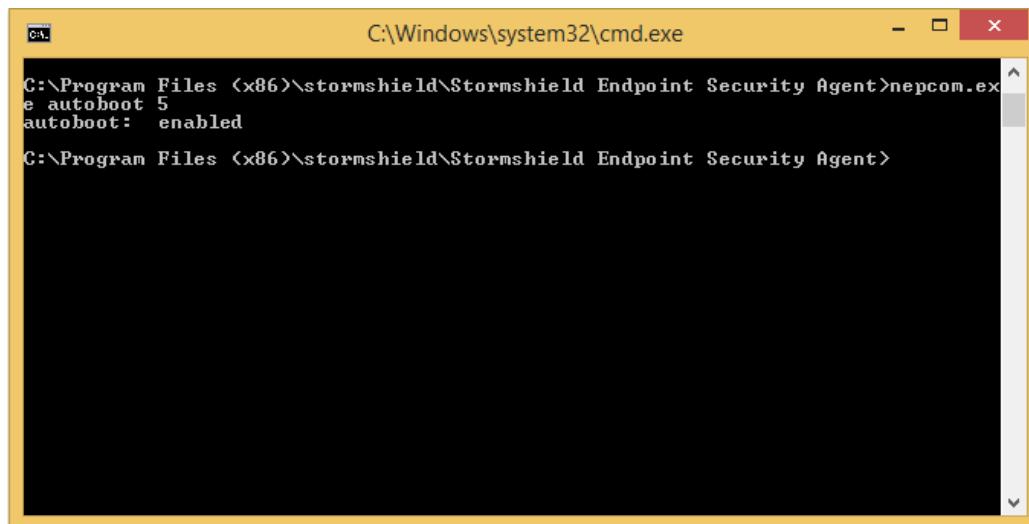
Procedure

To allow automatic restarts on the agent, follow the steps below:

1. Open a command prompt window.

2. Go to the Stormshield Endpoint Security agent directory.

3. Enter the following command:

   `nepcom.exe autoboot [number of automatic restarts allowed]`

   To check that the command has been enabled, the `enabled` message is displayed.
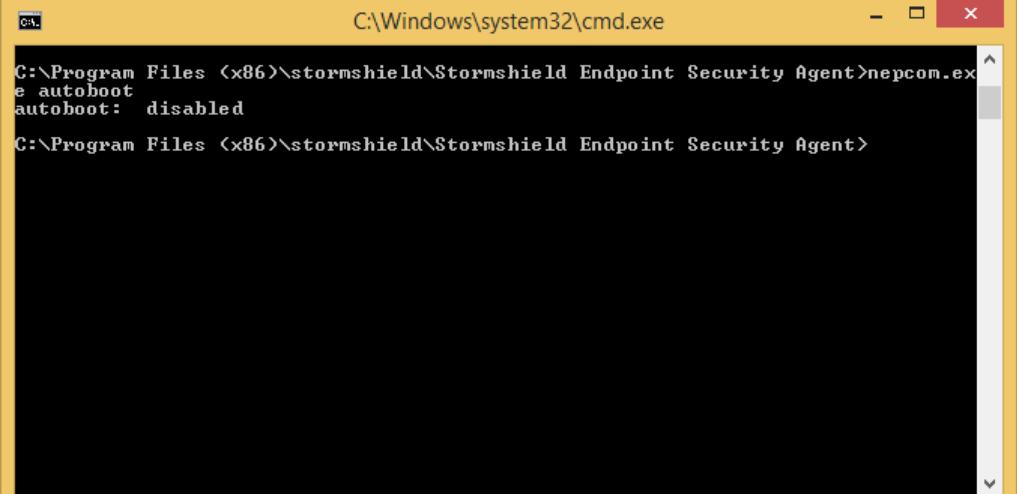
To disable automatic restarts on the agent, follow the steps below:

1. Open a command prompt window.

2. Go to the Stormshield Endpoint Security agent directory.

3. Enter the following command:

   `nepcom.exe autoboot`

To check that the command has been enabled, the `disabled` message is displayed.

Single Sign-On (SSO)

This option is used to combine two authentications (Encryption+Windows) for the main user.

When the user authenticates for the first time with his/her login and Windows password via Stormshield Endpoint Security authentication service, user authentication information will be encrypted with the encryption key and stored on the agent.

From now on, the user will **no longer** need to enter his/her login or Windows password as the agent has decrypted and sent this information to Stormshield Endpoint Security authentication service. The service will at present fill in automatically Windows account authentication details.

If the user changes his Windows password, he will follow the steps below:

- The user will proceed as usual under Windows in order to change his password.

- He/She will reboot his machine.

- He/She will enter his new Windows password when opening a new session so that Stormshield Endpoint Security will encrypt and store at agent level his new user password.

  If the user directly clicks OK (or enter his old password), the authentication process will be blocked. A window will indicate to the user that he must enter his new Windows password.

  On next session, the user will no longer need to enter his/her login or Windows password.

One-time recovery password

When the user authenticates with his recovery password, this option generates a new recovery password on next login.

Use guest account

This option is enabled by default. It is designed to create a temporary guest account. The guest account makes it possible to authenticate on the workstation without using the main user account.

- To define a guest account, right-click the Stormshield Endpoint Security ⊙ icon in the taskbar. Select **Full disk encryption**, and then **Create Guest Account**.

- To delete a guest account, right-click the Stormshield Endpoint Security ⊙ icon in the taskbar. Select **Full disk encryption**, and then **Remove Guest Account**.

- At machine startup, select **Guest** (F3) and enter the password for the guest account.

Available options are the following:

- Disabled.

- Use challenge.

- Never expires.

- With expiry date.
  If you select **With expiry date**, you have to set the **Maximum guest account age**.

For more information about challenges, see Administrator managing the challenge requests sent by the user.

13.6 Applying an encryption policy to an object of the directory

Encryption policies are applied to objects of the directory.

To apply an encryption policy to a directory object, follow the steps below:

1. Click the object in the **Environment** menu in the **Environment Manager** section.

2. Go to the *Policies linked* panel.

3. Select the encryption policy in the drop-down list in the **Encryption** category.

4. Click **Deploy to the environment**.
   This action must be performed each time you edit the encryption policy.

13.7 Recovery

13.7.1 Password recovery when using file encryption

Agent side

Overview

When the user creates a password, a **backup password** is automatically generated.

To replace a lost password, the user may contact the administrator. The administrator locates the backup password and sends it to the user.

Once the backup password is located, the administrator can copy, paste and send it by email to the user. The user can paste it directly into the password field.

The backup password works in the same way as the regular password.

To help the administrator locate the user's backup password by his user ID instead of his User Name, the user can proceed as described further on in Get IDs.

> ⚠ **WARNING**
> If Active Directory is not used, users working on different workstations can have the same **User Name** (example: administrator account), but **not** the same **User ID**.
> To locate a user by his user ID, ask the user to email it to the administrator.
> The **Domain** column only contains computer names.

Get IDs

To obtain his user ID, the user must perform the steps below:

1. Right-click the Stormshield Endpoint Security icon in the taskbar.

2. Select **Authentication > Get IDs**.

3. The user ID is displayed.
   Copy the **User ID** number and email it to the administrator.

   > ℹ **NOTE**
   > The user should change his backup password as soon as possible in order to use it as old password.

4. Paste the backup password sent by the administrator into the **Old password** field.
   Enter and confirm your new password.

   > ⚠ **WARNING**
   > If the user creates a new password on one computer and goes to another computer using the same account, the user must enter the new password and not the backup password.

Administrator side

Prerequisites

In order that the administrator can search for backup passwords, **Roles** > **Permissions** > **Decrypt data on hard disk** must be set to Authorized.
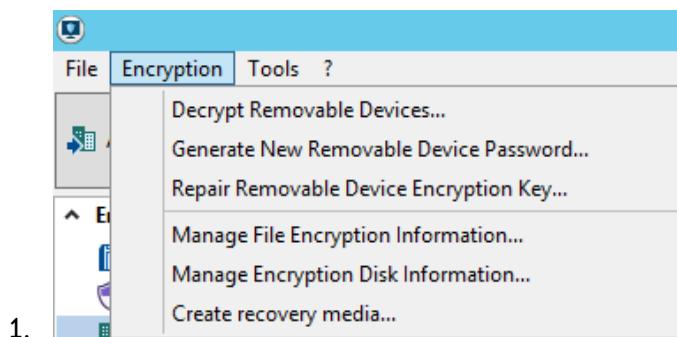
> ℹ **NOTE**
> The **Roles** menu is used to create the roles assigned to the SES console users.

Backup password recovery

To recover the backup password, you must follow the steps below:

1. Select **Encryption > Manage File Encryption Information**.

1.

2. Enter the password for the console certificate.

   The **Manage File Encryption Information** window is displayed.

   > **NOTE**
   > If you receive an error message, the console has not been correctly configured.
   > Check that console certificate paths are correct.

3. Locate the User Name in the list of **Active Keys**.

   For long lists, you can use the **Search** field on the top right to locate the name quickly.

4. Send the **Backup Password** to the user.

Change secondary authentication password

To change the secondary password used for encryption by the user, the administrator must follow the steps below:

1. Select **Encryption > Manage File Encryption Information**.

2. Enter the password for the console certificate.

   The **Manage File Encryption Information** window is displayed.

3. Select **Change password**.

4. Enter and confirm the new password.

5. Click **OK**.

   > **NOTE**
   > To activate the new password, the user must first log off from the system and then log in.
   > For the encryption process to take effect, the user must enter the new secondary
   > authentication password after Windows startup.
   > The Stormshield Endpoint Security agent must be connected.
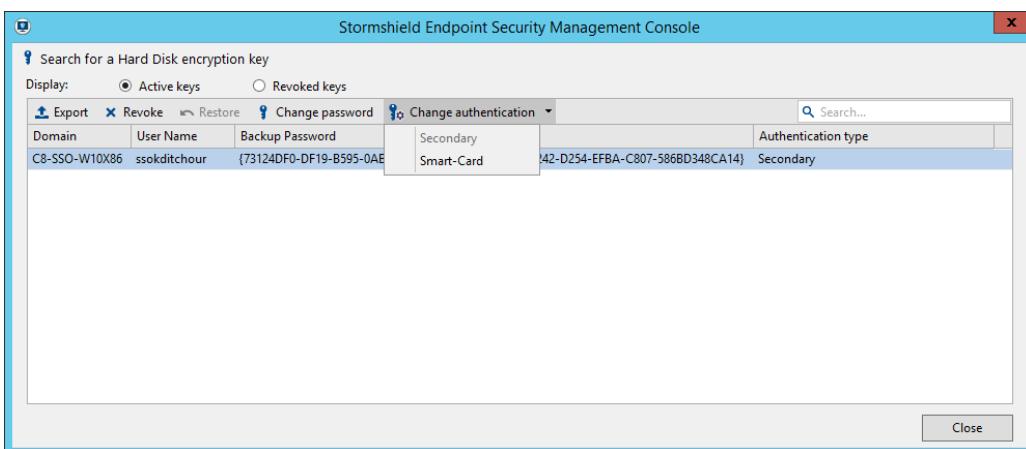
Change authentication type

To change the authentication type of the agent, you must follow the steps below:

1. Click on the user name to highlight it.

2. Click **Change authentication** and select the authentication type from the dropdown menu.

> **NOTE**
> The encryption policy assigned to the agent must be configured so as to have the same authentication type as the one defined for the user.

3. Enter the required information.

4. Validate your modifications.

5. Deploy changes to the environment.

> **NOTE**
> After the agent reconnects to the server and receives new information, the user must log off and log on again to apply the new authentication type.

Change to Smart-Card authentication

To change the authentication type of the agent, you must follow the steps below:

1. Click on the user name to highlight it.

2. Click **Change authentication** and select **Smart-Card** type from the dropdown menu.

3. Define the following parameters:

   ◦ Select the CSP.

   ◦ Select the certificate.

   ◦ Enter the PIN code.

4. Click **OK**.

5. Deploy changes to the environment.

> **NOTE**
> After the agent reconnects to the server and receives new information, the user must log off and log on again to apply the new authentication type.
> Upon login, Stormshield Endpoint Security prompts the user to insert the smart-card and enter the PIN code (provided by the CSP).

Revoking and restoring user keys

There are two types of user keys in **Manage File Encryption Information**:

• **Active keys:**

They are the keys belonging to active users who can authenticate themselves.

• **Revoked keys:**

They are the keys belonging to revoked users. The administrator can reactivate revoked keys.

> **ⓘ NOTE**
> A user with a revoked key will not be able to access encrypted files. Authentication will be rejected.

To revoke or restore user keys, you must follow the steps below:

1. Search for a user using the **Search** field and click **Revoke**.

2. The user is removed from the list of **Active keys**. On the other hand, his name will appear on the list of **Revoked keys**.
   To check this out, click the **Revoked keys** radio button.

3. Several actions are available from the toolbar:

   - **Export** the user key as a `[RecoveryKey].srk` file.

   - **Delete** the user key.

   - **Restore** the user key (Revoked key > Active key).

   - **Change user password**.

   - **Change user authentication**.

13.7.2 Recovering data from encrypted files (decryption)

You may need to decrypt some or all of the data on a hard disk.

Examples:

- When a user leaves the company.

- When data is to recovered from a damaged hard disk.

Recovery keyring

If you need to decrypt more than one hard disk, you can create a recovery key ring.
The recovery keyring is a file that can be copied onto a USB key and which can be used to manually decrypt each computer in turn.

To create a recovery keyring, see Decrypting data manually .

In Step 3 of the manual data decryption procedure, select the user names that you want to include in the recovery keyring.
You can then rename the file (if necessary), and export it to a USB key.

> **ⓘ NOTE**
> The recovery key ring includes all the keys of the computers used by selected users.

Decrypting data manually

Administrator procedure

To decrypt data manually, follow the steps below:

1. Select **Encryption > Manage File Encryption Information**.

2. Enter the password for the console certificate.

   The **Manage File Encryption Information** window is displayed.

> **ⓘ NOTE**
> If you receive an error message, the console has not been correctly configured.

3. Locate the user name in the list.

   For long lists, you can use the **Search** field to locate the name quickly.

   You can select multiple user names to create a key ring.

   For more information, see the section Recovery keyring .

   > **ⓘ NOTE**
   > If Active Directory is not used, users working on different workstations can have the same **User Name** (example: administrator account), but not the same **User ID**.
   > To locate a user by his user ID, ask the user to email it to you.
   > For more information, see the section Recovery.

4. After selecting the User Names (or User IDs), click **Export**.

5. Enter the path and file name.

   The file is saved as a [RecoveryKey].`srk` file which contains the keys used for file recovery.

   `SRK` files can be exported from the console and used on the Stormshield Endpoint Security Agent.

   For more information, see section Agent side or section Recovering data encrypted via the data encryption feature of chapter SURT.

   The file can be saved onto a USB key or another server.
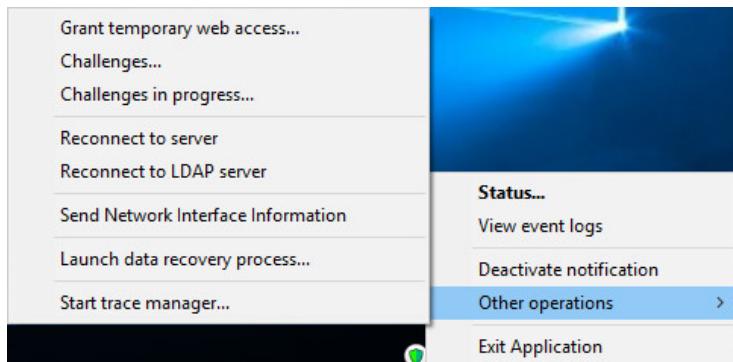
   > **⚠ WARNING**
   > It is highly recommended that the **SRK** file be stored in a secure location whose access should be reserved for authorized personnel (administrators).

Agent side

To decrypt data manually, follow the steps below:

1. Right-click the Stormshield Endpoint Security icon in the taskbar.

2. Select **Other operations > Launch data recovery process**.

3. In the **Encryption key file** field, enter the path and filename of the recovery key or click directly the Browse button [▾] .

   Use the **Folder to decrypt** field if you need to decrypt one folder at a time (Example: if you perform data recovery on a hard disk other than your computer HD).

4. Restart the computer.

   The decryption process begins when the computer restarts.

> ⚠️ **WARNING**
> If the encryption policy was not removed beforehand, the encryption policy is applied once again when the agent restarts in order to reencrypt files.
> The user can go on working during the recovery process. Decryption continues even when the computer is locked.
> If you repeat Step 1 to launch the data recovery process before the Stormshield Endpoint Security agent has restarted, you will be asked if you want to cancel data recovery **or** perform another data recovery process.

Automatic decryption

To achieve a successful automatic decryption process:

1. The Stormshield Endpoint Security agent must be able to connect to the Stormshield Endpoint Security server.

2. In the dynamic agent configuration, **Stop agent** must be set to **Allowed**.

3. In the server configuration, in the **Encryption** part of the policy edition panel:

   - The **Decrypt data at uninstallation** option must be set to **Enabled**.

   - The uninstall date must fall between **Start date of allow uninstall** and **End date of allow uninstall**.

   > ⚠️ **WARNING**
   > Only files encrypted with the **computer key** are recovered during automatic decryption. For files encrypted with a user key, you must perform one of the following:
   >
   > - Perform a manual recovery.
   >
   > - Reinstall the agent.
   >
   > - Transfer the files encrypted with a user key into a folder encrypted with a computer key.
   >
   > - Use SURT to decrypt files after uninstalling Stormshield Endpoint Security if the user does not wish to install the Stormshield Endpoint Security agent again.

If the **Decrypt data at uninstallation** parameter is **enabled** in the encryption policy, the decryption process begins automatically when the user runs the `Srend.exe` file to uninstall the Stormshield Endpoint Security agent.

During automatic decryption, it is not necessary to restart the computer if no user has logged in previously (**example**: when uninstalling with *Active Directory GPO*).
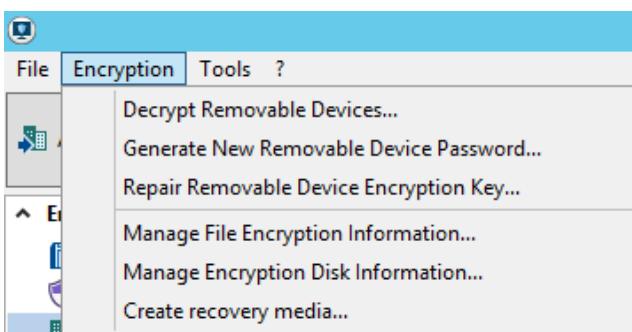
However, if the user is currently logged in or has logged in previously (with no reboot), then the computer must be restarted. The user will be prompted to restart the computer.

13.7.3 Password recovery when using full disk encryption

Recovery procedure
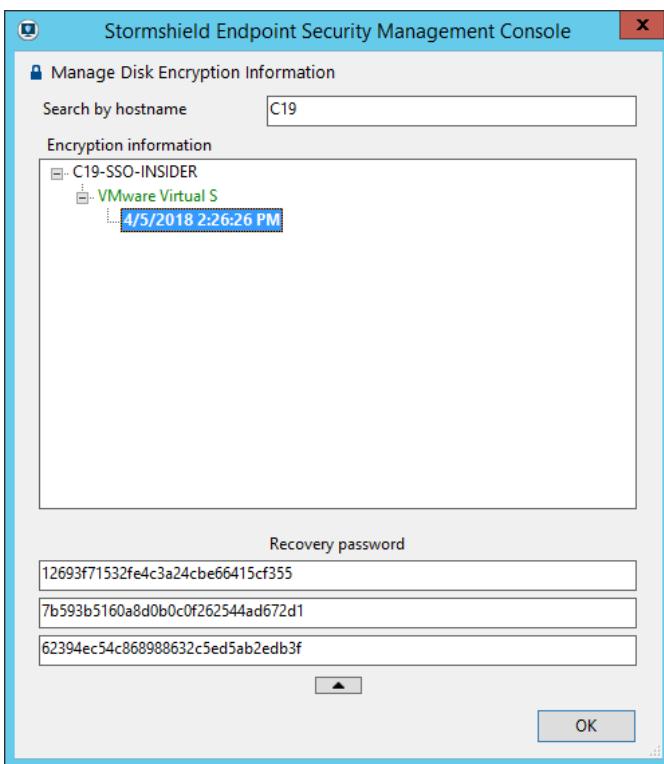
To access the recovery password when using full disk encryption, the user must follow the steps below:

1. Go to **Encryption > Manage Encryption Disk Information**.

2. Enter the password for the console certificate.

3. The encrypted disks of the agent are detected automatically and listed in a tree structure.

    To locate a disk or an encrypted system, use the Search by hostname field.

4. Click the date under the disk name. The recovery password is displayed in the **Recovery password** field.

    This key is sent to the agent by email or telephone in order to recover encrypted disk data.
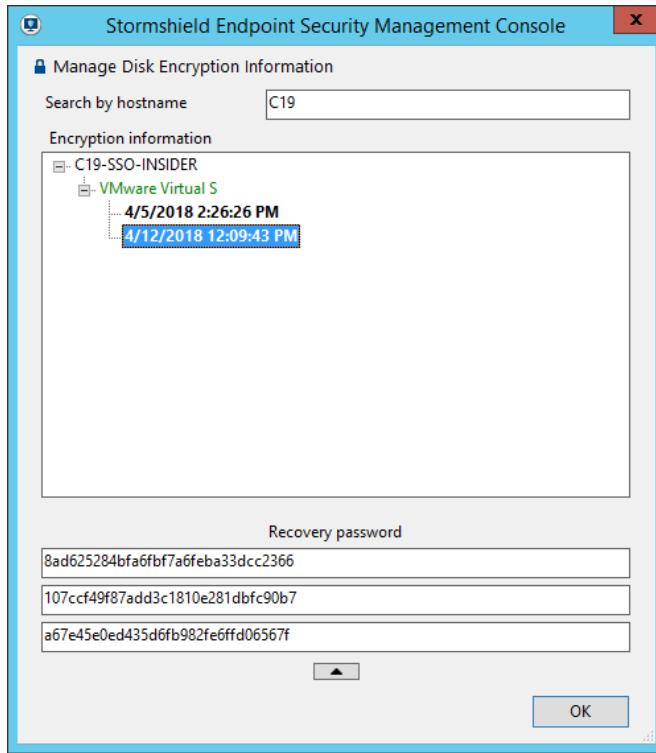
> **ⓘ NOTE**
> If several dates are associated with a given disk, it is recommended to use the recovery password located under the most recent date.
> Should a problem arise, the former recovery dates are kept in the list for reference.

> **ⓘ NOTE**
> If the administrator has enabled **One-time recovery password** in the encryption policy, and if the user cannot connect to the Stormshield Endpoint Security server, his recovery password will not be automatically updated. The administrator will send the user an old recovery password that will remain valid until next connection to the server.

Password change

Password change via the Stormshield Endpoint Security agent

1. On the agent computer:

   - Right-click the Stormshield Endpoint Security ⬡ icon in the taskbar.
   - Select **Full disk encryption > Change your password**.

2. In the window, enter the **Old password**.
   If you do not remember your old password, enter the recovery password that was sent by your administrator.
   If you check the **Use recovery password** box, the recovery password will be displayed in clear text.

   If you do not check the **Use recovery password** box, the recovery password will be automatically converted into QWERTY mode.

   Paste the recovery password sent by the administrator into the **Old password** field.

3. Enter and confirm the new password.

4. Click **OK**.

Password change upon startup

If you do not remember your user password, you can start the computer using the recovery password (Admin).

To do so, follow the steps below:

1. Press **F2** (admin).

2. Enter the recovery password in the prompt window.

3. Press Enter.

13.7.4 Recovering an encrypted disk on removable media

The administrator performs a full-disk encryption data recovery via CD if the encrypted disk did not launch properly.

Recovery is mainly used for disk decryption and when the machine cannot be started under normal conditions.
Examples: lost password or system crash even when booting in Safe Mode.

The media (CD-ROM or USB key) will enable users to:

• Decrypt data on the hard disk and delete the system's boot loader.

• Change passwords.
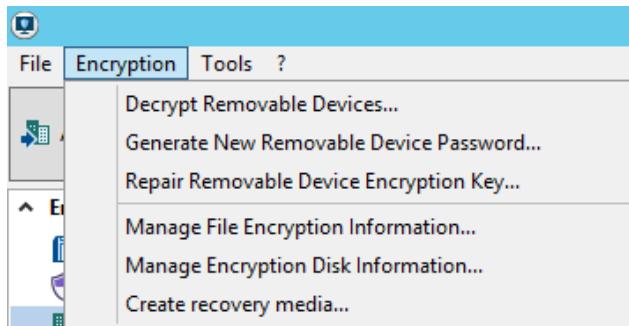
Creating removable media (Windows Preinstallation Environment)

Removable media can be created on the console in order to launch disk recovery on the agent's computer.
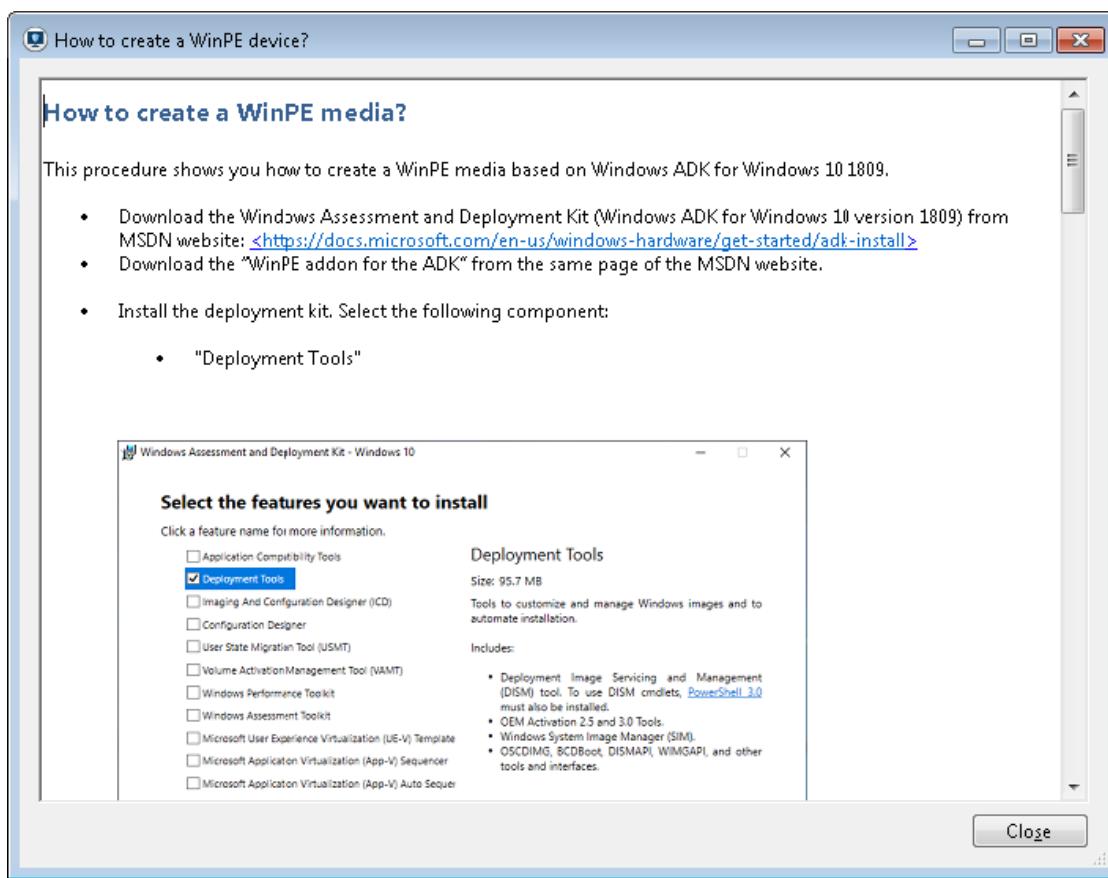
They must be created via the Windows Preinstallation Environment (WinPE). This tool is a lightweight version of Windows that can be booted via CD/DVD, USB keys or external drives. The recovery process is lauched via WinPE.

To create removable media, follow the steps below in the Stormshield Endpoint Security console:

1. Go to **Encryption > Create recovery media**.
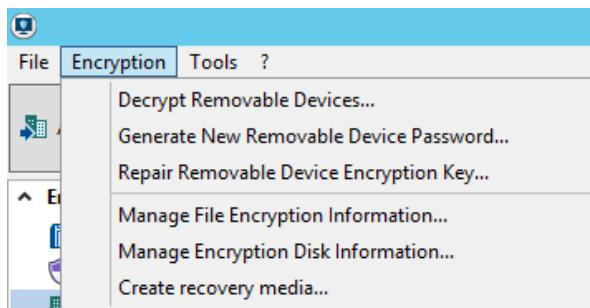
2. Click on the **How to create a WinPE device?** button to open the WinPE media creation wizard and follow the instructions provided.
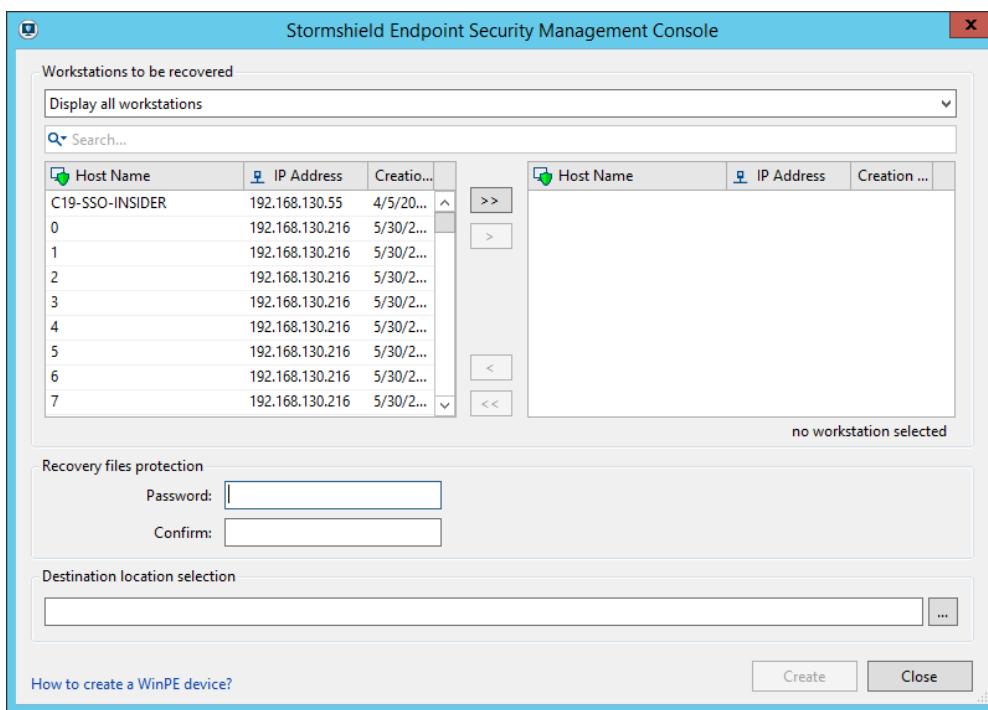
Create recovery media

To retrieve recovery information from the disk(s) to be decrypted, perform the following operations:

1. Go to **Encryption > Create recovery media**.

2. The following window opens. Machines can be filtered by Active Directory or by groups.

3. Select the workstations(s) to be decrypted.

4. In the **Recovery files protection** section, enter a password and confirm it to protect the recovery media.

    > ⚠️ **WARNING**
    > The recovery media will then grant access to all corporate data stored on exported workstations. Unauthorized persons might have access to this media and use it to steal company information. Extreme security measures must therefore be taken and applied to the CD. The strength of the password chosen when creating the recovery media is verified: it must be High.
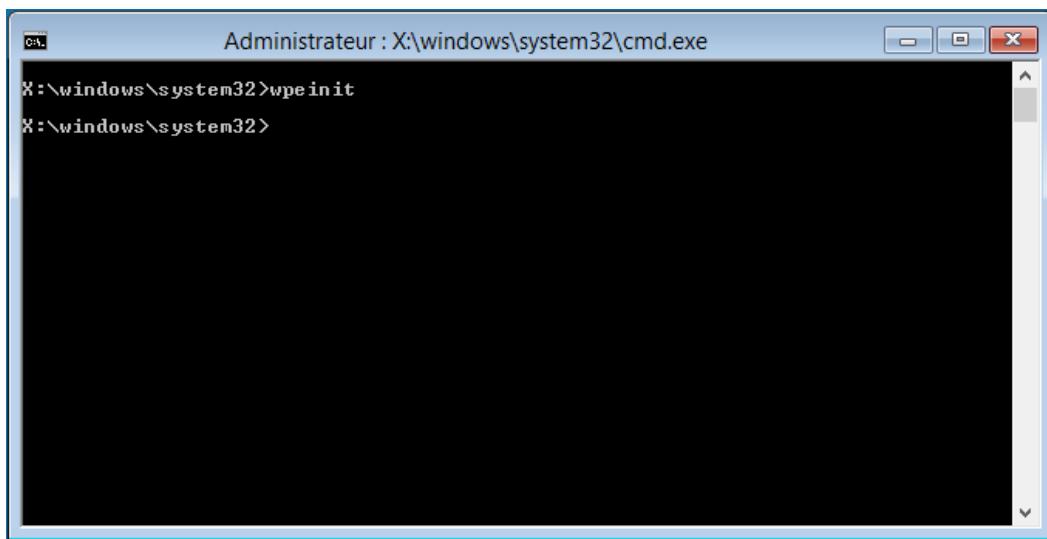
5. Select the target location of the files relating to the recovery process.

6. Click the **Create** button.

Starting the recovery manager

It is recommended to decrypt files on the agent workstation using the removable media recovery tool if encryption fails. The encryption process may fail due to a damaged block.

To repair a machine via removable media, the user must follow the steps below:
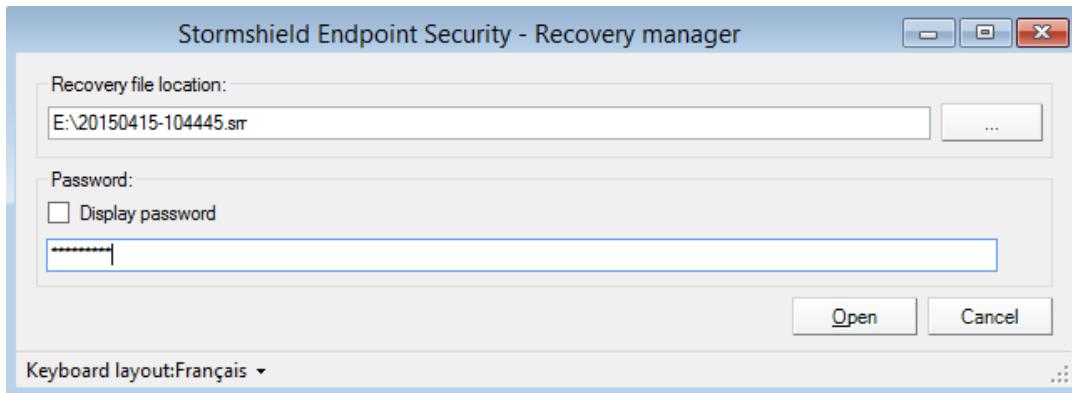
1. Insert the WinPE media.

2. Insert the recovery media.

3. Boot the workstation on WinPE.

4. The following command prompt will then appear:
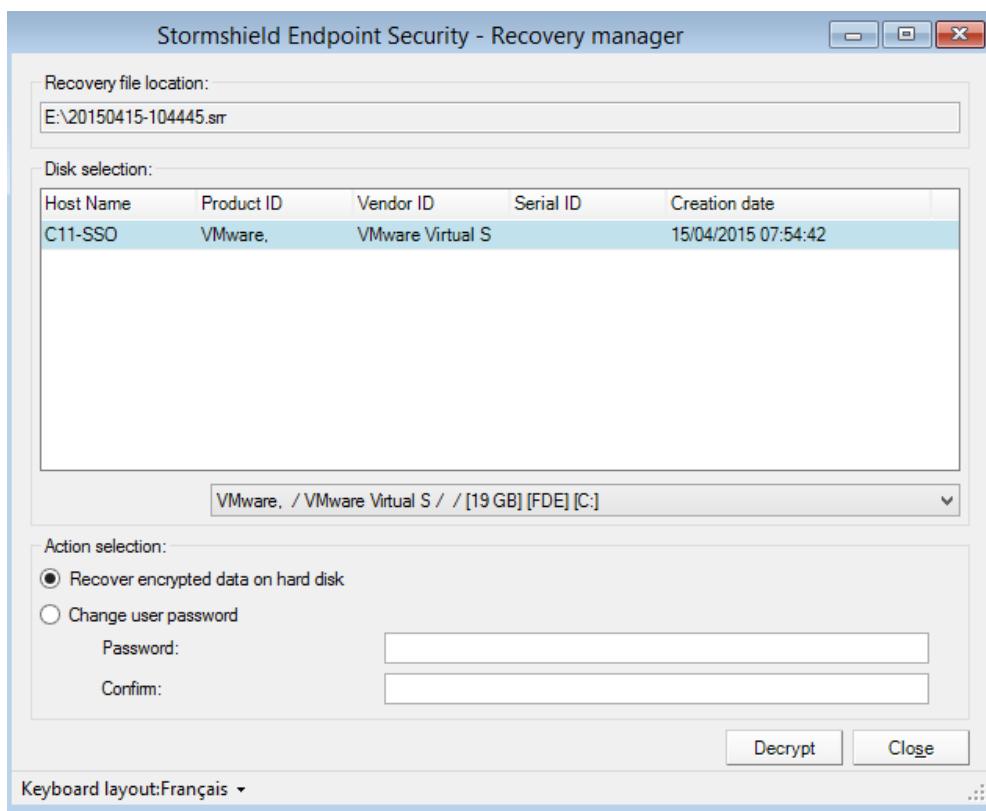
> **ⓘ NOTE**
> To quickly find out which drive corresponds to the USB key:
>
> - Execute the *diskpart* command.
> - Type "list volume".
> - The whole list of drives will appear (letter of the drive, name of the media, file system used, size, etc).
> - Type "exit" and press Enter to get out of the diskpart command.

5. Launch NepRecovery.exe through the recovery media:

6. The disk will be automatically selected, and two actions are offered (recovery of encrypted data or change of user password);

- Recover encrypted data on hard disk

You will be prompted to start the recovery by clicking on **Decrypt** if you selected **Recover encrypted data on hard disk** in the previous window.

A confirmation message will appear. Click on **Yes** to start decrypting the disk. The recovery process starts.

- Change user password

If the user forgets the encryption password, Stormshield Endpoint Security offers an option to guide the user through the password change process.

To change the encryption password, the user must follow the steps below:

1. Select **Change your user password**.
2. Enter the new encryption password (Standard force as a minimum).
3. Confirm the new encryption password.

The user will be notified if the password was changed successfully.

13.8 Uninstalling Stormshield Endpoint Security agents

13.8.1 Decryption before uninstallation

When agents are uninstalled, Stormshield Endpoint Security must decrypt the folders and files stored on the agent's hard disk, so that the users can access their data after software removal.

Multiple agents can be uninstalled at the same time using Group Policy Objects (GPO), without any need for user intervention.

However, in order to use GPOs in the **Environment Manager** section, parameters must be configured as follows:

- The agent must be connected to the server.

- The **Decrypt data at uninstallation** option must be set to **Enabled**.

- Stop Agent must be allowed in the configurations.

- The Start date of allow uninstall and End date of allow uninstall must be specified.

  During this period, agents can request the encryption key which enables Stormshield Endpoint Security to decrypt the hard disk without the need for user authentication.

Only files encrypted with the **computer key** are recovered during automatic decryption.

To recover files encrypted with a **user key**, you must perform one of the following actions:

- Perform a manual recovery. For more information, see the section Decrypting data manually
  .

- Reinstall the agent.

- Use the SURT **Data recovery** feature. For more information, see Recovering data encrypted via the data encryption feature.

  > **ⓘ NOTE**
  > If the automatic decryption process is launched and the recovery procedure fails, the **Stormshield Endpoint Security agent** will be uninstalled anyway. It is then necessary to decrypt files manually.

13.9 Changing a user account on a machine

After changing a user account on a machine, check that the Start date of allow uninstall and the End date of allow uninstall cover the time period when the user first logs on.

This is to ensure that:

- The agent will be able to request the server encryption key.

- The user will be able to access encryption features.

To maintain encryption security, keep the allow uninstall period to a minimum.

14. SURT

14.1 Overview

> **🛈 NOTE**
> A user who does not have Stormshield Endpoint Security installed on his computer may download Stormshield Endpoint Security Express Encryption free of charge from MyStormshield website.

SURT (also called Stormshield Endpoint Security **Express Encryption**) is a portable software that can be used without having to install it on your computer.
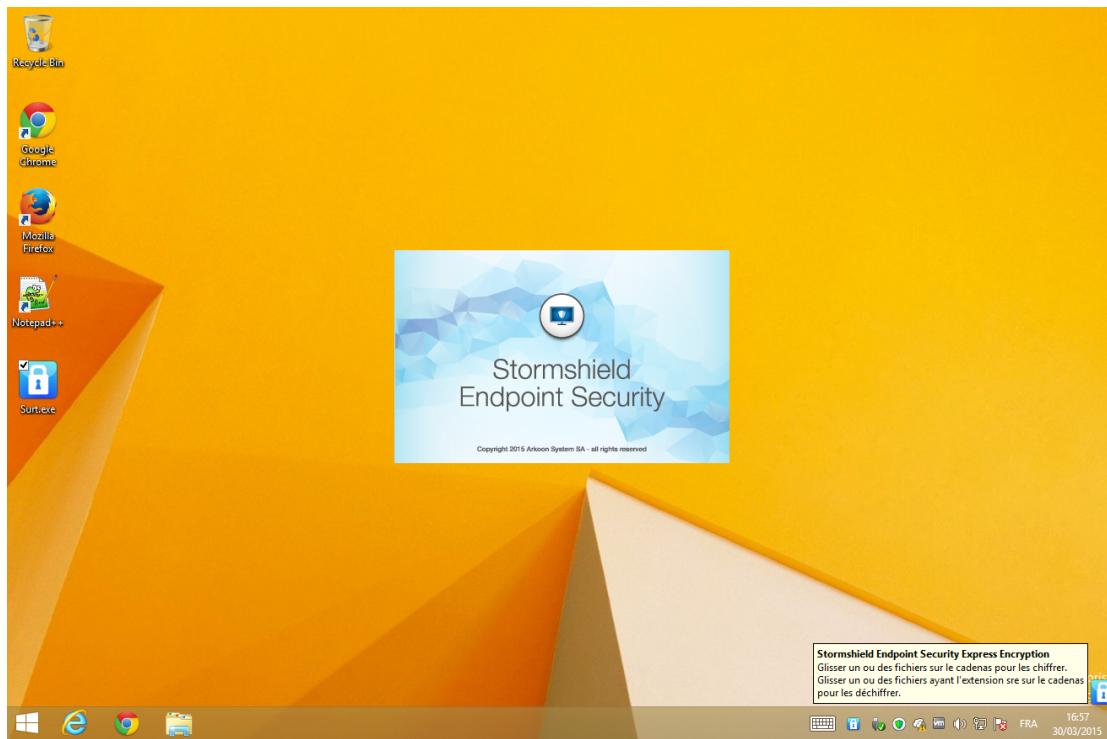
SURT is associated with the file extension `.sre`. Therefore, when you copy it from another location to your computer, it will be displayed as `Surt.exe`.

If you double-click SURT, the following window will be displayed including the icons below:

- Icon in the taskbar: 🔒.

- Desktop overlay: 🔒.

- Executable icon: 🔒.

14.2 Encrypting a file

14.2.1 Procedure

To encrypt a file, follow the steps below:

1. Double-click the `surt.exe` icon on your desktop or in the location in which you copied SURT.

    A startup screen will be displayed and another 🔒 icon will appear on the lower right corner of your Windows desktop.

2. Drag the desired file to the icon 🔒.

3. Specify the encryption parameters:
    - Password to access the encrypted archive.
    - Confirm the password.
    - Encrypted archive name.
    - Archive destination:
        - Within the same folder.
        - On my desktop.
        - In my documents.
        - Browse for a location.

    > **ℹ️ NOTE**
    > The **Generate an encrypted archive** box is checked by default.

4. You may write directly the encrypted archive onto the CD-ROM.

    To do so, check the **Write to a CD/DVD** box and specify the following settings:
    - Recorder name.
    - Media name.
    - Other options:
        - Erase CD/DVD.
        - Eject CD/DVD after burning.
        - Add Stormshield Endpoint Security Express Encryption to the media.

5. Click **OK**.

6. If you have checked the **Write to a CD/DVD** box, the burning process starts immediately.

7. When the burning process is completed, a new window is displayed.
   Click **OK**.

14.3 Decrypting a file

14.3.1 Procedure

To decrypt a file, follow the steps below:
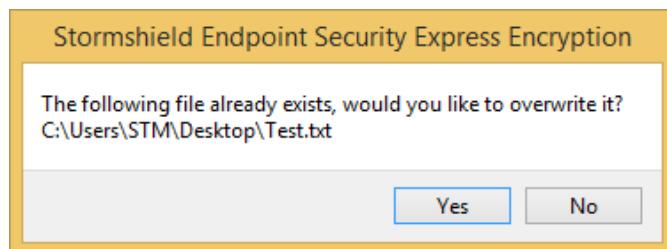
1. Drag and drop the file to be decrypted on the desktop overlay .
   The following window is displayed:
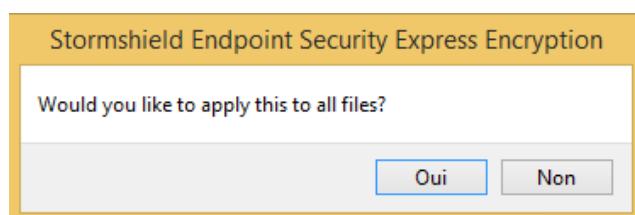
2. Enter the password of the encrypted file.

3. Specify the decrypted file path.

4. Click **OK**.

i NOTE

If you want to overwrite an already existing file in the same location, click **Yes**.

The following message is displayed to apply overwrite to all files.

14.3.2 Progress bar

The progress bar is displayed during file encryption only when:
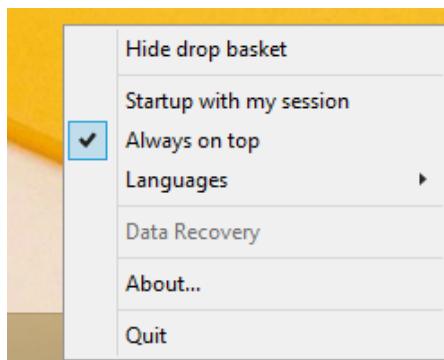
- The user drags and drops more than one file at a time.
- The file that the user is encrypting is bulky.

14.4 Reference menu

14.4.1 Graphical interface

The Stormshield Endpoint Security Express Encryption reference menu is displayed when the user right-clicks the taskbar icon 🔐.

14.4.2 Options

Reference menu options are the following:

- **Hide/Show drop basket**:

  If **Hide drop basket** is enabled, the icon 🔒 is displayed only in the taskbar.

  If **Show drop basket** is enabled, the icon 🔒 is displayed on the desktop.

- **Startup with my session**:

  This option automatically starts Stormshield Endpoint Security Express Encryption during Windows login.

- **Always on top**:

  This option keeps the icon 🔒 on top of all running applications.

- **Languages**:

  This option sets the language used (French, English, Spanish or Portuguese).

- **Data recovery**:

  This option recovers the encrypted files created with the data encryption feature on the management console.

  > 🛈 **NOTE**
  > To recover encrypted files created with the data encryption feature on the management console, the user must start his computer in **SAFE** mode.
  > If the user wishes to be in NORMAL mode, the Stormshield Endpoint Security agent must be uninstalled.
  > For more information about data recovery, see Recovering data encrypted via the data encryption feature.

- **About**:

  This option shows the software version and copyright information.

- **Quit**:

  This option exits the application.

14.5 Removable device encryption and SURT

14.5.1 Removable device encryption settings

On the management console, SURT is set to **Allowed** or **Denied** in the security policy edition window, under the **Removable Devices** category in the **Group Settings** panel.

Removable Devices / Default Group

Group Settings	
Device Type	Mass storage
Default access rights	Denied
Audit	☒ Deactivated
File encryption	Disabled
Access right if encryption is cancelled	Read
Stand-alone decryption tool (SURT)	
USB Settings	✅ Allowed
Removable devices enrollment	☒ Denied

14.5.2 SURT settings

SURT settings are the following:

- **Allowed:**

The user can encrypt and decrypt data on removable devices.

The executable file `SURT.exe` will be automatically copied onto the USB key.
This way, any attempt to replace the `SURT.exe` by a hacked SURT file will be countered as a new version of SURT.exe will overwrite the hacked file.

- **Denied**:

The user cannot use SURT to encrypt or decrypt data on removable devices.

14.5.3 Removable device encrypted with the agent and decrypted with SURT

SURT allows decrypting removable devices encrypted with the Stormshield Endpoint Security agent. On a workstation without the Stormshield Endpoint Security agent, if an encrypted removable device is plugged, the following window displays:

Enter the password to decrypt data on the removable device. The **Default action to perform during decryption** option allows defining the application default behavior when decrypting data. If it is not checked, the application will ask the user what to do on each file. In this case, the following window displays:

Options are:

- **Replace original file**: decrypted files overwrite source files. When the device is ejected, the application encrypts again files which have been decrypted.

- **Decrypt file to my desktop**: the file is decrypted on the desktop. The source file is not altered. However modifications done in the decrypted file are not repeated on the removable device when it is ejected.

- **Decrypt file to my documents**: the file is decrypted in the personal documents of the connected user. The source file is not altered. However modifications done in the decrypted file are not repeated on the removable device when it is ejected.

- **Browse for a location**: the application asks the user which is the destination folder of the file which is currently decrypted. In this case too, the source file is not altered. However modifications done in the decrypted file are not repeated on the removable device when it is ejected.

When the authentication succeeds, the following window displays:

The ✏️ icon displays under the 🔒 icon.

To decrypt a file, open a file explorer on the removable device and drag it on the 🔒 icon.

The ✏️ icon represents the encrypted device you can use from SURT. By right-clicking the icon, you can:

- open an explorer on the drive in order to browse the content.

- eject the device in a secure manner.

To guarantee data integrity, you MUST eject the removable device from SURT. In addition, this allows encrypting data previously decrypted via SURT when the **Replace original file** option has been selected.

When you eject the removable device, the following window displays:

14.6 Recovering data encrypted via the data encryption feature

14.6.1 Prerequisites

To recover encrypted files created with the data encryption feature on the management console, the user must start his computer in **SAFE** mode.
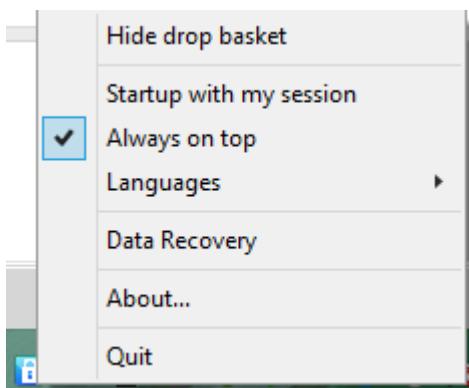
> 🛈 **NOTE**
> If the user wishes to be in **NORMAL** mode, the Stormshield Endpoint Security agent must be uninstalled.

A recovery key provided by the administrator from the Stormshield Endpoint Security management console is also required. For more information, see section Recovery.
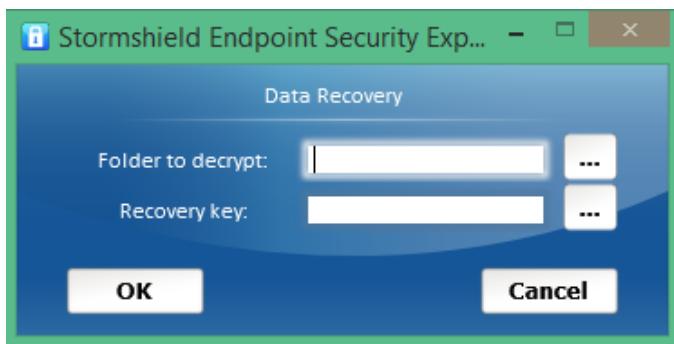
14.6.2 Procedure

To recover data encrypted via the data encryption feature, follow the steps below:

1.   Right-click the icon 🛡 and select **Data Recovery**.

2.   The following window is displayed.

Specify the settings using the Browse button ⋯ .

- ° The name and path of the folder to decrypt.
- ° The path of the recovery key file sent by the administrator.

3. Click **OK**.
   Folder decryption starts.

4. After decryption, a window notifies the user that the process is completed.

5. Reboot in NORMAL mode.

15. Activity Monitoring

15.1 Overview

Stormshield Endpoint Security is used to control, monitor and record activity on workstations via the following features located in the **Environment Manager**, **Monitoring** and **Console Manager** sections:

- Agent Monitoring.
- Dashboard.
- Logs.
- Log Manager.
- Console Monitoring.

> **NOTE**
> If you are using Stormshield Endpoint Security for the first time, it is unlikely that any event captured by the Stormshield Endpoint Security agents has been recorded in the reporting database.
> In this case, the functions covered in this chapter will of course be available but without any data.

15.2 Agent monitoring

15.2.1 Graphical interface

Display options

Agent monitoring display options (**Monitoring** > **Agents** menu) in the menu bar are the following:

- **Real-Time:**

  Continuous display of monitoring information which is updated as the information is refreshed.

  By default, monitoring information is automatically updated according to the **Agent monitoring refresh time** (sec.) set in **Configuration** in the **Console** section.

- **Review:**

  Display of monitoring information without automatic update.

  Click **Refresh** when you want to update information.

- **Refresh:**

  Forces a refresh of monitoring information (displayed in real-time mode or review).

- **Active Directory:**

  Used to determine which machines do not have the Stormshield Endpoint Security agent software installed.

- **Export:**

  Used to export agents to a file in the XML format.

  - Export all: all agents are exported.
  - Export selected agents: selected agents are exported.

- Export displayed agents: only the agents displayed by the filter are exported.

Details

In the **Monitoring / Agents** area, each line displays the following information on the agent selected:

- **Host Name**.

- **OS**.

- **Agent identifier**.

  This column is hidden by default. It allows refining the search and filter on agents.

- **IP Address**.

- **Net Mask:**

  Sub-network mask.

- **Option:**

  Packages of the product.

- **AD Name:**

  Full hostname in the Active Directory domain.

- **Agent Version:**

  Version number of the Stormshield Endpoint Security agent.

- **Config. Status :**

  The configuration status can be valid or invalid:

  - **Valid** indicates that the configuration is up-to-date.

  - **Invalid** indicates that the administrator has sent a new configuration but that the latter has not yet been received by the agent.

- **Policies:**

  Name of the applied policy and its version number.

- **Configuration:**

  Name of the applied configuration and its version number.

- **Last synchronization:**

  Date and time when the agent applied the last configuration and/or the last policy it received from the server. This date is directly related to the **Policy** and **Configuration** columns.

- **Agent Status:**

  - Connected.

  - Disconnected.

  - Warning.

  - StandBy.

  - Unknown.

◦ License exceeded.

- **Recommendation:**

Status of a variable (used in Test scripts and Action scripts) which can be used by TNC clients (Trusted Network Connect) such as Odyssey Access Clients on Juniper Networks (R).

Available options are:

◦ Allow.

◦ Isolate.

◦ No access.

◦ No recommendation.

No recommendation is enabled by default and works only in Juniper server mode.

> ### NOTE
> Should a driver be missing (heimdall, loki, thor), the value applied by default will be **No recommendation**. It will be impossible to modify this value until the next reboot of the agent. Besides, drivers will have to be installed properly.

- **First Connection:**

The first time the agent and the server communicated with each other.

- **Last Connection:**

The most recent time the agent and the server communicated with each other.

Filters

The administrator can filter agents using the following elements:

- **Status**:

◦ Connected agents.

◦ Agents in StandBy mode.

◦ Agents in Warning mode.

◦ Disconnected agents.

◦ Agents with an unknown status.

◦ License exceeded.

- **Servers**.

- **Options**:

◦ Professional Edition.

◦ Secure Edition.

◦ Server-Side Edition.

- **Agent Version**.

Right-click menu

Merge

The administrator can merge machine identifiers to display only one entry concerning the monitoring of an agent. This is designed to update the number of licenses effectively used.

To do so, the administrator will right-click in the agent list to display the following options:

- **Selected**:

  The entries selected by the administrator will be merged. The administrator must select at least two entries to enable this option.

- **By hostname**:

  All the entries on the same machine will be merged. The fusion by hostname applies to the entire agent list.

- **By AD name**:

  All the entries having the same AD name will be merged. The fusion by AD name applies to the entire agent list.

Remove

The administrator can delete the status history of an agent. If the agent is no longer present on a workstation, its license will become available for another workstation.

Alerts sent by the agent are retained.

15.2.2 Presence/absence of the agent on a workstation

To check the presence or absence of the agent on workstations, follow the steps below:
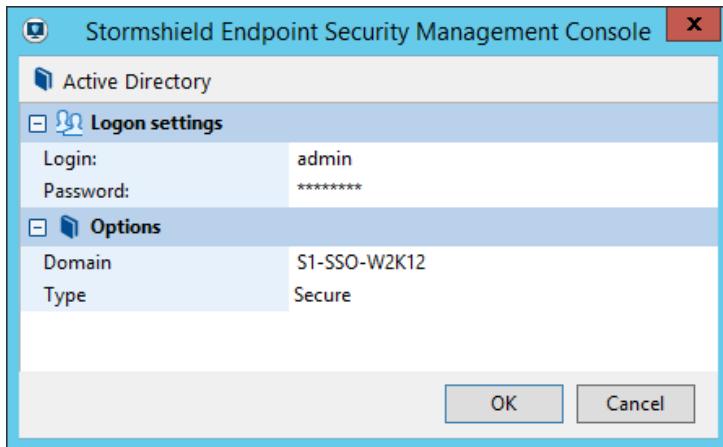
1. In the **Agent** window; click **Active Directory**. The AD list is displayed.

2. Click **Connect**.

3. Enter the following information:

   - Login.
   - Password.
   - Domain.
   - Type (of connection).

4. Click **OK**.

   A list of machines is displayed showing their respective status:

   - If the agent software has been installed, a ticked icon ❌ is displayed.
   - If the agent software has not been installed, a cross icon ✅ is displayed.
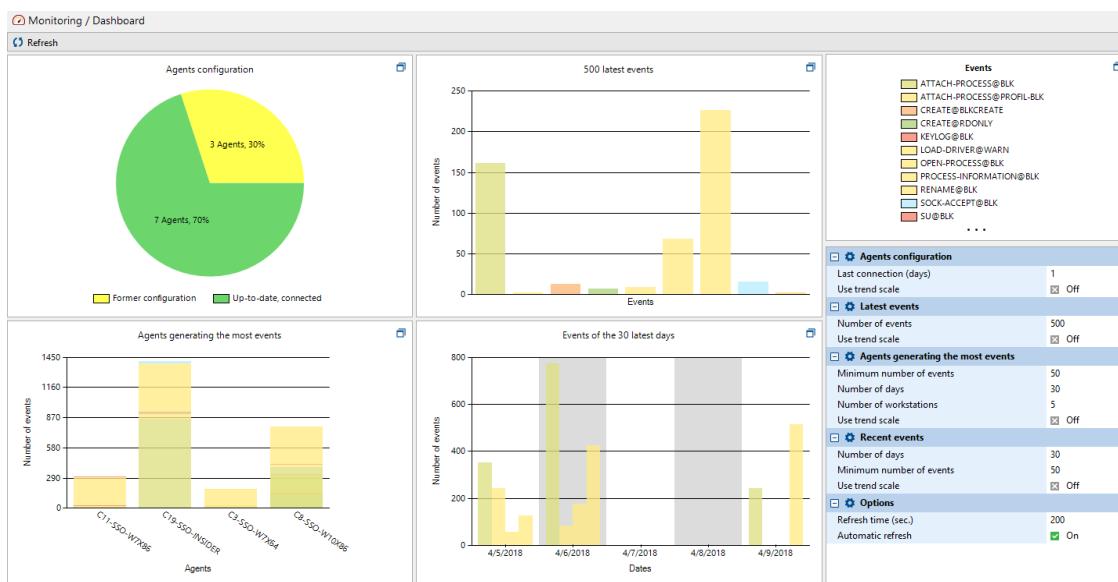
5. You can use **Export as** to save the information to a file in either of the following formats:

   - TXT (tabs used as separators).
   - CSV (commas used as separators).
   - XML.

15.3 Dashboard

The **Dashboard** provides a global and up-to-date overview of workstations. It shows four configurable charts allowing the user to see various information at a glance.

Each chart can be undocked from the window by clicking the 🗗 icon. You can browse the other panels of the console while keeping one chart or more undocked.

Agents configuration

This chart displays the status of all Stormshield Endpoint Security agents: all agents which have been connected to a server are taken into account in this chart.

The possible statuses are:

- **Up-to-date, connected**: the agent has been connected to a server for less than N days. The configuration and security policy of this agent are up-to-date and protections are functional.

- **Up-to-date, disconnected**: the agent has not been connected to a server for more than N days. The configuration and security policy of this agent are up-to-date.

- **Former configuration**: the agent did not retrieve yet the last version of the configuration and security policy applied to the server. Just after clicking **Deploy to the environment**, all the agents have this status, until their next connection to the server. Updating the configuration of an agent can take between a few hours and a few days according to the number of workstations and servers.

- **No configuration**: no configuration is assigned to the agent, for example when it is installed on the workstation. It has to retrieve a valid configuration the next time it connects to servers.

- **Configuration error**: the agent cannot activate all protections because one of the drivers has not started or does not have any valid configuration. This is the case when the agent is installed and the machine has not been restarted yet. If the problem persists after restarting the agent, a re-installation will be required.

You can specify the following settings for this chart:

- **Last connection (days)**: define the number of days since the last connection agent-server for the agent to be considered as "disconnected" in the chart. In a local network client environment, the recommended value to identify disconnected workstations is one or two days.

- **Use trend scale**: angles are calculated according to the logarithm of the percentage of the total number of agents. This view keeps the order of values but allows pointing out small values which can sometimes hardly be seen on a linear scale.

Latest events histogram

This chart displays the N last system events which occurred on agents. It provides an overview of recent activity on agents.

You can specify the following settings for this chart:

- **Number of events**: define the total number of events to be displayed. Adjust the number according to the number of workstations and the log generation policy defined in order to get a precise view of the activity.
  For less than 300 workstations, the value 50 is recommended.
  For more than 1000 workstations, select a value between 100 and 500.
- **Use trend scale**: the height of bars is calculated according to a logarithmic scale. This view keeps the order of values but allows pointing out small values which can sometimes hardly be seen on a linear scale.

Agents generating the most events

This chart displays workstations which have generated the most events during the last days. It enables identifying possible attacks if many protection logs have been recently generated on some workstations.

Workstations are displayed in abscissa (X). Bars represent generated events. Events are divided by type and displayed by order of importance.

You can specify the following settings for this chart:

- **Minimum number of events**: define the minimum number of events a workstation must generate to be considered in this chart. This allows not displaying workstations with a too small amount of events to be considered as significant enough to be displayed.
- **Number of days**: define the number of days for which events have been generated. This allows restricting display to the recent activity of agents: an agent which has generated many old events is considered as less important than an agent which has recently generated events. The value 7 is recommended.
- **Number of machines**: define the maximum number of machines to be displayed. This chart is meant to display only machines which have generated the most events recently. It is thus useless to display too many machines in this chart. The value 10 is recommended.
- **Use trend scale**: the height of bars is calculated according to a logarithmic scale. This view keeps the order of values but allows pointing out small values which can sometimes hardly be seen on a linear scale.

Recent events

This chart displays events generated over the last few days by all workstations. Events are grouped by day and displayed by order of importance.

You can specify the following settings for this chart:

- **Number of days**: define the rolling day period (from the current day) during which events must be displayed.
- **Minimum number of events**: define the minimum number of occurrences of an event on a particular day required to be displayed. Adjust the number according to the number of workstations and the log generation policy defined.
- **Use trend scale**: the height of bars is calculated according to a logarithmic scale. This view keeps the order of values but allows pointing out small values which can sometimes hardly be seen on a linear scale.

15.4 Log monitoring

Log Monitoring records any suspicious activity on client workstations and servers and the corresponding reaction of the Stormshield Endpoint Security agent.

This data is consolidated in a database where it can be consulted via the management console.

Stormshield Endpoint Security logs contain a record of all events triggered by the following:

- Software
- System
- Network
- Devices

Activities that trigger an event are defined in the security policies.

Software logs

A software log records the agent behavior whenever:

- The agent applies a configuration or a policy.
- The agent downloads a certificate or an update.
- There is a CPU overload on a server.
- The number of agents exceeds the maximum allowed by the license.

Etc.

For more information, see section Software Logs.

System Logs

The system logs contain information on system protection.

For more information, see section System logs.

Network logs

The network logs contain information on:

- Network Firewall (Category).
- Intrusion Detection System (**General Settings > Network security control**).

For more information, see section Network logs.

Device Logs

The Device logs contain information on:

- Removable devices (Category).
- Device control (General settings).
- WiFi encryption and authentication (General settings).

For more information, see section Device Logs.

15.4.1 Log monitoring graphical interface

The log monitoring panel includes four areas:

- The display options.
- The filters area.
- The events.
- The description of the selected event.

Display options

The Display options area includes the following:

- **Automatic refresh:**

  Continuous display of monitoring information which is updated as the information is refreshed.

  By default, monitoring information is automatically updated every 30 seconds.

- **Advanced filters:**

  Enables advanced filtering. Refer to the section Filter area.

- **Options:**

  Specifies the number of logs to be displayed per page and the log monitoring refresh time.

- **Logs displayed:**

  Specifies the period of time to be used to display data.

- **Export As:**

  Saves log information to a file.

This feature enables the administrator to export the visible log (i.e. what is currently displayed on the management console).

The following file formats are supported by the **Export As** feature:

- TXT (tabs used as separators).
- CSV (commas used as separators).
- XML.

The information included in the exported file consists of the currently selected log (the log displayed) and identification information.

To export a log to a file, follow the steps below:

1. Select the logs that you want to export.
2. Click **Export as**.
3. From the drop-down list, select the file format that you want to use (example: `txt`).
4. Set the file path and enter the filename.
5. Click **Save**.

Filters area

The **Filters** area contains filter criteria for selective display.

Both simple and advanced filters are available.

Advanced filters allow embedding tests with various operators at different levels.

If the option **Automatic refresh** is enabled, filters apply as soon as the refresh request is sent.

Add a simple filter

1. In the drop-down menu, select the column on which to apply the filter.
2. Select the comparison type.
3. Enter the value to compare.
4. Click **Add** to apply the filter.

You can create as many simple filters as necessary.

Add an advanced filter

In the display options, select **Advanced filters**.

When creating or modifying filters, you can move items by a simple drag-and-drop.

Add an operator

1. Click **Add operator** or right-click the appropriate operator or test.
2. In the **Filter criteria** panel, select the condition of the operator. Three conditions are available:
   - IF AND: returns 'TRUE' if all the sub nodes return 'TRUE'.
   - IF OR: returns 'TRUE' if at least one sub node returns 'TRUE'.
   - IF NOT: returns 'TRUE' if all the sub nodes return 'FALSE'.

Add a test

1. Click **Add test** or right-click the appropriate operator or test.
2. Configure the test in the **Filter criteria** panel.

If "contains" or "doesn't contain" is selected in the **Comparison** field, the search of the value is based on the SQL engine search and its syntax. This syntax implies the following:

- _ : stands for any character.
- %: stands for any character repeated 0 or n times.

To search for a metacharacter ("_" or "%" character) without interpreting it, the user must place it between square brackets.

The console encapsulates the search string into "%" characters when the user does not enter SQL metacharacters (example: file => %file%), which corresponds to the filter "contains".

If the user adds an "_" or "%" to the search string, the console no longer encapsulates the search string. The search is thus totally based on what the user has entered in the Value field.

The following table shows how the mode Comparison = "contains" works. The "Searched string" column is the value entered in the **Value** field. The "Interpreted string" column is the value sent to the SQL search engine. The "Match" column displays examples which would match the searched string. The " Do not match" column displays examples which would not match the searched string.

Searched string	Interpreted string	Description	Match	Do not match
FILE[_]	%FILE[_]%	All values containing "FILE_"	FILE_READ and FILE_	_READ and FILE
FIL_	FIL_	All values equal to "FIL" + one letter	FILE	FILE_READ, FILE_ and _READ
%[_]READ	%[_]READ	All values ending with "_READ"	FILE_READ and _READ	FILE_ and FILE
FILE[_]%	FILE[_]%	All values beginning with "FILE_"	FILE_ and FILE_READ	_READ and FILE
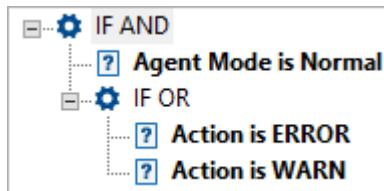
It is also possible to create a filter with the contextual menu of a workstation, an organizational unit or a domain in the Active Directory view with the option **Show logs**.

The log monitoring screen will be displayed with a filter corresponding to the selected object in the Active Directory view.

This filter is temporary and will be removed when the console will be closed.

Examples of filters

Simple embedded filters
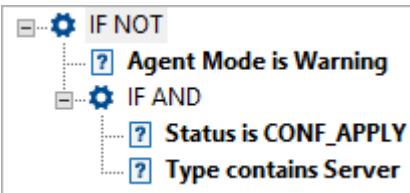
This construction allows displaying logs matching <u>both criteria</u> at the same time:

- Agent mode: Normal
- Action: ERROR <u>or</u> WARN

Multicriteria exclusion with IF NOT

The IF NOT operator allows hiding logs matching at least one of the specified criteria.

In this construction, logs matching at least one of the two following criteria are hidden after filtering:

- Agent mode: Warning
- Status: CONF_APPLY and Type: Server

Details of the filtering analysis:

Nodes	Filtering action
Node 1: test "Agent Mode is Warning"	The test returns 'TRUE' if the value of the **Agent mode** column in the log is **Warning**.
Node 2: IF AND operator including two tests	The test returns 'TRUE' if the values of the **Status** and **Type** columns in the log are **CONF_APPLY** and **Server**.

Result	The final result of the IF NOT test returns 'FALSE' if the Node 1 or the Node 2 return 'TRUE'. All logs matching these criteria are thus hidden.

Events

The variables of the four types of logs available in the **Monitoring** section are detailed in the section Information logs about agents.

In the logs table, right click the columns titles to select the columns to display.

Logs are displayed in the management console with filters applied. However, when you export a log to a file, the entire log is included (without any filter being applied).

15.5 Log Manager

15.5.1 Overview

The **Log Manager** menu in **Environment Manager** is used to customize Stormshield Endpoint Security agent logs. It is designed to configure event reporting for:

- Software Logs.
- System Logs.
- Network Logs.
- Device Logs.

The events used to generate reports are triggered by certain actions and statuses.

The actions and statuses which trigger a log are defined in the security policies.

Example 1:

The **INFO** action with status:

- **AGENT_START**:

Creates reports based on the agent version.

- **SERVER_VERSION**:

Creates reports based on the server version and server name.

- **CONF_APPLY**:

Creates reports based on the policy or configuration name.

Example 2:

The **WARN** action with status **FLOOD_DETECTED** is used to create flood reports (repeated log messages until saturation).

⚠️ **WARNING**

If the administrator filters any of these actions in the **Log Manager**, reports based on any of the following cannot be displayed:

- The version.
- Policy name.
- Configuration name.
- Server flood.

ℹ️ **NOTE**

After **updating** Stormshield Endpoint Security, new log filters may be located after the "*" wild card. To use these new filters, for each log type you must:

- Go to the **Log Manager** menu.
- Move the "*" wild card at the end of the list.
- Click **Deploy to the environment** to refresh the server.

In the **Log Manager** menu, it is possible to configure logs and add information related to logs and/or general information. The table below shows global variables which can be used in logs:

Variable	Description
%BR%	Insert a line break in the message
%TIMESTAMP%	Date format: 20/01/2010 11:16:30
%ACTION%	ERROR, INFO or WARN
%STATUS%	Shows the value of the status
%LOG%	Information message
%MODNAME%	Module name
%USERNAME%	User name
%RID%	Rule identifier
%LID%	Log identifier
%PRODUCT%	Product name
%COMPANY%	Company name

%HOSTNAME%	Agent hostname
%HOSTADNAME%	Agent AD name
%HOSTIP%	Agent IPv4 address
%HOSTID%	Agent certificate identifier (variable available only for a message sent to SMTP and/or Syslog servers)

15.5.2 Graphical interface

The graphical interface includes three sub-areas:

1. Log Types.
2. Display options.
3. Messages.

Log type

The log types which can be managed from the **Log Manager** are the following:

- Software.
- System.
- Network.
- Device.

Editing logs

Simply click in the appropriate column to parameterize the display of each log.

If you enable a parameter, the column will contain the icon ✅ .

If you disable a parameter, the column will contain the icon ❌ .

For more information, see Enable Logs.

All logs contain the **Action** and **Status** columns.

According to your configuration, logs can be consulted and stored in the following locations:

- User Interface.
- Pop-up.
- Database.
- Syslog.
- SMTP.
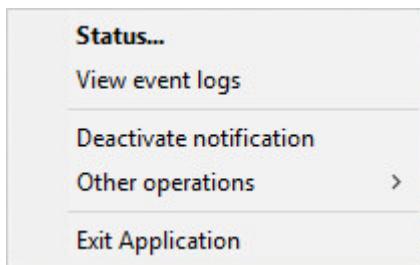
ⓘ NOTE
You can add or delete logs coming from an agent in the **Log Manager** on the management console.

User interface

This is the System log file of the Stormshield Endpoint Security agent. To display this file on the agent computer, follow the steps below:

1. Click **View event logs**.

2. Click **Show Log File**.

The following window is displayed.

Pop-up

The log will be displayed in the notification window of the Stormshield Endpoint Security agent.

Database settings

The log will be recorded in the log database.

Syslog

The log will be sent to a Syslog server (if it is configured on the SES server).

SMTP

The log will be sent to an SMTP server (if it is configured on the SES server).

Messages

Language

In the **Messages** window, you can choose the language used to display messages. The default language is English.

Message types

The **Messages** window includes four types of messages:

- Short Message.
- Long Message.
- Notification Message.

- External Message.
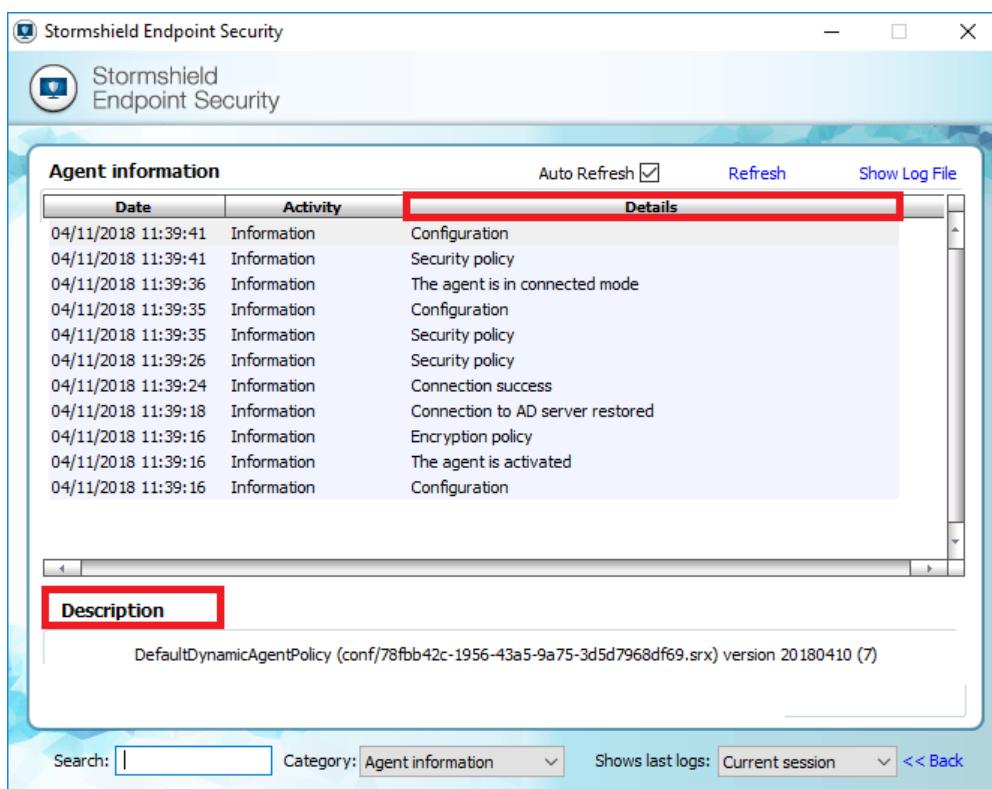
1. **Short Message**

   This is the message displayed in the **Details** column after selecting **View event logs** on the Stormshield Endpoint Security agent.

2. **Long Message**

   This is the message displayed in the **Description** column after selecting **View event logs** on the Stormshield Endpoint Security agent.

3. **Notification Message**

   This is the message displayed in the notification pop-up of the agent.

4. **External Message**

   This is the message which will be sent to an external system (Syslog or SMTP).

Actions based on detection of events

In the **Script** column of the edition settings, you can associate a script you set up in the policies to a specific log. The script is executed each time the log is generated.

For more information about creating script, see section Scripts.

If policies and configurations are applied through these scripts, they take priority over those applied through the *Policies linked* tab of an object of the directory.

If an action is triggered based on the detection of a specific event, when a process is executed from a script through the menu **Run a process** in the Actions or Tests (**Script Resources** menu, or directly in a script in the policies), the following environment variables, related to the event which triggered the action, are automatically provided to the process:

Software Logs	SES_Port_Source: Source port
System Logs	SES_PID: Process Pid SES_Source_Path: Path process source + (if any) SHA2, MD5, CERT SES_Destination_Path: Destination or Action
Network Logs	SES_IP_Source_Destination: Source IP -> Destination IP SES_Port_Destination: Destination port SES_Port_Source: Source port
Device Logs	SES_Source_Path: Process source SES_MAC_Volume_Letter: MAC address or volume letter SES_SSID: SSID (if any)

⛔ WARNING
We do not recommend to create loops in the scripts to be executed in case of detection of events. As soon as the agent reconnects to the server, the execution of new scripts triggered by a running script is stopped.

15.6 Exporting logs to an external system (SMTP or Syslog)

The administrator can use **Syslog** and/or **SMTP** (email) to send logs to an external server. You will have to configure external log transfer.
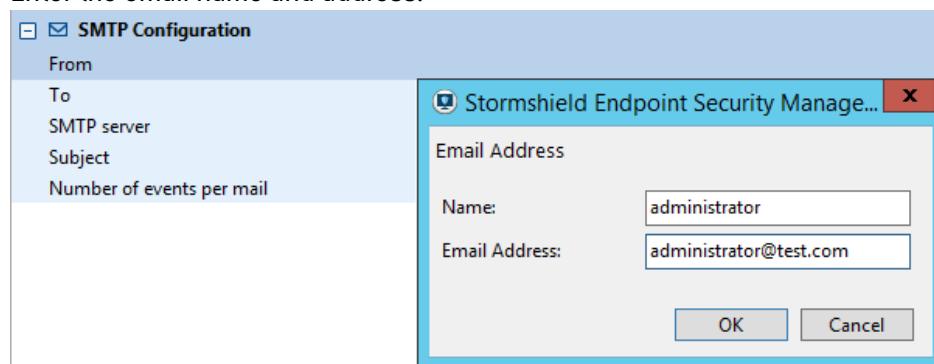
15.6.1 Exporting logs via SMTP

To export logs via SMTP, follow the steps below:

1. Define the SMTP redirection settings in the **SMTP configuration** panel of the server configuration policy:
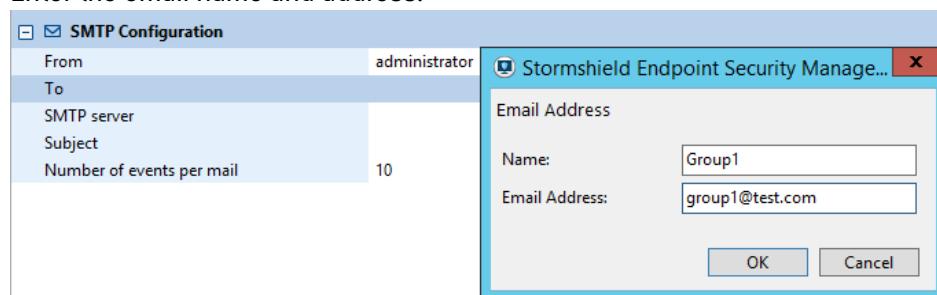
   - Click the **From** field.
     Enter the email name and address.
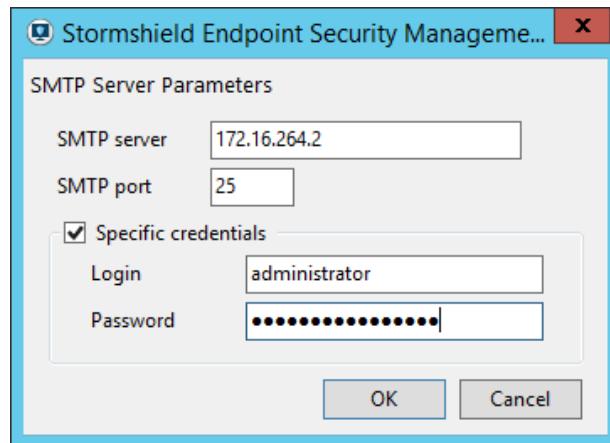
- Click the **To** field.
  Enter the email name and address.
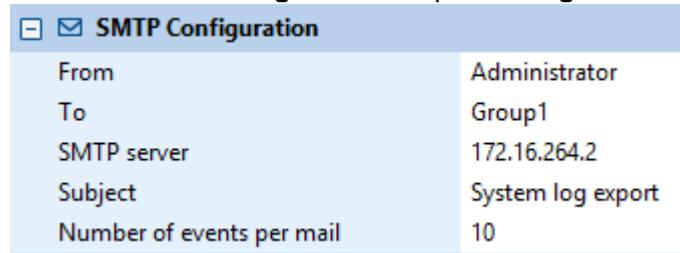
- Click the **SMTP Server** field.
  Enter the SMTP server and port information.

  If you want to use a login and a password, check the Login box and enter appropriate information.

- Enter the number of logs to be sent per message.

2. Validate your modifications.

> **NOTE**
> Use this feature **only** to send a few specific logs.

15.6.2 Exporting logs via Syslog

To export logs via Syslog, follow the steps below:

1. Define the Syslog redirection settings in the **Syslog configuration** panel of the server configuration policy:

   - In the **Address/Hostname** field, enter the IP address of the Syslog server.

   - In the **Port** field, change the port number (if necessary).

   - In the **Protocol** field, enter the protocol required (TCP or UDP).

   - Select a **Facility** level.

- ◦ Select a **Severity** level.

2. Validate your modifications.

> **ℹ NOTE**
> Use this feature **only** to send a few specific logs.

15.7 Console monitoring

15.7.1 Overview

All actions performed on the management console by an administrator can be recorded in logs accessible from the **Monitoring** menu.

The administrator's actions which are recorded in the Console Monitoring are the following:

Policies:

- Add.
- Remove.
- Rename.
- Modify.
- Apply to a a directory object.

Configuration:

- Add.
- Remove.
- Rename.
- Modify.

Script (action, test, etc.):

- Add.
- Remove.
- Rename.
- Modify.
- Send a policy to a server.

Managing users and roles:

- Add.
- Remove.
- Rename.
- Modify.
- Log configuration
- Updates

15.7.2 Graphical interface

The graphical interface includes four areas:
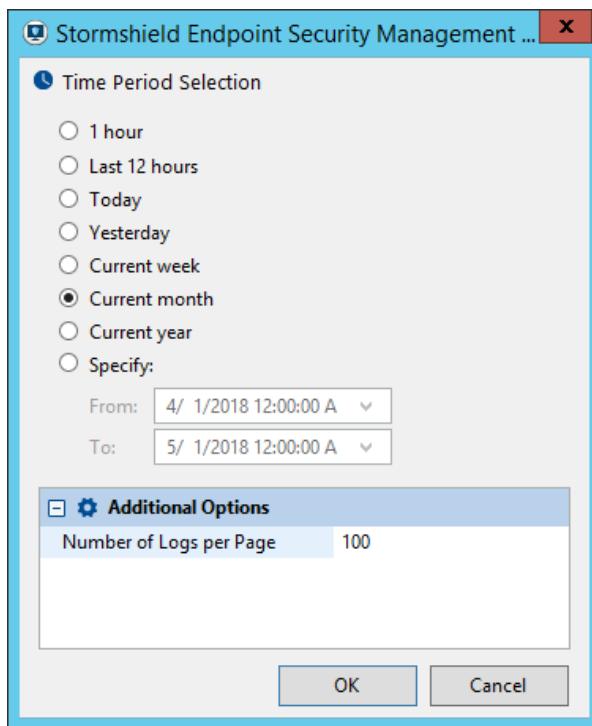
- The menu bar.
- The columns.
- The **Expand/Collapse** panel.
- The **Details** panel.

Menu bar

The menu bar includes the following commands:

- **Refresh:**

  Updates the display of the administrator's actions which are recorded in the Console Monitoring.

- **Options:**

  Defines the display options.

- ° **Time Period Selection:**

  Specifies the period of time to be used to display data in Review mode.

- ° **Additional Options:**

  Specifies the number of logs to be displayed per page.

- **Export:**

  Used to save the information to a file in the `XML` format.

- **Search:**

  For long lists, you can use the **Search** field to locate the event quickly.

Columns

The information contained in the Console Monitoring columns are the following:

- **Date:**

  Date and time of the administrator's action.

- **User Name**:

  Administrator's name.

- **Action**:

  Type of administrator's action which is reported in the Event Viewer.

  Here are a few examples of administrator's actions:

  ◦ Application of changes.

  ◦ Update.

  ◦ Add.

  ◦ Etc.

- **Entity**:

  Element associated with the administrator's action reported.

  Here are a few examples of entities:

  ◦ Security Policy.

  ◦ Encryption Policy.

  ◦ Agent configuration policy.

  ◦ Server configuration policy.

  ◦ Script.

  ◦ File.

  ◦ Etc.

- **Entity Name**:

  This column contains details on the administrator's action reported.

  Example:

  08/01/201011:31:37||admin||Application of changes||Master server||**Master 1**

  The column specifies the name of the server configuration policy applied to servers [Master1].

Date	User Name	Action	Entity	Entity Name
4/11/2018 11:46:47 ...	admin	Creation	Server Configuration	Server 2
4/11/2018 9:35:49 AM	admin	Connection	User	S1-SSO-W2K12
4/11/2018 9:35:32 AM	admin	Connection	User	S1-SSO-W2K12
4/10/2018 5:10:43 PM	admin	Application of changes	Master	\S1-SSO-W2K12 (192.168.128.69)
4/10/2018 4:55:17 PM	admin	Application of changes	Master	\S1-SSO-W2K12 (192.168.128.69)
4/10/2018 4:55:15 PM	admin	Update	Encryption	FDE
4/10/2018 4:54:23 PM	admin	Application of changes	Master	\S1-SSO-W2K12 (192.168.128.69)

Console Manager / Monitoring

← Page 1 → () Refresh Options Export

from 1/1/2018 12:00:00 AM to 1/1/2019 12:00:00 AM

Expand/Collapse

The **Expand/Collapse** panel displays an updated tree structure of the administrator's actions.

To display a deeper level of details on the console, click the appropriate level in the **Expand/Collapse** panel.
Example: **Group Settings**.

Click [+ Expand] to expand the tree structure.

Click [- Collapse] to collapse the tree structure.

Details

After clicking the appropriate level on the **Expand/Collapse** panel, the **Details** panel will display additional information (Old Value and New Value) on the updated administrator's action.

Example:
Here is the **Details** panel after clicking **Group Settings** in the **Expand/Collapse** panel.

Element	Old Value	New Value
Mass storage recovery	❌ Denied	✅ Allowed
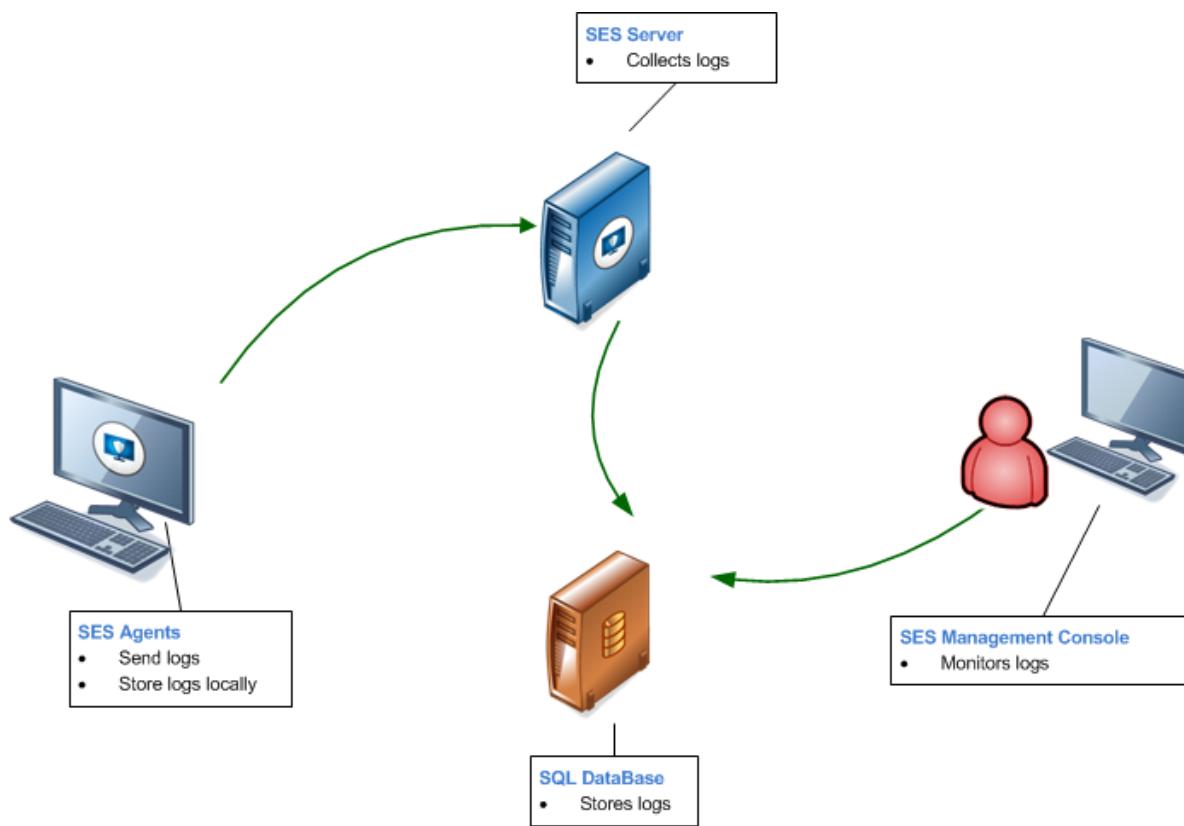
16. Agent Logs and Alerts

16.1 Introduction

Log data is collected by the Stormshield Endpoint Security agent on the client workstation and stored locally.

The path followed by the information used to generate reports is described below:

1. Logs are sent by the agents to the Stormshield Endpoint Security server.

2. The server sends these logs to the Stormshield Endpoint Security SQL database.

3. Logs are displayed on the management console.

In the event logs on the workstation (right-click on the ⊕ icon in the **View event logs** menu), the agent will show logs from the current session by default, i.e., since the last Windows startup or since the agent's last reconnection after a shutdown. Other display options may be selected in the drop-down list at the bottom left of the window.

16.2 Information logs about agents

16.2.1 Software Logs

Location

Information on agent activity and status is stored in a log file which path is:

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\log\software.sro
```

The structure of this file is similar to the structure of a *.csv* file. Values are written between square brackets, separated by the character 'ÿ'.

Each time the agent starts, the following line is inserted in the log file:

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and *xx:yy:zz* represent the start date and time.

Each time the agent stops, the following line is inserted:

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and *xx:yy:zz* represent the stop date and time.

This is an example of log:

```
[Fri Jun 19 08:20:34 2015]ÿÿ[INFO]ÿ[AGENT_STOP]ÿ[agent stopped]ÿ
[SSMON]ÿ[amartin]ÿ[A]ÿ[0]
```

In this example, the variables mean:

- TIMESTAMP : Fri Jun 19 8:20:34 AM 2015: time the message was generated.
- ACTION : INFO: message type.
- STATUS : AGENT_STOP: message status.
- LOG: agent stopped: English description of the log.
- MODNAME: SSMON: name of the module which sent the log.
- USERNAME: amartin: agent user name.
- TYPE : A: A means the message comes from the agent and S from the server.
- LID : 0: Stormshield Endpoint Security internal indicator indicating if the message must be sent to the agent, the database, the console or via Syslog.

Correspondence between variables and console display

Some log variables are displayed in the console as follows:

Variable	Console display
TIMESTAMP	Date
USERNAME	User Name
ACTION	Action
STATUS	Status
TYPE	Type
MODNAME	Mod. Name
LOG	Log

Details

The table below shows the possible values of each variable described above. Refer to the appendix Logs Tables Schema to see the schema of the SQL table storing the Software logs. Consult also some easy SQL scripts allowing retrieving logs directly from the database.

Variable	Keyword	Description
TIMESTAMP	20/01/2010 11:16:30	Date format
ACTION	ERROR	Blocks

Variable	Keyword	Description
	INFO	Audit
	WARN	Warning mode
STATUS	ACTION-FAILED	An action in the script in progress returned an error
	ACTION-MISSING	Script engine fails to interpret the action
	AGENT_IN	Agent connected
	AGENT_OUT	Agent disconnected
	AGENT_START	Agent started
	AGENT_STOP	Agent stopped
	BAN_HOST	Host banned by the Stormshield Endpoint Security server because its certificate is used by another connected machine
	BATCH_LOG	Message
	CGI_DENIED	Certificate server denies agent certificate download request
	CGI_ERROR	Error when downloading the certificate
	CGI_INVALID	Error when downloading the certificate
	CGI_SLEEP	Certificate server is in sleep mode and cannot download certificates
	CHALLENGE_INVALID_VALUE	Invalid action or duration
	CHALLENGE_FAILED	Stormshield Endpoint Security server fails to send a token to a connected agent because the agent token key is outdated
	CHECK-FAILED	A test in the script returned FALSE
	CHECK-MISSING	Script engine fails to interpret the test
	CIPHER_CONF	Encryption policy has been read
	CIPHER_NEED_RECOVERY	File encryption has been disabled. Manual recovery is required
	COM_ERROR	Internal communication error
	COM_EXT	An external element has generated a Stormshield Endpoint Security log in the message
	CONF_APPLY	Application of the configuration or security policy to the agent
	CPU_CONTROL	CPU overload on the server
	CUSTOMACTION_1	Script 1 executed
	CUSTOMACTION_2	Script 2 executed
	CUSTOMACTION_3	Script 3 executed
	CUSTOMACTION_4	Script 4 executed

Variable	Keyword	Description
	CUSTOMACTION_5	Script 5 executed
	CUSTOMACTION_ALLOWDRIVER	**Install drivers** action executed
	CUSTOMACTION_NEPGUESTACCOUNT	**Create Guest Account** action executed
	CUSTOMACTION_STANDBY	**Disable Protections** action executed
	CUSTOMACTION_STOP	**Disable Protections/Complete Stop** challenge executed
	CUSTOMACTION_UNINSTALL	**Uninstall Agent** challenge executed in %seconds
	DB_ERROR	Internal communication error with the database
	DRIVER_ERROR	Agent failed to connect to the driver
	FILE_NOT_FOUND	File cannot be found
	FLOOD_DETECTED	Log repeated and finally removed
	GET_KCM	Attempt to retrieve recovery keys denied by the server
	GET_PATCH	Update cannot be obtained because available disk space is insufficient.
	HOTSPOT_START	Beginning of the temporary web access period. Access duration is displayed in seconds
	HOTSPOT_STOP	End of the temporary web access period
	INCORRECT_DATA	The minimum configuration file present in Apache is incorrect
	INTERNAL_ERROR	Internal error (message)
	INVALID_BATCH_PARAM	The test or action in the batch includes an incorrect number of parameters at its input
	KRM_GEN	Agent has generated its unique identifier
	KU_GEN	The encryption keys assigned to the user have been downloaded
	LICENCE	Log generated if the number of agents connected to the servers exceeds the license threshold.
	LOKI_POLICY_CHANGE	Kernel protection status has changed
	LOKI_SET_CHALLENGE	Error when setting the number of reboots for driver installation
	MIGRATION_END	End of the migration of key files to the database
	MIGRATION_ERROR	Failure of the migration of key files to the database
	MIGRATION_START	Beginning of the migration of key files to the database
	NEP_CIPHERED_DRIVES	The X partition(s) have been encrypted
	NEP_DECIPHERED_DRIVES	The X partition(s) have been decrypted

Variable	Keyword	Description
	NEP_GUEST_ACCOUNT	Add/remove a guest account Failure to create/remove a guest account
	NEP_INSTALL_BUSY	Failure to change a password because a configuration is being applied
	NEP_INSTALL_COM_FAILURE	A communication error occurred when applying the configuration
	NEP_INSTALL_CONF_CANCELED	The application of the encryption configuration has been cancelled
	NEP_INSTALL_DISK_FAILURE	A disk-related error occurred when applying the configuration
	NEP_INSTALL_INVALID_CONF	Failure when applying the configuration. The configuration is invalid
	NEP_INSTALL_INVALID_DISK	Failure when applying the configuration. The disk is invalid.
	NEP_INSTALL_INVALID_SYSTEM	Failure when applying the configuration. The operating system is invalid
	NEP_INSTALL_REBOOT	Reboot the machine to complete the application of the full disk encryption policy
	NEP_INSTALL_REGISTRY_FAILURE	A registry-based error occurred when applying the configuration
	NEP_INSTALL_SHM_FAILURE	A shared memory error occurred when applying the configuration
	NEP_INSTALL_SIMU_FAILURE	A simulation error prevents the configuration from being applied
	NEP_INSTALL_SUCCESS	Successful application of the full disk encryption configuration
	NEP_INSTALL_SYNC_FAILURE	An error occurred when synchronizing/desynchronizing the disk
	NEP_INSTALL_SYSTEM_FAILURE	A system error prevents the configuration from being applied
	NEP_INSTALL_UNKNOWN	An unknown error prevents the configuration from being applied
	NEP_RECOVERED_DRIVES	The data recovery media has successfully completed disk decryption
	NEP_POSTPONE_ENCRYPTION	User postponed full disk encryption
	NEP_BOOT_SUCCESS_AUTHENT	Authentication successful at computer startup
	NEP_RECOVERED_USER_PASSWORD	The data recovery media has successfully changed user password
	NEP_BOOT_FAILED_AUTHENT	Authentication failed at computer startup
	NET_IN	Network interfaces have been dumped

Variable	Keyword	Description
	NEWCERT	New certificate has been downloaded
	NO_CONF	No configuration
	OBTAIN_FILE	File cannot be obtained because available disk space is insufficient
	ODIN_ERROR_ACCES	Agent fails to access a file for encryption/decryption purposes
	OPTIM	Network filtering rules hide lower rank rules (hidden rules removed to speed up processing) An identical dynamic filtering rule already exists (the Add operation is ignored to speed up processing)
	PIPE_CALL_FROM_NAME	Error occurred when the pipe called a function
	POLICY_CHANGE	A new policy has been received. Reboot to apply the policy
	PWD_CHG_NOT_APPLY	Failure to change the password assigned to the specified user
	RECOMMENDATION	Whenever the UAC state changes (NAP or Juniper)
	RECOVER_PATH	Recovery of a machine or directory using a file including a key ring Param1: [Directory]/Param2: [File]
	RECOVERY_COMPLETE	Successful recovery
	RECOVERY_DATA_CREATED	Generation of recovery elements
	RECOVERY_DATA_UPDATED	Updating recovery elements
	RECOVERY_DATA_CHECKED	Checking recovery elements
	RECOVERY_DATA_FIXED	Fixing recovery elements
	RECOVERY_ERROR	Internal error during recovery
	RECOVERY_FAILURE	Failed recovery
	SEND_FAILED	Data transfer to the server failed Challenge transfer to an agent failed
	SERVER_VERSION	Displays the server version number
	SET_KEY	Displays whether the synchronization was successful or not and the time required for its completion
	SIG_ERROR	The profiling resource file is not accessible
	SSMON_SESSION_HANDLER	Error when handling session events
	SSMON_STORECAMODE_FAILURE	Error when saving information
	SSMON_STORECAMODE_INVALID	Invalid data
	START	The Userland module succeeded in connecting to its driver

Variable	Keyword	Description
	STOP	The Userland module stopped successfully
	STOPAGENTDENIED	Stop Agent action failed
	STOPAGENTEXE	Agent was stopped via stopagent.exe
	SYNC_DIR	An error occurred when synchronizing/desynchronizing a directory
	UAC	UAC status changed (NAP/Juniper)
	UNSET_KEY	Keys have been flushed
	UPDATING	A new update has been downloaded on the agent
	USER_REVOKED	Authentication on a revoked user
	COMPUTER_GROUP_INHERITANCE	The computer is linked to more than one Stormshield Endpoint Security group.
	CONNECT_SUCCESS	Connection to server succeeded
	GROUP_RECURSIVITY	Error while browsing object's parent (Active Directory)
	IP_CANT_CONNECT	Secured connection to the server denied (IP address provided)
	IP_UNREACHABLE	Impossible to reach the server (IP address provided)
	LDAP_AVAILABLE	The connection to the Active Directory server has been restored
	LDAP_UNAVAILABLE	with ERROR action: Unable to contact the Active Directory server. The agent never could reach the Active Directory and does not have cache to consolidate policies. with WARN action: Unable to contact the Active Directory server. The agent uses the cache to consolidate policies.
	LICENSE_CHECK_ERROR	Error while checking the license: the server could not check the status of the license
	LICENSE_CHECK_OK	The server has validated the agent's license
	LICENSE_EXCEEDED	License exceeded, agent is not registered.
	LOAD_BALANCING	Load balancing, the server is overloaded. Another server is selected.
	LOAD_BALANCING_FORCE	Overloaded servers, all the servers are overloaded. Connection will be forced!
	VOLUME_BROWSE	An error occurred during encryption.
	WTS_SYNC	Error when creating the pipe for the SID
LOG	*	Refer to the document *Stormshield Endpoint Security - Logs Format.xls*
TYPE	A	Agent
	S	Server

Variable	Keyword	Description
MODNAME	ALL	
	HEIMDALL	
	HEIMDALL/THOR	
	MODACTION	
	MODAUTH	
	MODCERT	
	MODCOM	
	MODDB	
	MODENFORCEMENT	
	MODFLOOD	
	MODGETCONF	
	MODKEYGEN	
	MODLDAP	
	MODMULTI	
	MODNEP	
	MODRECOVERY	
	MODROOTCERT	
	MODTOKENROOT	
	MODUPDATE	
	ODIN	
	SSMON	
	THOR	
USERNAME	*	Name of the user of the computer on which the agent is installed
LID	*	This parameter is internal to Stormshield Endpoint Security

Variable	Keyword	Description
TIMESTAMP	20/01/2010 11:16:30	Date format
ACTION	ERROR	Blocks
	INFO	Audit
	WARN	Warning mode
STATUS	ACTION-FAILED	An action in the script in progress returned an error
	ACTION-MISSING	Script engine fails to interpret the action
	AGENT_IN	Agent connected
	AGENT_OUT	Agent disconnected

Variable	Keyword	Description
	AGENT_START	Agent started
	AGENT_STOP	Agent stopped

16.2.2 System logs

Location

Information on system activity and status is stored in a log file with this path:

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\log\heimdall.sro
```

The structure of this file is similar to the structure of a *.csv* file. Values are written between square brackets, separated by the character 'ÿ'.

Each time the agent starts, the following line is inserted in the log file:

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and xx:yy:zz represent the start date and time.

Each time the agent stops, the following line is inserted:

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and xx:yy:zz represent the stop date and time.

This is an example of log:

```
[Thu May 08 12:38:05 2014]ÿÿ[RENAME]ÿ[BLK]ÿ
[c:\windows\explorer.exe<CN=Microsoft Windows Verification PCA,
O=Microsoft Corporation, L=Redmond, S=Washington,
C=US><332FEAB1435662FC6C672E25BEB37BE3><5A49D7390EE87519B9D69D3E4AA66C
A066CC8255>]ÿ [c:\test.exe]ÿ[0]ÿ[amartin]ÿ[0]ÿ[61455]
```

In this example, the variables mean:

- TIMESTAMP : Thu May 08 12:38:05 PM 2014: time the message was generated.
- ACTION : RENAME: action requested.
- STATUS : BLK: Stormshield Endpoint Security action related to the requested action.
- SOURCE : c:\windows\explorer.exe<CN=Microsoft Windows Verification PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US><332FEAB1435662FC6C672E25BEB37BE3><5A49D7390EE87519B9D69D3E4AA6 6CA066CC8255> : process that caused the action.
  The SOURCE field is divided in three parts: Path<Certificate issuer><Binary file MD5><Binary file Sha-1>. Some fields can be empty if the application is not digitally signed for example.
- DEST: **c:\test.exe**: target file related to the action.
- OPTION: 0: option of the action.
- USERNAME: amartin: user name.
- RID: 0: identifier of the rule that initiated the action.
- LID: 61455: Stormshield Endpoint Security internal indicator indicating if the message must be sent to the agent, the database, the console or via Syslog.

Correspondence between variables and console display

Some log variables are displayed in the console as follows:

Variable	Console display
TIMESTAMP	Date
USERNAME	User name
ACTION	Action
STATUS	Status
SOURCE	Source path
CERT	Issuer of the digital signature certificate
MD5	MD5 hash of the source application.
SHA-1	SHA-1 hash of the source application
DEST	Details
OPTION	Option

Details

The table below shows the possible values of each variable described above. Refer to the appendix Logs Tables Schema to see the schema of the SQL table storing the System logs. Consult also some easy SQL scripts allowing retrieving logs directly from the database.

Variable	Keyword	Description
TIMESTAMP	20/01/2010 11:16:30	Date format
ACTION	ACCESS-REG	Access to registry
	ATTACH-PROCESS	Attempt to attach a process
	AUTO-PROTECTION	Attempt to modify a file, a registry key or any SES resource by another application blocked
	BAD-KEY	The decryption key used to open the file is invalid
	BLOCKED-DRIVER	Driver download has been blocked Possible kernel protection values in the **Option** column under **Monitoring > System logs**: **1**: The driver is hidden **2**: The driver is hooked **3**: The driver's name has changed **4**: The driver file does not exist on the disk **5**: The driver is hooking
	CHECKSUM	The application hash has been modified
	CREATE-PROCESS	Process creation (running an application)
	CREATE	File opening in Create mode
	DELETE	Attempt to delete a file

Variable	Keyword	Description
	EXE_ON_USB	Execution of an application from a removable device Possible values about the context of approval or denial of the execution of the application in the **Option** column under **Monitoring > System logs** are: **0**: the user has explicitly accepted or denied the execution of the application **1**: the agent is in warning mode, the execution of the application has been automatically accepted **2**: the user has not answered or has not been able to answer (if ssmon.exe is not launched for example), the execution of the application has been automatically denied.
	HOOK	Attempt to perform a global hook
	HOOKED-DRIVER	Driver hooked by another driver For more details on kernel protection values, see BLOCKED-DRIVER.
	KEYLOG	Attempt to keylog
	LINK	Creation of a symbolic link denied.
	LOAD-DRIVER	Notification that a new driver has been loaded For more details on kernel protection values, see BLOCKED-DRIVER.
	LOAD-OBJECT	DLL loading or shared memory use
	LOCK-KEY	Access to files encrypted with a script is denied
	OPEN	Attempt of execution denied
	OPEN	Access to PATH file blocked by an extension ACL
	OPEN-PROCESS	Attempt to open a process
	OVERFLOW	Memory overflow
	PROCESS-INFORMATION	Attempt to access list of active processes
	REBOOT	Attempt to reboot the system
	RENAME	Attempt to rename a file
	SOCK-ACCEPT	Using an accept (server socket)
	SOCK-BIND	Using a bind (server socket)
	SOCK-CONNECT	Using a connect (server socket)
	SOCK-ICMP	Creation of an ICMP socket
	SOCK-LISTEN	Using a listen (server socket)
	SOCK-RAWIP	Creation of a raw or UDP socket
	SU	Attempt to elevate process privileges
	SUSPECT-DRIVER	Suspect operation performed by the driver For more details on kernel protection values, see BLOCKED-DRIVER.

Variable	Keyword	Description
	TERMINATE-PROCESS	Process was terminated (mainly due to CPU overload)
STATUS	BLK	Blocks
	BLKCREATE	Blocked during creation
	BLKEXECUTE	Blocked during execution
	INVALID-BLKEXECUTE	The execution of an application identified by certificate was blocked although it should have been allowed.
	INVALID-EXECUTE	The execution of an application identified by certificate was allowed although it should have been blocked.
	DYN-BLK	Blocked by a dynamic rule
	EXT-BLK	Blocked by an extension rule
	HEAP-BLK	Blocked due to heap overflow
	LEVEL-BLK	Warning and blockage by level
	LIBC-BLK	Blocked by ret-into-libc
	PROFIL-BLK	Blocked by a deviation from standard profile
	RDONLY	Forces read-only access
	STACK-BLK	Blocked by stack overflow
	TOKEN-MODIFIED-BLK	Fraudulent modification of processes privileges blocked
	TOKEN-STOLEN-BLK	The process has been blocked because of the spoofing of a process's security context.
	WARN	Warning without blockage
SOURCE		Name of the process that triggered the event Note: Even if Stormshield Endpoint Securityprotection is enabled at startup, if the event occurs before the Stormshield Endpoint Securityservice starts, an exclamation point "!" will precede the name of the process that triggered it.
DEST		Target object path
OPTION		Socket (default value is 0) Hook identifier if the action type is HOOK or KEYLOG
USERNAME		Name of the user of the computer on which the agent is installed
RID		Unique Rule IDentifier Remark: You can double-click the log entry RID to go directly to the rule.
LID		This parameter is internal to Stormshield Endpoint Security

Examples of use of the SOURCE, CERT, MD5 and SHA1 variables

The SOURCE, CERT, MD5 and SHA1 variables relate to the application which generates the log. They are grouped into a single column in the **Log Manager** menu.

In order to sort out logs according to a particular variable, use a regular expression containing the characters < and >.

	Action	Status	User interface	Pop-up	Database	Syslog	SMTP	%SOURCE%<%CERT%><%MD5%><%SHA1%>
☑	(#.)?OPEN	BLK	✅	❌	✅	✅	✅	.*\\ssmon.exe(<.*><.*><.*>)?
☑	(#.)?CREATE	BLK	✅	❌	✅	✅	✅	.*(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)
☑	(#.)?OPEN	EXT-BLK	✅	❌	✅	✅	✅	.*\\explorer\.exe(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)
☑	.*	.*	✅	❌	✅	✅	❌	.*(<.*><.*><.*>)?

Example 1 - Filter applied on the path only

.*\\ssmon.exe(<.*> <.*> <.*>) ?

The path is the first element, therefore keep the entire block '(<.*> <.*> <.*>) ?' which allows sorting out logs from previous versions of SES and logs matching the new column format.

This filter on the %SOURCE%<%CERT%><%MD5%><%SHA1%> column allows filtering all System logs generated by the *ssmon.exe* application.

Example 2 - Filter applied on the MD5 hash

.*(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)

You need to specify the variable which must be recognized. Remove the character '?' from the block (<.*> <.*> <.*>) because it makes the block optional.

This filter allows sorting out all applications having the MD5 hash 332FEAB1435662FC6C672E25BEB37BE3, regardless of the path, the digital signature or the SHA-1 hash.

Example 3 - Filter applied on the path and the MD5 hash

.*\\explorer\.exe(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)

Like in example 2, the block (<.*> <.*> <.*>) must not be optional. Remove the final '?'.

This filter only recognizes the *explorer.exe* application with the MD5 hash 332FEAB1435662FC6C672E25BEB37BE3.

> **ℹ NOTE**
> To take into account certificates and hashes filtering, ensure the SES agent correctly works out these data. Refer to the use of the parameter **Force detailed logs** in section **Application control**.

16.2.3 Network logs

Location

Information on network activity and status is stored in a log file which path is:

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\log\thor.sro
```

The structure of this file is similar to the structure of a *.csv* file. Values are written between square brackets, separated by the character 'ÿ'.

Each time the agent starts, the following line is inserted in the log file:

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and xx:yy:zz represent the start date and time.

Each time the agent stops, the following line is inserted:

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and xx:yy:zz represent the stop date and time.

This is an example of log:

```
[Mon Jun 22 09:47:08 2015]ÿÿ[FW_PORT]ÿ[OUT]ÿ[00:00:00:00:00:00]ÿ
[192.168.129.22->192.168.129.20]ÿ[49189]ÿ[16005]ÿ[0x0800]ÿ[0x06]ÿ
[amartin]ÿ[61]ÿ[65280]
```

In this example, the variables mean:

- TIMESTAMP: Mon Jun 22 9:47:08 AM 2015: time the message was generated.
- ACTION: FW_PORT: action requested.
- STATUS: OUT: status related to the requested action.
- METADATA: 00:00:00:00:00:00: data related to the action.
- IP: 192.168.129.22->192.168.129.20 : packet source and destination.
- PORTSRC: 49189: source port.
- PORTDST: 16005: destination port.
- PROTO1: 0x0800: code for the type of request executed, here IPV4.
- PROTO2: 0x06: code for the protocol used, here TCP.
- USERNAME: amartin: user name.
- RID: 61: identifier of the rule which initiated the action.
- LID: 65280: Stormshield Endpoint Security internal indicator indicating if the message must be sent to the agent, the database, the console or via Syslog.

Correspondence between variables and console display

Some log variables are displayed in the console as follows:

Variable	Console display
TIMESTAMP	Date
USERNAME	User Name
ACTION	Action
STATUS	Status
METADATA	MAC Address
IP	IP Address
PORTSRC	Src. Port
PORTDST	Dst. Port
PROTO1	Protocol
PROTO2	Over IP
RID	RID

Details

The table below shows the possible values of each variable described above. Refer to the appendix Logs Tables Schema to see the schema of the SQL table storing the Network logs. Consult also some easy SQL scripts allowing retrieving logs directly from the database.

Variable	Keyword	Description
TIMESTAMP	Tue Apr 20 11 :22 :15 2010	Date

Variable	Keyword	Description
ACTION	ARP_ATTACKING_0x21	Identity theft attempt detected on an IP address on the network. Packet blocked.
	ARP_BLOCK_0x1	ARP stateful error (reply without request) or ARP_POISON flood
	ARP_DELETE_0x5	Entry associated with the IP address has been removed from the Windows ARP cache. Packet blocked after sending a gratuitous request (IDS set to **High** or **Critical**).
	ARP_POISON_0x45	ARP cache poisoning attempt detected. Packet blocked. Entry associated with the suspect IP address has been removed from the Windows ARP cache.
	ARP_POISON_0x49	ARP cache poisoning attempt detected. Packet blocked. Windows ARP cache has been updated from the previous entry.
	ARP_SPOOF_0x112	IP theft attempt detected. Packet accepted. Network protection (IDS set to **Critical**).
	ARP_SPOOF_0x12	IP theft attempt detected. Packet accepted.
	FLOOD	Repeated log entry
	FW_ICMP	Rule applied to an ICMP message. METADATA, PROTO1, IP, PROTO2, PORTSRC and PORTDST variables are filled in.
	FW_IP	Rule applied to an IP address (only METADATA, PROTO1, IP and PROTO2 variables are filled in)
	FW_IPV6	Attempt of communication through IPv6 protocol blocked.
	FW_MAC	Rule applied to MAC address (only METADATA and PROTO1 variables are filled in). The MAC address (hardware address of the network card) indicated in the MAC ADDRESS column is the remote machine address since its local address remains the same.
	FW_PORT	Rule applied to port filtering. METADATA, PROTO1, IP, PROTO2, PORTSRC and PORTDST variables are filled in.
	PORTSCAN	Port scan detected
	STATEFUL_STATUS	PROTO1 variable indicates the stateful status code of the previously blocked packet
STATUS	CONNECTION_CLOSED	One or several connections have been closed because they are too slow
	IN	Filtering of incoming traffic
	INOUT	Filtering of incoming or outcoming traffic
	IP_BLOCKED	Suspect IP address causing flood blocked
	OUT	Filtering of outgoing traffic

Variable	Keyword	Description
	SCAN_IN	Incoming port scan detected
	SCAN_OUT	Outgoing port scan detected
IP	SSID (WiFi)	Name of the wireless network
	IP fragment	Partial IP address
	IP Address	Complete IP address
METADATA	*	In the case of a FLOOD, indicates the number of occurrences of the event. Otherwise, indicates the MAC addresses.
IP	*	Packet source and destination
PORTSRC	*	Source port number
PORTDST	*	Destination port number
PROTO1 PROTO2	*	Protocols being filtered. Refer to Protocols.
USERNAME	*	Name of the user of the computer on which the agent is installed
RID	*	Unique Rule IDentifier
LID	*	This parameter is internal to Stormshield Endpoint Security

16.2.4 Device Logs

The device log contains information on removable devices and WiFi activity.

Location

Information on removable device and WiFi activity is stored in a log file which path is:

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\device.sro
```

The structure of this file is similar to the structure of a *.csv* file. Values are written between square brackets, separated by the character 'ÿ'.

Each time the agent starts, the following line is inserted in the log file:

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and xx:yy:zz represent the start date and time.

Each time the agent stops, the following line is inserted:

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

XX/YY/ZZZZ and xx:yy:zz represent the stop date and time.

This is an example of log:

```
[Mon Jun 22 10:07:56 2015]ÿÿ[VOLUME_DENIED]ÿ[INFO]ÿ[]ÿ[]ÿ[]ÿ[0]ÿ[USB]ÿ
[DISK]ÿ[35DF010EF40D19636380661A7983BB82]ÿ[5398]ÿ[34344]ÿ
[00000000000000007BEF94A6]ÿ[Flash]ÿ[Drive AL_USB20]ÿ[UNENROLLED_
CORRUPT_ENROLL]ÿ[]ÿ[amartin]ÿ[0]ÿ[61455]
```

In this example, the variables mean:

- TIMESTAMP: Mon Jun 22 10:07:56 2015: time the message was generated.
- ACTION: VOLUME_DENIED: action requested.

- STATUS: INFO: status related to the requested action.
- SOURCE: (empty): name of the network card (WiFi) or process (removable mass storage device).
- DEST1: (empty): name of the file (removable mass storage device) MAC Address (WiFi).
- DEST2: (empty): file name after renaming (removable mass storage device) or SSID (WiFi).
- SIZE: 0: device size.
- TYPE: USB: device type.
- CLASSID: DISK: device class identifier.
- MD5: 35DF010EF40D19636380661A7983BB82: MD5 checksum of a combination of parameters allowing the unique identication of a device.
- VENDORID: 5398: vendor identifier.
- PRODUCTID: 34344: product identifier.
- SERIALID: 00000000000000007BEF94A6 : serial identifier.
- VENDORNAME: Flash: vendor name.
- PRODUCTNAME: Drive AL_USB20: product name.
- ENROLLMENTSTATE: UNENROLLED_CORRUPT_ENROLL: enrollment type.
- OWNERNAME: (empty): device owner name.
- USERNAME: amartin: user name.
- RID: 0: identifier of the rule which initiated the action.
- LID: 61455: Stormshield Endpoint Security internal indicator indicating if the message must be sent to the agent, the database, the console or via Syslog.

Correspondence between variables and console display

Some log variables are displayed in the console as follows:

Variable	Console display
TIMESTAMP	Date
USERNAME	User Name
ACTION	Action
STATUS	Status
SOURCE	Source
DEST1	Destination
DEST2	Destination2
SIZE	Size
TYPE	Type
CLASS	Class
MD5	Checksum of a combination of parameters allowing the unique idetification of a device
VENDORID	Vendor IDentifier
PRODUCTID	Product IDentifier
SERIALID	Serial number of the device

Variable	Console display
VENDORNAME	Vendor name
PRODUCTNAME	Product name
ENROLLMENTSTATE	Enrollment state
OWNERNAME	Owner name
RID	Unique identifier of the rule

Details

Device log table

The table below shows the possible values of each variable described above. Refer to the appendix Logs Tables Schema to see the schema of the SQL table storing the Device logs. Consult also some easy SQL scripts allowing logs to be retrieved directly from the database.

Variable	Keyword	Description
TIMESTAMP	20/01/2010 11:16:30	Date format
ACTION	AP_ACL	Access point with ACL filtering rule (Status: WARN)
	AP_ADHOC	Access point in adhoc mode (Status: WARN)
	AP_INSECURE	Unsecured access point (Status: WARN)
	AP_WIFI	WiFi access point set to on/off (Status: WARN)
	AUTO_ENROLL	Removable device enrolled from the agent
	BAD_UNPLUG	USB key incorrectly removed
	BLUETOOTH	Bluetooth device blocked
	CD	CD reading process blocked
	CDWRITER	CD burning process blocked
	DEVICE_UNPLUG	Device plugged out
	DEVICE_PLUG	Device plugged in
	ENROLLMENT	Non enrolled device blocked
	FILE_CREATE	File created (Status: INFO).
	FILE_DELETE	File deleted on the removable device (Status: INFO)
	FILE_OPEN	File open on removable device (Status: BLK)
	FILE_OVERWRITE	File overwritten on the removable device (Status: INFO)
	FILE_READ	Data read on the removable device (Status: INFO)
	FILE_RENAME	File renamed on the removable device (Status: BLK or WARN)
	FILE_WOPEN	File opened for overwrite operation on removable device (Status: BLK)
	FILE_WRITE	Data written to a file on the removable device (Status: INFO)
	IRDA	Device using infrared port blocked

Variable	Keyword	Description
	MODEM	Modem blocked
	PARALLEL	Device connected to the parallel port blocked
	PCMCIA	PCMCIA device blocked
	SERIAL	Device connected to the serial port blocked
	USB_CLASSID	Class ID of the removable device (in the Status field)
	VOLUME_DISMOUNT	Disconnected removable device (Status: INFO)
	VOLUME_MOUNT	Connected removable device (Status: INFO)
	VOLUME_DENIED	Access to the device is forbidden. Generated if a rule specifies a filter on the enrollment status (Status: INFO)
	VOLUME_READONLY	Access to the device is read-only. Generated if a rule specifies a filter on the enrollment status (Status: INFO)
	VOLUME_READWRITE	Access to the device is authorized. Generated if a rule specifies a filter on the enrollment status (Status: INFO)
STATUS	BLK	Blocks
	INFO	Audit
	WARN	Warning mode
	SUCCESS	Action succeeded
	USER_MISSING	User not connected
SOURCE	*	Network card name (WiFi) Process name (mass storage device)
DEST1	*	File name
DEST2	*	File name after renaming (mass storage device) SSID (WiFi)
SIZE	*	Size of the device or modification
TYPE	FIREWIRE NETWORK PCMCIA USB	Refer to Type variables.

Variable	Keyword	Description
ClassID	BLUETOOTH CDROM DISK IRDA MODEM PARALLEL PCMCIA SERIAL USB_ACTIVE_SYNC USB_APPLICATION_ SPECIFIC USB_AUDIO USB_CDCDATA USB_ COMMUNICATION USB_CONTENT_ SECURITY USB_DIAGNOSTIC USB_HID USB_HUB USB_IMAGING USB_ MISCELLANEOUS USB_PALM_SYNC USB_PHYSICAL USB_PRINTER USB_SMARTCARD USB_STORAGE USB_VENDOR_ SPECIFIC USB_VIDEO USB_WIRELESS_ CONTROLLER WIFI	Refer to Class ID variables.
MD5	*	MD5 checksum of a combination of parameters allowing the unique identification of a device
VENDORID	*	Vendor IDentifier
PRODUCTID	*	Product IDentifier
SERIALID	*	Serial ID
VENDORNAME	*	Vendor name
PRODUCTNAME	*	Product name
ENROLLMENTSTATE	*	Enrollment status. Refer to Enrollment status variables.
OWNERNAME	*	Owner of the enrolled device
USERNAME	*	Name of the user of the computer on which the agent is installed
RID	*	Unique Rule IDentifier
LID	*	This parameter is internal to Stormshield Endpoint Security

WiFi variables

Each WiFi variable can assume the following values:

Variable	Keyword	Description
ACTION	AP_ACL	Access point with ACL filtering rule
	AP_ADHOC	Access point in adhoc mode
	AP_INSECURE	Unsecured access point
	AP_WIFI	WiFi access point set to on/off
STATUS	WARN	Warning mode
SOURCE		Network interface name
DEST1		Access point MAC address
DEST2		Access point SSID
SIZE		Channel
TYPE		Network
CLASSID		WiFi
USERID		Information message
ID		User Identifier

Type variables

Each Type variable can assume the following values:

Variable	Action
FIREWIRE	Firewire access control and audit
NETWORK	WiFi access control
PCMCIA	PCMCIA access control and audit
USB	USB access control and audit

Class ID variables

Each class ID variable can assume the following values:

Variable	Description	Action
CDROM	CD-ROM, DVD-ROM, Blu-Ray reader	Access control, Write protection
DISK	Removable mass storage device	Access control, Audit
FLOPPY	Floppy disk drive	Heimdall
NETWORK	WiFi network	Access control
U3	U3 USB key	Access control
USB_AUDIO	USB audio card	Access control
USB_HID	USB HID devices (keyboard, mouse, graphics tablet, etc.)	Access control
USB_IMAGING	USB imaging devices (webcam, scanner, etc.)	Access control
USB_ACTIVE_SYNC	USB removable mass storage device	Class ID control

Variable	Description	Action
USB_APPLICATION_SPECIFIC	USB_APPLICATION_SPECIFIC class device	Class ID control
USB_CDCDATA	USB_CDCDATA class device	Class ID control
USB_COMMUNICATION	USB_COMMUNICATION class device	Class ID control
USB_CONTENT_SECURITY	USB_CONTENT_SECURITY class device	Class ID control
USB_DIAGNOSTIC	USB_DIAGNISTIC class device	Class ID control
USB_HUB	USB_HUB class device	Class ID control
USB_MISCELLANEOUS	USB_MISCELLANEOUS class device	Class ID control
USB_PALM_SYNC	USB_PALM_SYNC class device	Class ID control
USB_PHYSICAL	USB_PHYSICAL class device	Class ID control
USB_PRINTER	USB printer	Access control
USB_SMARTCARD	USB smart-card reader	Class ID control
USB_STORAGE	USB removable mass storage device	Class ID control
USB_VENDOR_SPECIFIC	USB_VENDOR_SPECIFIC class device	Class ID control
USB_VIDEO	USB_VIDEO class device	Class ID control
USB_WIRELESS_CONTROLLER	USB_WIRELESS_CONTROLLER class device	Class ID control
WIFI	Wireless network interface	WIFI (modap)

Enrollment status variables

Each Enrollment status variable can assume the following values:

Variable	Description	ACTION
UNENROLLED	The device is not enrolled	
UNENROLLED_CORRUPT_ENROLL	The enrollment file is corrupted	The device is considered as not enrolled
UNENROLLED_CORRUPT_FOOTPRINT	The footprint file is corrupted	The device is considered as not enrolled
UNENROLLED_WRONG_ORGANIZATION	The removable device is enrolled, but not for the organization on which the user is trying to use it	It is possible to enroll the device again in order to use it on the new organization
ENROLLED	The device is enrolled.	
ENROLLED_CONTENTCHANGED	The device is enrolled but its content has changed out of the perimeter	The device is considered as enrolled
ENROLLED_NOTRUST	The device is enrolled but its trust status could not be restore	The device is considered as enrolled
TRUSTED	The device is trusted	Trust status maintained when performing operations on the device

Alert types

Removable device alerts issued by the **Log Manager** are the following:

- **Short Message:**

  This is the message that you can read in the list of logs on the agent computer when clicking the icon Stormshield Endpoint Security 🛡 in the taskbar.

  ```
  Block Process : %SOURCE%
  ```

- **Long Message:**

  This is the detailed message that you can read when selecting a log on the Stormshield Endpoint Security agent.

  ```
  Access to [DEVICE NAME] device performed by %SOURCE% has been
  blocked. Please contact your administrator for further information.
  ```

- **Notification Message:**

  This is the message that you can read in a pop-up on the agent (if the field is empty, no pop-up is displayed).

  ```
  Access to [DEVICE NAME] device is not allowed on this workstation.
  ```

- **External Message:**

  This is the message that you can read on the external logging system (example: Syslog).

  ```
  Access to [DEVICE NAME] device performed by %SOURCE% has been
  blocked.
  ```

  > 🛈 **NOTE**
  > Variables between % are replaced with the name of the resource when displayed on the agent.

16.3 Certificate server logs

Information issued by the certificate server is stored in a log file which default path is:

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Server\Apache\logs\cgi.log
```

Log entries fall down into three categories:

- **Info**

  ◦ `Info: RECOVERY certificate created [IP]:`

    A recovery certificate has been requested by the IP host and generated.

  ◦ `Info: Permission denied [ERRCODE] [IP]:`

    Certificate download request from the IP host has been rejected.

  ◦ `ERRCODE = e:`

    Internal error.

  ◦ `ERRCODE = s:`

    Current date is not comprised within the certificate download period.

  ◦ `ERRCODE = d:`

    Agent origin is not valid (the agent has been downloaded from another master server).

  ◦ `Info : certificate created [IP]:`

    A certificate has been generated for the IP host.

- **Warning**

  - `Warning: Deleting old cgi.lock:`

    Lock file deletion has been forced. This occurs when the server is not shut down normally.

- **Error**

  - `Error: CGI is locked. Exiting process:`

    CGI has failed to access the lock file for 5 minutes. The certificate request is cancelled.

  - `Error: Invalid configuration file. Error: could not retrieve IP address:`

    The configuration file is invalid. The server failed to retrieve the IP address of the client host.

  - `Error: Wrong RECOVERY login/password:`

    The login and password set in the recovery certificate request form are not valid.

  - `Error: RECOVERY certificate creation failed [IP]:`

    An internal error occurred while using the recovery certificate request form.

  - `Error: could not retrieve request parameters [IP]:`

    The server failed to retrieve request parameters.

  - `Error: certificate creation failed [IP]:`

    An internal error occurred.

16.4 Sending logs customized by the user

The SSUSRLOG command-line tool allows the user to send customized logs to the SES management console from the agent.

The tool allows directly writing the new log in the command-line interface or sending a set of logs from a CSV file. It is located in the Stormshield Endpoint Security agent directory (`ssusrlog.exe`).

The settings of these customized logs are defined in the **Log Manager** in the SES management console (sending logs to a server or an external tool, pop-up windows, etc.). It is also possible to create new log status and use them with the SSUSRLOG tool. For more information, see the section **Log Manager**.

It is possible to create log messages for each language supported by Stormshield Endpoint Security.

To send one or few logs directly with the command-line interface, the user must use the syntax as follows:

- ssusrlog "log message" (default status: USER_LOG)

- ssusrlog LOG_STATUS "log message"

  ⓘ NOTE
  The SSUSRLOG tool automatically converts status to capital letters.

The user can add the following options:

- -e: ERROR action

- -w: WARNING action

- -i: INFO action

These values display in the **Action** column of the **Software logs**, **System logs**, **Network logs** and **Device logs** panels of the SES management console. The default value is INFO.

To send a set of logs, the user can enter a CSV file as a parameter of the command line as follows:

ssusrlog -f csv_file_name

The CSV file must contain 3 columns and the separator character is a comma :

- column A: ERROR or WARN or INFO
- column B: the log status
- column C: the message

This is an example of lines of a CSV file:

WARN,USER_PASSW,The user Bob has just changed his password

ERROR,USER_PGM_EXIT,The prog.exe program has ended normally

INFO,USER_TEST,"The xx utility program has just been installed, the workstation needs to be restarted"

> **NOTE**
> If the file has not been built by Microsoft Excel, you need to pay attention to how double quotes and commas are used.

The user can add the following option:

- -s: separator

> **NOTE**
> If CSV files are built with international versions of Excel, the separator character may be another character than the comma. The user must declare it in the command line.

The following additional options are available for both modes:

- -verbose: displays additional information.
- -simul: displays additional information and analyzes the CSV file or the command line. Logs are not sent to Stormshield Endpoint Security. It may be useful to test tools and scripts building CSV files. This option automatically enables the "verbose" mode. In this case, the tool can be executed on a workstation without Stormshield Endpoint Security.

The following table gives examples of how to use the SSUSRLOG tool:

Example	Explanation
ssusrlog -w WIN_INFO "test number 1"	Log written in the command-line interface and sent to the console
ssusrlog -f d:\test\tmp.csv -s ;	Logs listed in the file `d:\test\tmp.csv` and sent to the console. The separator character is the semi-colon.
ssusrlog f d:\test\tmp.csv -s ; -simul	Test of the log file `d:\test\tmp.csv`. The separator character is the semi-colon. Logs are not sent to Stormshield Endpoint Security.

SSUSRLOG return codes are:

- 0: everything is ok
- 1: empty command line, help is displayed
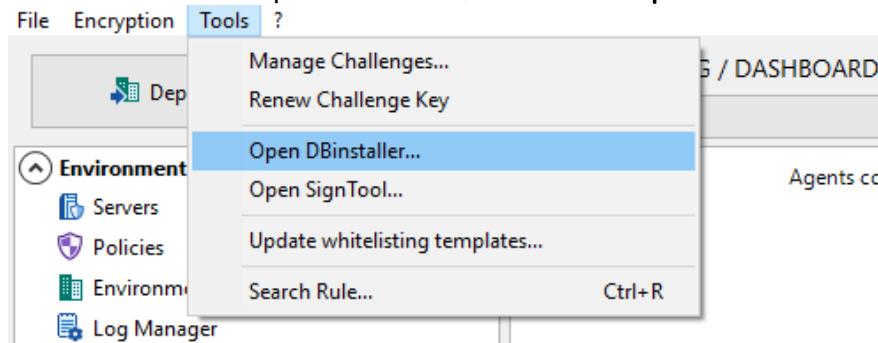
- 2: an error occurred

16.5 Flushing logs from the database

You have the possibility to delete the logs from the database by using the database maintenance wizard DBinstaller.
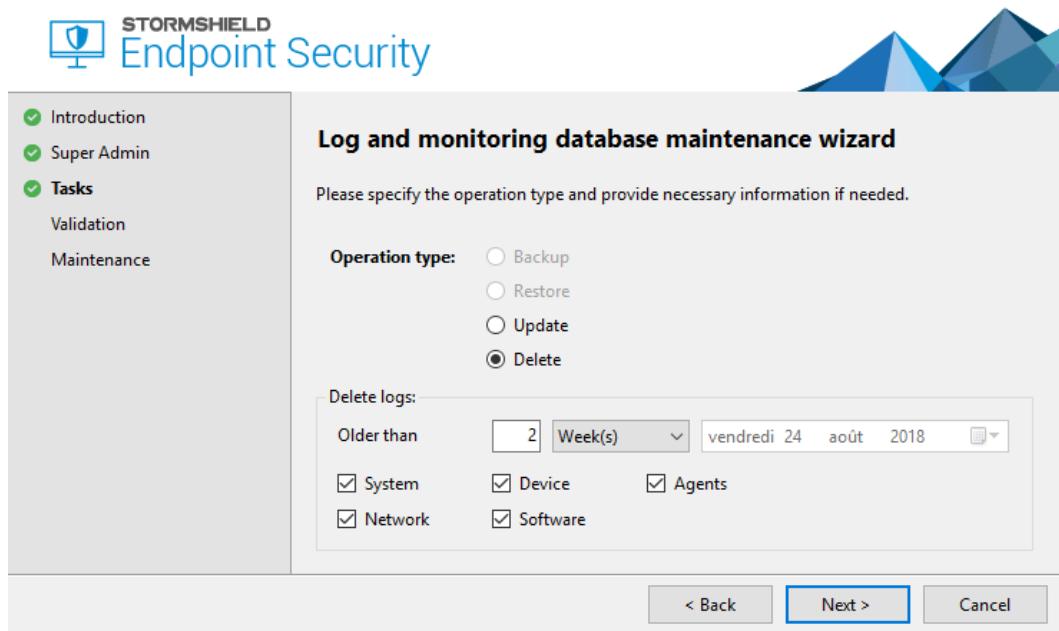
To delete the logs:

1. Click on **Tools** at the top of the console, then click on **Open DBinstaller** to open the wizard.

2. From DBinstaller, click on **Log and monitoring database maintenance wizard** and then on **Next**.

3. Fill in the fields to connect to the database.

4. Choose the **Delete** operation type and then the time period and the type of logs to delete.

5. Click on **Next** to go through the **Validation** and **Maintenance** steps.

17. Stormshield Endpoint Security Reporting

17.1 Overview

The SES console allows generating synthesis reports about the status of the installed agents. They are available in the **Monitoring** section of the console.

There are two types of reports:

- "Graphical" reports:
  - Servers and Agents
  - Workstation Integrity
  - System Security
  - Removable Devices
  - Licenses
- "Table" reports:
  - Agent Status
  - Stormshield Endpoint Security Configuration Changes
  - Stopped Agents
  - Agents' Configuration
  - Agents' Policies
  - Policy Violations by User and Agent
  - Blocked Files
  - Devices Accesses

Reports have two operating modes: **Real-time** mode and **Historical** mode.

Real-time reports provide the latest information, i.e. data of the current day only.

This information is automatically updated depending on the settings defined in **Log monitoring refresh time (sec.)** under **Configuration** in the **Monitoring** section.

For "table" reports, you can modify the date format in the **Date format** option under **Configuration** too. For more information about date format, see Appendix Date and time format strings

⊟ ⚙ Options	
Date format	G
CSV separator	, (Comma)
Layout (You must restart the console)	Save
Language (You must restart the console)	English
Log and monitoring databases	192.168.128.69\SES
Database for encryption keys	192.168.128.69\SES
Agent monitoring refresh time (sec.)	30
Log monitoring refresh time (sec.)	10
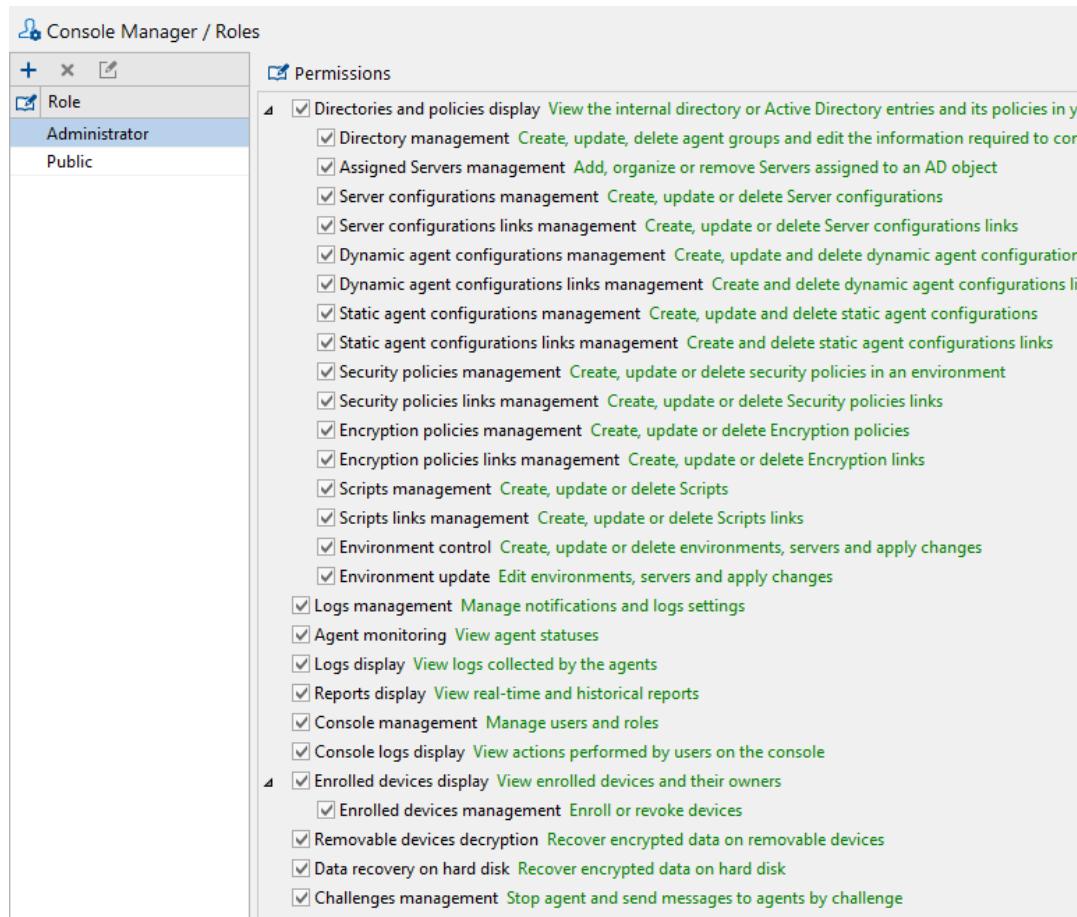
17.1.1 Prerequisites

To generate and view reports, the console user must have appropriate permissions.

Permissions are given to the console user by the administrator via the **Roles** in the **Console Manager** section.

The administrator determines who has access rights to reports by checking the appropriate boxes in the Role Manager.

Example: The **Reporting** role is allowed to view historical reports and real-time reports (checked boxes). The **Logs display** role is also required.

For more information, see the section "Monitoring" section.

17.1.2 Report path

The path followed by the information used to generate reports is described below:

1. Reports are based on the logs sent by the agents to the Stormshield Endpoint Security server.

2. The server sends these logs to the Stormshield Endpoint Security SQL database.

3. The database stores these logs.

17.2 Graphical interface

17.2.1 Menu bar

The menu bar is displayed as follows:

The menu bar contains the following actions:

- **Reports**:

  This action is used to select the category of report to be generated.

- **Save Report**:

  This action is used to save reports to the location specified, in the `.png` (for graphical reports) or `.csv` (for table reports) format.

- **Update Report**:

  This action is used to update reports.

17.2.2 Display settings

Options

Depending on the category selected, the report can include the following options:

- Type.
- Date.

- Period.
- Top value.

Unavailable options are greyed out.

Type

This option is used to select the **Historical** or **Real-Time** report type.
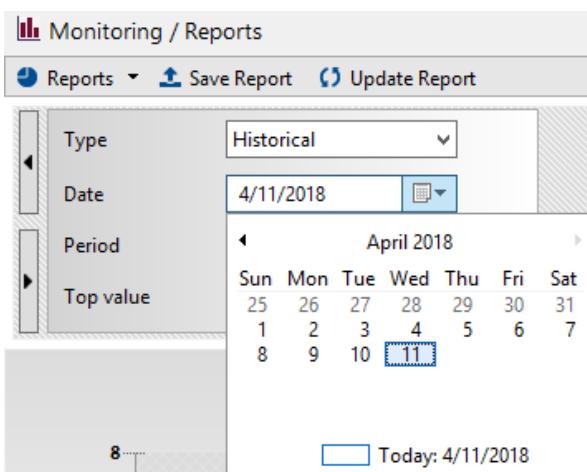
If you select **Real-Time**, only the information of the current day (from midnight to the current time) is provided.

If you select **Historical**, the information displayed covers the time interval specified by the administrator.

Date
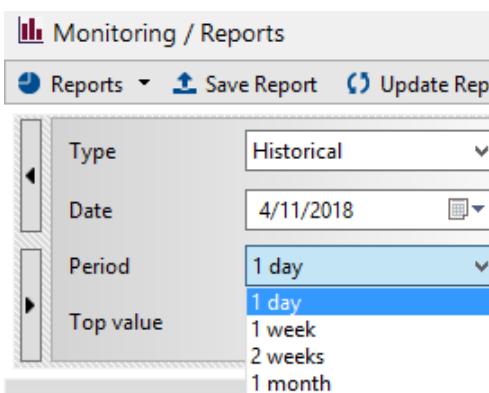
This option is used to select the start date to generate a **Historical** report.
The current date is selected by default.

Period

This option is used to define the time interval required to generate a **Historical** report:

- 1 day.
- 1 week.
- 2 weeks.
- 1 month.

Top value
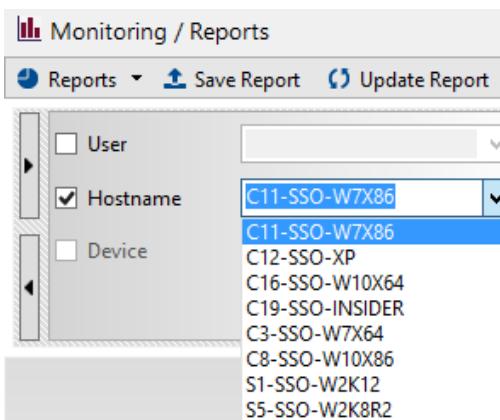
This option is used to display the most significant elements (top 5 or top 20) of a report type.

Filters

Depending on the category selected, the report can be generated by applying the following filters:

- User
- Hostname
- Removable Devices
- Viruses

Unavailable filters are grayed out.
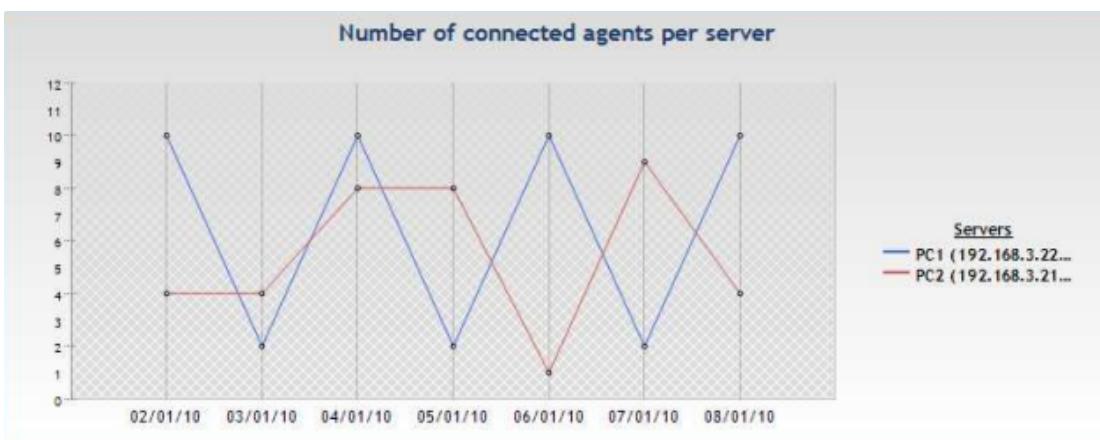
17.3 "Graphical" reports

17.3.1 Servers and agents

Servers and Agents reports show in a summarized way information related to Stormshield Endpoint Security servers and agents.

- **Number of connected agents per server:**
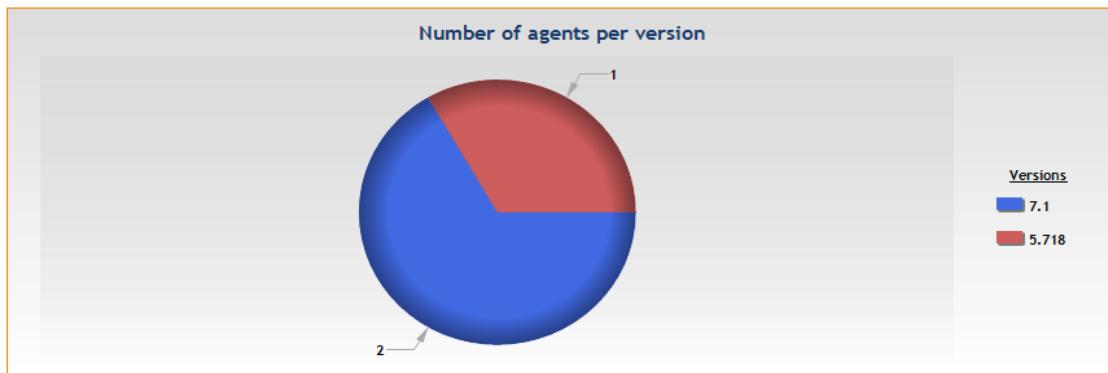
- **Agent compliance**

This sub-report only displays in **Real-Time** mode. It shows the distribution of recommendations among agents. Possible recommendations are: authorize, isolate, no access or no recommendation. Recommendations are set up by script and allow communicating a status to TNC clients (Trusted Network Connect) such as Juniper.
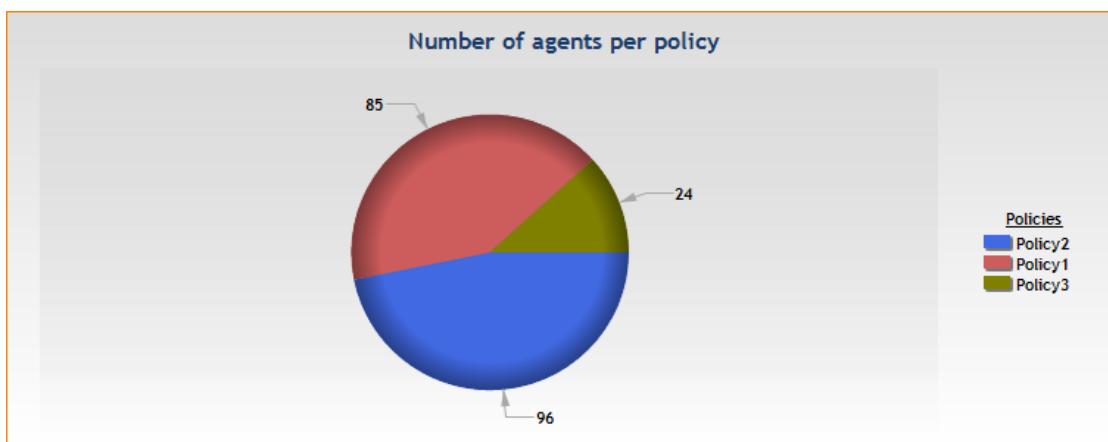
- **Number of agents per version:**
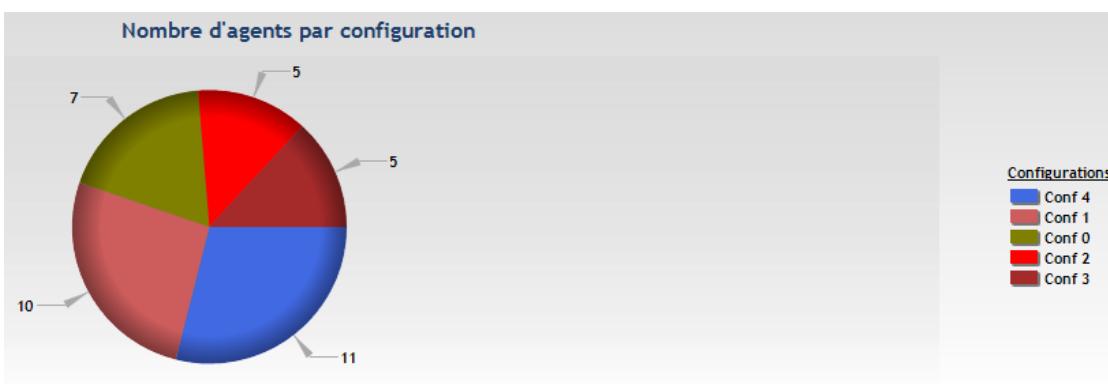
- **Number of agents per policy:**

  This is the security policy applied to the agents.

- **Number of agents per configuration:**
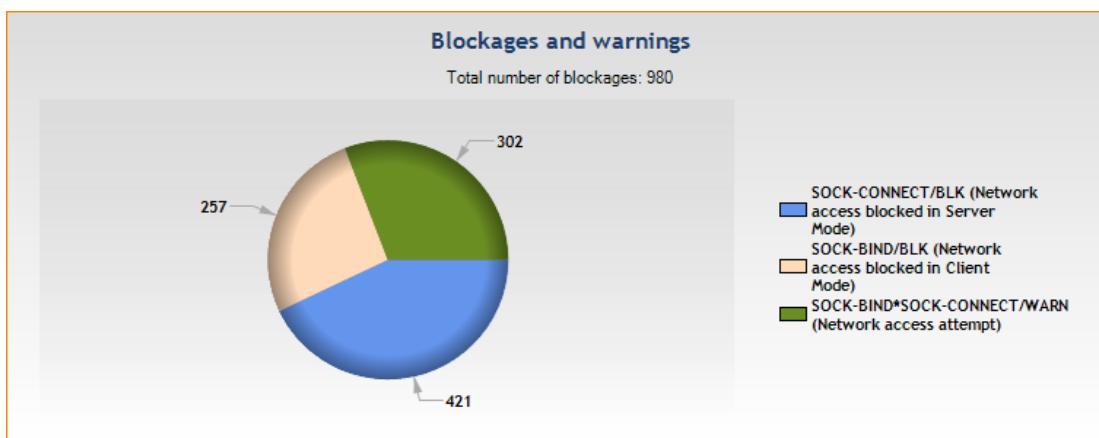
   This is the dynamic configuration policy applied to the agents.
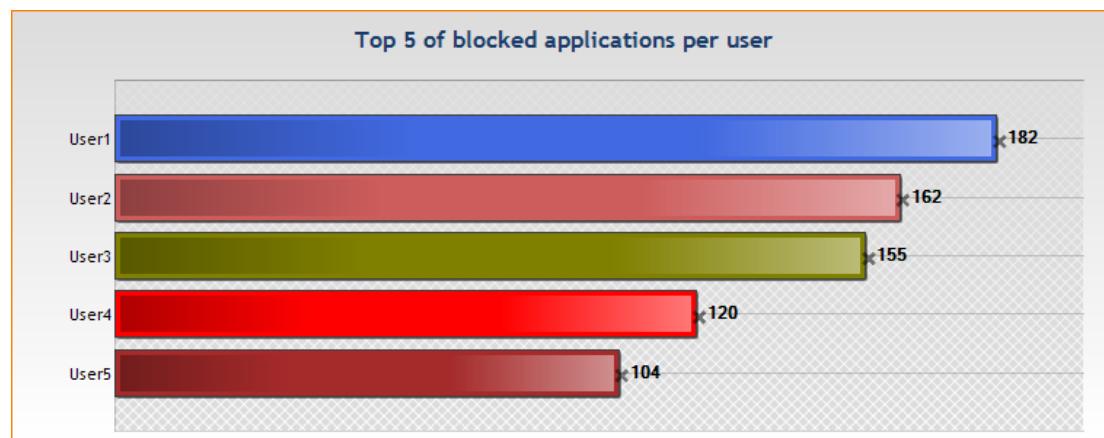
17.3.2 Workstation integrity

These reports summarize blockages and warning logs which have been generated. Results are grouped by types, users and hosts.
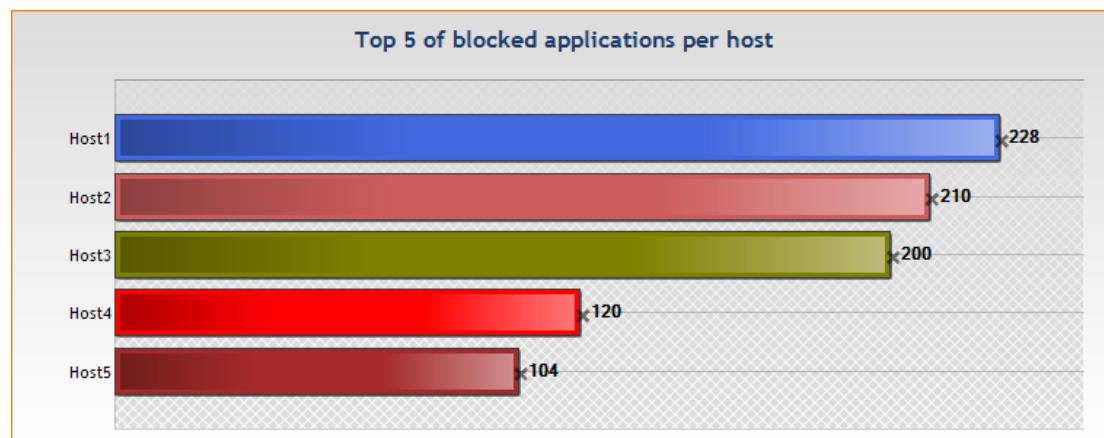
- Blockages and warnings:

- Top [X] of blocked applications per user:

Top 5 of blocked applications per user

User	Value
User1	182
User2	162
User3	155
User4	120
User5	104

- Top [X] of blocked applications per host:

Top 5 of blocked applications per host

Host	Value
Host1	228
Host2	210
Host3	200
Host4	120
Host5	104

- Top [X] of network accesses blocked in Client Mode per user:

Top 5 of network accesses blocked in Client Mode per user

User	Value
User1	56
User2	41
User3	30
User4	25
User5	21

- Top [X] of network accesses blocked in Client Mode per host:

Top 5 of network accesses blocked in Client Mode per host

Host	Value
Host1	1495
Host2	1230
Host3	948
Host4	871
Host5	523

- Top [X] of network accesses blocked in Server Mode per user:

Top 5 of network accesses blocked in Server Mode per user

User	Value
User1	149
User2	114
User3	82
User4	12
User5	8

- Top [X] of network accesses blocked in Server Mode per host:

Top 5 of network accesses blocked in Server Mode per host

Host	Value
Host1	526
Host2	359
Host3	351
Host4	120
Host5	114

- Top [X] of network access attempts per user:
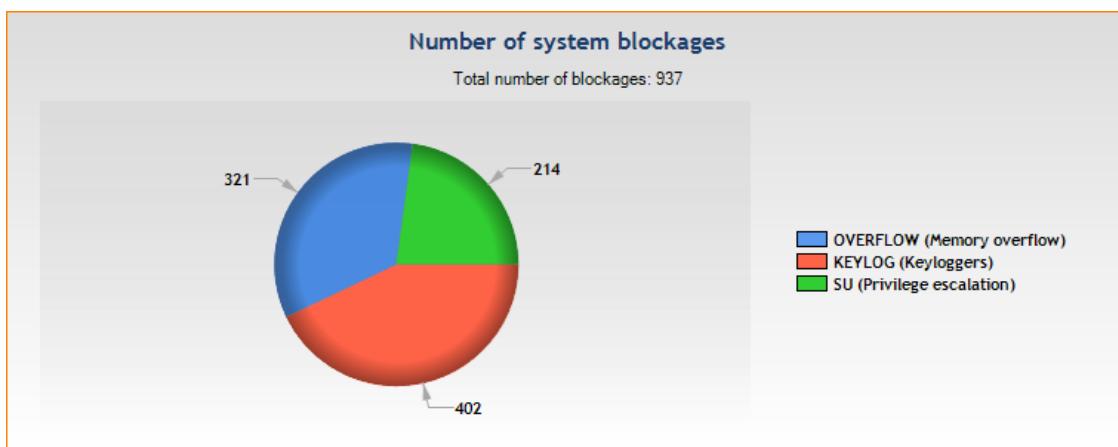
- **Top [x] of network access attempts per host:**
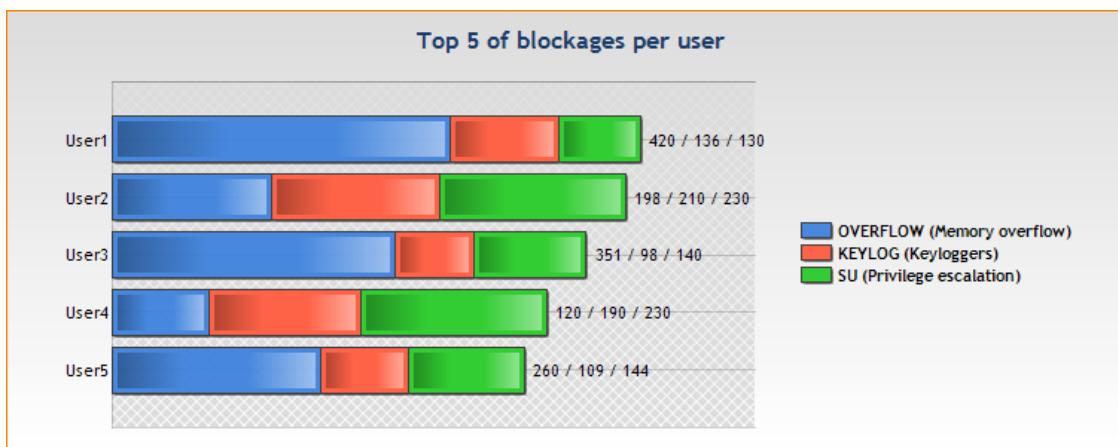
17.3.3 System security

These reports show data related to blockages applied by the agent in order to keep host machines secured. They show the distribution of blockages by types, users and hosts.
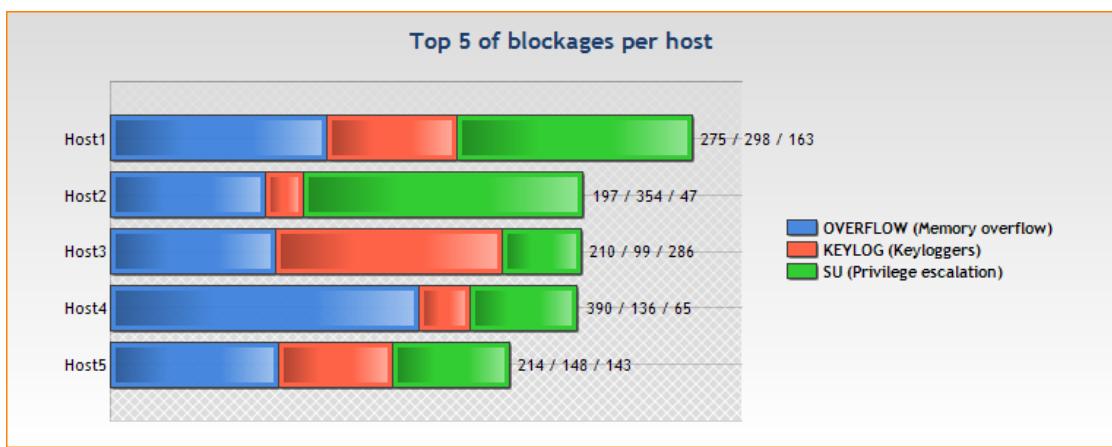
- **Number of system blockages:**

- **Top [X] of blockages per user:**
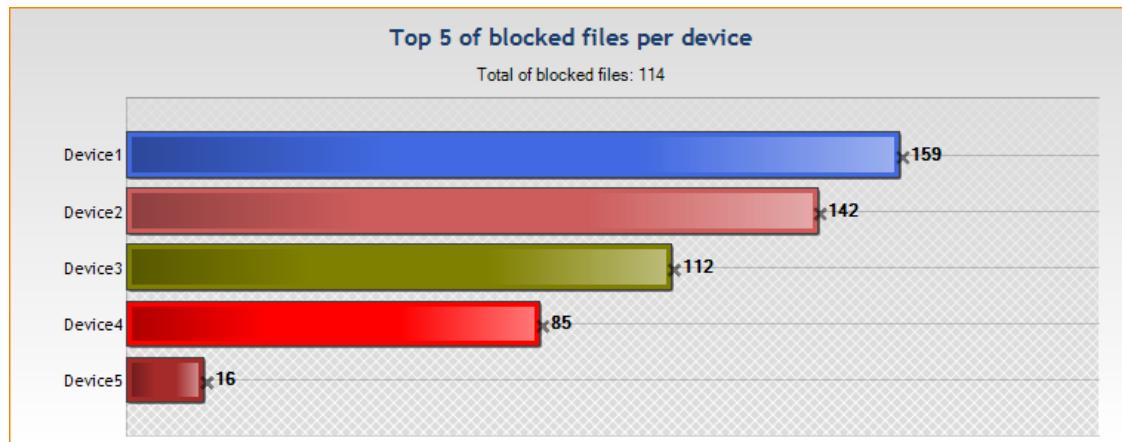
- **Top [X] of blockages per host:**
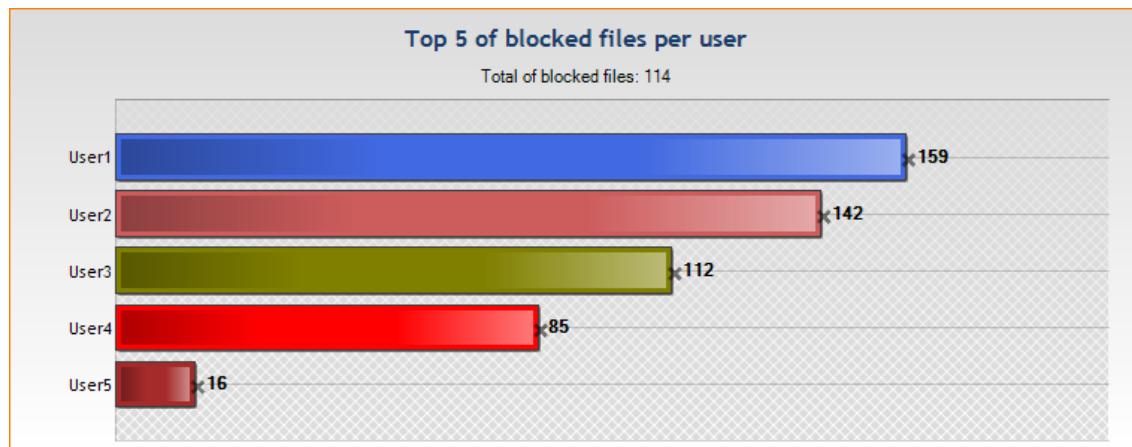
17.3.4 Devices

These reports show statistics about the use of removable devices on agents.
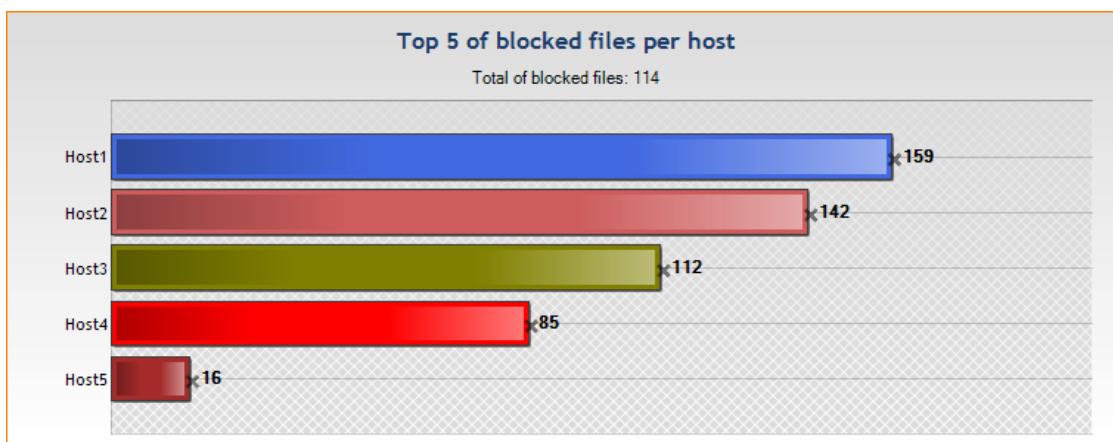
- **Top [X] of blocked files per device:**
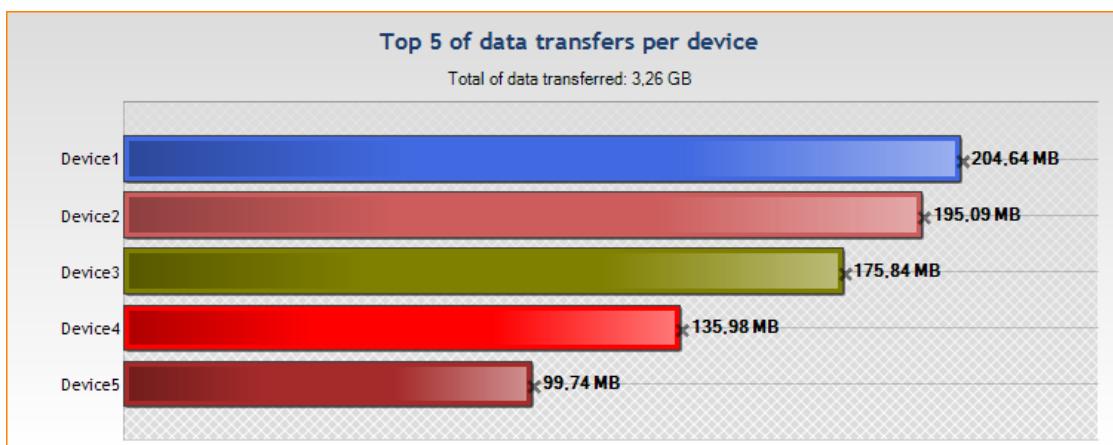
- **Top [X] of blocked files per user:**

- **Top [X] of blocked files per host:**

Top 5 of blocked files per host
Total of blocked files: 114

Host	Value
Host1	159
Host2	142
Host3	112
Host4	85
Host5	16

- **Top [X] of data transfers per device:**

Top 5 of data transfers per device
Total of data transferred: 3,26 GB

Device	Value
Device1	204,64 MB
Device2	195,09 MB
Device3	175,84 MB
Device4	135,98 MB
Device5	99,74 MB

- **Top [X] of data transfers per user:**

Top 5 of data transfers per user
Total of data transferred: 3,26 GB

User	Value
User1	204,64 MB
User2	195,09 MB
User3	175,84 MB
User4	135,98 MB
User5	99,74 MB

- **Top [X] of data transfers per host:**

Top 5 of data transfers per host

Total of data transferred: 3,26 GB

Host	Data
Host1	204.64 MB
Host2	195.09 MB
Host3	175.84 MB
Host4	135.98 MB
Host5	99.74 MB

- **Top [X] of most used devices:**

Top 5 of most used devices

Total number of removed/plugged-in devices: 146

Device	Count
Device1	289
Device2	132
Device3	114
Device4	100
Device5	50

- **Top [X] of users using removable devices:**

Top 5 of users using removable devices

Total number of removed/plugged-in devices: 146

User	Count
User1	289
User2	132
User3	114
User4	100
User5	50

- **Top [X] of hosts using removable devices:**

Top 5 of hosts using removable devices
Total number of removed/plugged-in devices: 146

17.3.5 Licenses

These reports display information about:

- The number of agents deployed (taking into account the Stormshield Endpoint Security package that you have installed).

- The number of licenses that are still available.

17.4 "Table" reports

17.4.1 Agent status

This report summarizes the agents status. It shows the following data:

- Connection state: connection to server state

- Hostname: name of the machine hosting the agent

- Agent version

- Last connection: date and time of the last connection to server

- Username: name of the Windows user connected to the host

- Last User Log: date and time of the last Stormshield Endpoint Security system log

17.4.2 Stormshield Endpoint Security configuration changes

This report shows the modifications applied to configurations and policies from a management console. It shows the following data:

- Id: event identifier

- Date:: date on which the event occurred

- Username: name of the Windows user who made the modification

- Action: see the codes table below

- Type: see the codes table below

- Objects: objects impacted by the modification

Type	Meaning
U	Operation on Users
R	Operation on Roles
E	Operation on the Environment
S	Operation on Servers
M	Operation on Server policy (Master)
N	Operation on Agent group (Network)
C	Operation on Dynamic Agent Configuration policy
CS	Operation on Static Agent Configuration policy
PS	Operation on Security policy
PC	Operation on Encryption policy
T	Operation on Test
A	Operation on Action
B	Operation on Script
F	Operation on File
GA	Operation on Agent collection

ACTION	MEANING
CN	Connection
AD	Addition
RE	Renaming
UP	Update
SE	Synchronization
LA	Link creation
FA	File added
RA	Role added
RU	Role update
DE	Deletion

17.4.3 Stopped agents

This report shows the date on which an agent was stopped It shows the following data:

- Hostname: name of the machine hosting the agent
- Date: date on which the log was generated

17.4.4 Agents' configuration

This report lists the dynamic agent configurations applied to agents. It shows the following data:

- Hostname: name of the machine hosting the agent
- Configuration name: name of the dynamic agent configuration applied
- Date: date on which the log was generated

17.4.5 Agents' policies

This report lists the security policies applied to agents. It shows the following data:

- Hostname: name of the machine hosting the agent
- Policy Name: name of the security policy applied to agents
- Date: date on which the log was generated

17.4.6 Policy Violations by User and Agent

This report shows system logs indicating the agent blocked something. It shows the following data:

- Username: name of the Windows user for whom the log was generated
- Hostname: name of the machine hosting the agent
- Action: indicates what the agent blocked
- Status: block type
- Source: depends on the "Action/Status" pair
- Dest: depends on the "Action/Status" pair
- Rid: id of the rule which generated the log
- Date: date on which the log was generated

Possible "Status" and "Action" combinations and the meaning of the content of the four "Source" fields (Source path, Source MD5, Source SHA-1 and Source sender) and the "Dest" field are:

Status	Action	Description
BLK	ATTACH-PROCESS	Stormshield Endpoint Security prevented a process from attaching to another process. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to attach itself. *Detail field content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) to which the source process attempted to attach itself.
BLK	ACCESS-REG	Stormshield Endpoint Securityprevented a process from accessing a Windows registry key. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to access the registry key. *Detail field content*: path to the key protected by Stormshield Endpoint Security.

Status	Action	Description
BLK	BAD-KEY	The opening of an encrypted file is blocked because the user does not have the correct encryption key. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to open the file. *Detail field content*: absolute path to the encrypted file. Beware: to see this log, you must enable the generation of this log in the database from the Log Manager.
BLK	COPY-PASTE	A process which is not allowed to use Copy/Paste has been blocked. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to "copy". *Detail field content*: same as the Source field. Beware: to see this log, you must enable the generation of this log in the database from the Log Manager.
BLK	CREATE	An attempt by a process to open a file in creation mode has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to open the file. *Detail field content*: absolute path to the file that the source process tried to open.
BLK	DELETE	An attempt to delete a file has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to delete the file. *Detail field content*: absolute path to the file meant to be deleted.
BLK	HOOK	Stormshield Endpoint Security blocked a hook installation attempt. *Detail field content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to install the hook. *Detail field content*: Windows API function blocked.
BLK	LINK	Stormshield Endpoint Security denied the creation of a symbolic link. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to create the symbolic link. *Detail field content*: absolute path to the file.
BLK	LOCK-KEY	An attempt to open an encrypted file has been blocked because the user key is blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to open the file. *Detail field content*: absolute path to the file. Beware: to see this log, you must enable the generation of this log in the database from the Log Manager.
BLK	KEYLOG	A keylogging attempt has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted keylogging. *Detail field content*: Windows API function blocked.
BLK	OPEN	An attempt by a process to open a file has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to open the file. *Detail field content*: absolute path to the file that the process tried to open.

Status	Action	Description
BLK	OPEN-PROCESS	An attempt by a process to open another process in memory has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to open the process. *Detail field content*: Windows API function blocked.
BLK	PROCESS-INFORMATION	An attempt by a process to retrieve data on another process has been blocked. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to retrieve data. *Detail field content*: name of the Windows API blocked.
BLK	REBOOT	An attempt to restart the machine hosting Stormshield Endpoint Securityhas been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to restart the machine. *Detail field content*: privilege type used to restart the machine (SE_SHUTDOWN_PRIVILEGE or SE_REMOTE_SHUTDOWN_PRIVILEGE).
BLK	RENAME	A file renaming attempt has been blocked. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to rename the file. *Detail field content*: absolute path of the file that the source process tried to rename.
BLK	RDISK	An attempt to open a file in creation mode on a removable device has been blocked. *Source fields content*: absolute path to the process which tried to access the removable device. *Detail field content*: description of the device.
BLK	SOCK-ACCEPT	An incoming connection on the host machine has been blocked. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) listening on a port. *Detail field content*: remote host IP address.
BLK	SOCK-BIND	Stormshield Endpoint Security prevented an application from listening on incoming connections. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to listen on incoming connections. *Detail field content*: local IP address.
BLK	SOCK-CONNECT	An outgoing connection on the host machine has been blocked. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to set up a connection. *Detail field content*: remote host IP address.
BLK	SOCK-ICMP	Stormshield Endpoint Security denied the creation of an ICMP connection. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to set up a connection. *Detail field content*: remote host IP address.

Status	Action	Description
BLK	SOCK-RAWIP	Stormshield Endpoint Security denied the creation of a RAW or UDP connection. *Source fields content* : identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to set up a connection. *Detail field content*: remote host IP address.
BLK	SU	A privilege escalation attempt has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to escalate privileges. *Detail field content*: privilege type (SE_LOAD_DRIVER_PRIVILEGE, SE_DEBUG_PRIVILEGE), or the string "Kernel escalation" if the elevation of privilege attempt comes from the kernel side.
BLK	TERMINATE-PROCESS	A process termination attempt has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to shut down a process. *Detail field content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) on which there had been a termination attempt.
BLKCREATE	CREATE	An attempt to create a file has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to open the file. *Detail field content*: absolute path to the file that the source process tried to open.
BLKCREATE	CREATE-PROCESS	An attempt to create a process has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to create a new process. *Detail field content*: absolute path to the process that the source process tried to execute.
INVALID-BLKEXECUTE	CREATE-PROCESS	An attempt to create a process during Windows startup was illegally blocked. *Source fields content*: identifier to the process (identified by certificate) created illegally. The process that was illegally blocked must be identified by path or certificate in order to be properly authorized.
INVALID-EXECUTE	CREATE-PROCESS	An illegal execution occurred during Windows startup. *Source fields content*: identifier to the process (identified by certificate) authorized illegally. The process that was illegally created must be identified by path or certificate in order to be properly blocked.
BLKEXECUTE	EXE_ON_USB	An attempt to launch a process on a removable device has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that attempted to launch a process on the removable device . *Detail field content*: absolute path to the binary file that the source process tried to launch.

Status	Action	Description
BLKEXECUTE	OPEN or CREATE	Attempt to execute a process has been blocked. *Source fields content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) that executed the process. *Detail field content*: identification information for the process (absolute path, certificate issuer, MD5, SHA-1) for which the execution was blocked

17.4.7 Blocked files

This report lists all the blockages related to files which occurred among agents. It shows the following data:

- Hostname: name of the machine hosting the agent
- Action: indicates what the agent blocked
- Status: blockage type
- Source: depends on the couple "Action/Status"
- Dest: depends on the couple "Action/Status"
- Rid: id of the rule which generated the log
- Date: date on which the log was generated

For details about the meaning of the Source and Dest columns, refer to the table of the report **Policies Violations by User and Agent**.

17.4.8 Devices accesses

This report gives an history of write accesses on storage devices. It shows the following data:

- Copy Date: date on which data were written
- Hostname: name of the machine hosting the agent
- Username: name of the Windows user for who the log was generated
- Type: device type on which the operation occurred
- Manufacturer: device manufacturer
- Model: device model
- Serial Number: device serial number
- Copied File: name of the file on which the operation occurred
- Copied Size: size in bytes of copied data

18. Troubleshooting

This chapter explains how to solve technical problems that may arise while using Stormshield Endpoint Security.

18.1 Certificates

18.1.1 The console cannot communicate with the server

If the problem is related to the certificates used to encrypt communications between the server and the console, a specific message is displayed in the **Messages** area in the **Log Manager** menu.

In this case, follow the steps below while respecting the order indicated:

1. Check that the certificates are located in an environment where they can be accessed by both the console and the server.

   If certificates are accessible, the problem is probably due to the certificate itself (example: the certificate has expired).

   The console will indicate the most likely reason for this in the Message column.

2. If there is no certificate problem, check the connectivity between the console and the server:

   ◦ Use ping from the console to test access to the server IP address.

   ◦ If the ping is successful, use telnet on the server address through port 16007 to test the opening of the port used for communication between the console and the server.

3. If connectivity is available, the Stormshield Endpoint Security server is effectively running on the server host machine.

   If connectivity is not available, restart the server.

4. If the problem is solved, send the configuration again.

   The console will display a message verifying that the configuration was sent and that the server received it.

18.1.2 The agent cannot download its certificate

After installation, the agent has to download an X509 certificate to communicate securely with the server.

1. If the agent fails to download its certificate, a message is logged on the workstation.
   This message can be consulted by right-clicking the Stormshield Endpoint Security icon displayed in the taskbar and by selecting View event logs.

   The most common reasons for such a failure are the following:

   ◦ The **Checking server source** option under Authentication Service is enabled on the management console and the agent has been downloaded from another Stormshield Endpoint Security server instance.

     Two solutions can be considered:

     - Reinstall an agent generated by the appropriate server.

     - Disable the **Checking server source** option from the server configuration policy.

○ The certificate deployment period has expired.

The period must be renewed. You can modify it on the management console under **Authentication Service** of the server configuration policy.

2. If the configuration is correct and the agent still cannot download its certificate:

○ Check the communication by sending a ping to the Stormshield Endpoint Security server IP address from the workstation.

○ Stop the Stormshield Endpoint Security server.

○ Run telnet on port 443.

The connection should fail.

3. If the connection is established, this means that another Web server is present on the server host. Stop this server, and start the Stormshield Endpoint Security server again.

When the problem is solved, check that the agent actually downloads its certificate.

18.1.3 Unable to download certificates manually

If you cannot access the certificate downloading page, make sure that another Web server is not already running the server host.

If manual download fails, one of the following error messages is displayed:

- `Wrong login or password`:

  The login and/or password that have been entered do not match with those defined on the management console.

- `The server is unable to respond to your request (server is locked)`:

  The server is locked. Try again later.

- `An internal error occurred. Please contact your administrator`:

  An internal error occurred. Server logs should be analyzed in order to diagnose the origin of the problem.

18.2 Configurations

18.2.1 Unable to apply the configuration

The simplest way to check that a security configuration has been properly applied to a client workstation is to attempt an operation explicitly banned by a rule defined on the management console.

A good example is the rule that bans the use of Windows notepad (`notepad.exe`) to open a file with a `.txt` extension.

1. If the blocking rule works, the application will not be allowed to access the file.

2. If the blocking rule is not applied, check the following:

○ The configuration has been assigned to the target machine by the management console.

○ The Stormshield Endpoint Security agent is running on the client workstation.

To do so, verify the Stormshield Endpoint Security Agent service status.

If the service is not found in the list of Windows services, there has probably been a problem with agent installation.

Correct installation is shown in the following file:

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\srservice.log
```

3. After verifying that the security configuration has been applied to the client workstation, check that the data collected by the agent:

    ◦ Has effectively been sent to the server.

    ◦ Has effectively been stored in the database.

    ◦ Is accessible to the console.

    This data must be visible in the **Log Manager** menu on the management console.

4. If no data is displayed on the console, check database connection.

    If the console cannot connect to the database, a message indicates this on opening the console.

5. When no connection to the database is available, you should check:

    ◦ The database server accessibility by sending a ping to the machine that hosts the database.

    ◦ The database engine is started (via the services or taskbar icon).

6. If the database engine is running and the host machine is accessible, check the connection data that is specific to the Stormshield Endpoint Security database.

    To do so, verify the password in the **Database password** field and the IP address in the **SQL server instance** field in the server configuration policy.

7. If the connection to the database is active, verify that event feedback is properly configured on the console under **Configuration** in the **Console Manager** section.

    When the connection to the database is active, you can generate a log to check that the configuration has been correctly applied to the client workstation:

    ◦ Trigger rule application on the client workstation once again.

    ◦ Check data feedback.

    ◦ Check the frequency of configuration updates which is also the frequency of event feedback.

    ⚠ **WARNING**
    Avoid updating too frequently as this may cause network saturation.

18.3 Miscellaneous

18.3.1 Incorrect installation of the Stormshield Endpoint Security agent

You must use the **Administrator** account to install the Stormshield Endpoint Security agent.

If you use another account:

*   The installation starts but not all of the files are copied.

*   The service is not registered.

*   Nothing works (including the uninstaller).

To fix the problem, you must manually remove all of the Stormshield Endpoint Security files and registry keys.

⚠ **WARNING**

Before installing the agent, make sure that the Windows XP embedded firewall has been disabled.

18.3.2 Agent fails to be remotely deployed

When the **srdeployment** assistant fails to deploy the agent, the error message `Host unreachable` is displayed on the console.

In this case, follow the steps below while respecting the order indicated:

1. Send a `ping` command to the host IP address.
2. Check that the host netbios `C$` share is accessible.
3. Check that Use simple file sharing is disabled.
4. Check that port `445` can be accessed by sending a `telnet` command.
5. Check that there is no connection to the host which is already open.
6. Repeat the agent deployment procedure.

18.3.3 Hardware conflicts

Conflicts between drivers may sometimes cause a system crash called **BSoD** (Blue Screen of Death).
To determine the cause of the conflict, it is recommended to enable a Windows service that keeps a trace of system activity at the time of the crash.

This service is accessible from the **System Properties** panel on your workstation:

1. Click the *Advanced* tab.
2. Click **Settings** in the Startup and Recovery group.
3. From the Write debugging information group, select **Complete memory dump**.
4. Keep the default directory `%SystemRoot%\MEMORY.DMP`.

    `%SystemRoot%` usually corresponds to `c:\windows\` in Windows XP.

18.3.4 Degraded performance

Stormshield Endpoint Security operation has no significant impact on client workstation performance.

However, an application may repeatedly attempt to perform an operation that is blocked by Stormshield Endpoint Security . This in turn may cause CPU overload.

If workstation performance drops, it is first of all necessary to check the affected process by opening the Windows **Task Manager**.

If the affected process is indeed blocked by Stormshield Endpoint Security , a trace of the blockage will be recorded in one of the agent log files. Checking the logs will show whether the cause of the problem was indeed triggered by a Stormshield Endpoint Security -imposed blockage.

18.3.5 StopAgent does not work and/or Stormshield Endpoint Security cannot be updated

The issue may occur under Windows Server 2003 SP2 or R2 SP2.

The agent Stormshield Endpoint Security is not able to apply updates or to run StopAgent (if authorized) if it cannot verify the whole certificate chain.

However Windows Server 2003 SP2 or R2 SP2 may not have the root certificate of VeriSign, the authority releasing Stormshield Endpoint Security signature certificate.

Ensure the up-to-date VeriSign root certificates are in the **Trusted Root Certification Authorities** Windows store.

If not, the following error logs display in the *software.sro* file:

- [PIPE_ADD_REGISTERED_FUNCTION STOPAGENT::LOGACCESSDENIED friendlyname=sr_ stopagent error : 0x800b010a]

- [An error occurred while applying a patch]

18.3.6 Tracing on the agent and server

Tracing on the Stormshield Endpoint Security agent and server in Windows 7 versions and upwards

Whenever the Stormshield Endpoint Security agent behaves unexpectedly, the trace manager makes it possible to help technical support to establish a diagnosis and resolve the issue.
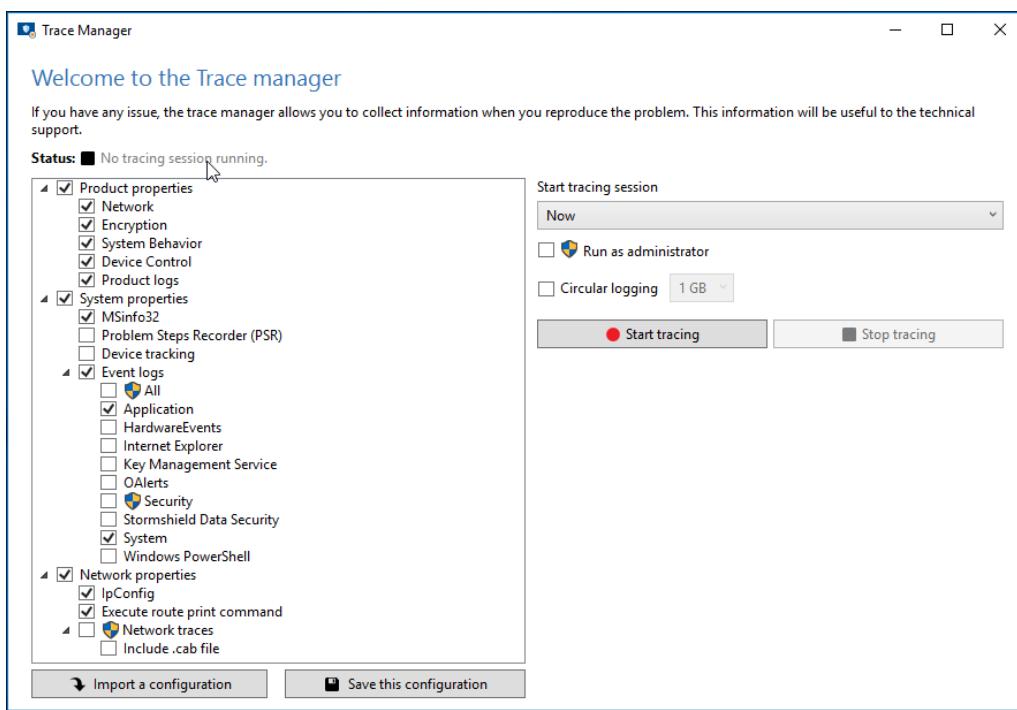
It allows tracing actions on an agent or server via a graphical interface or command line interface.

The following are instructions for users on how to save traces.

Tracing from the graphical interface

To open the Trace manager:

- On a server, double-click on the executable file *eir.exe* in the Stormshield Endpoint Security server's folder,

- On an agent, right-click on the Stormshield Endpoint Security agent icon in the taskbar and select **Other operations** > **Start trace manager**.

To start tracing:

1. In the panel on the left, select the items for which you wish to collect traces.

2. Click on **Start tracing.**

3. Repeat the actions which caused the unexpected behavior of the agent or server.

4. Click on **Stop tracing.**

5. Write a comment if needed.

6. Wait for the end of the process.

7. When the archive is created, the save window opens. Save the archive. All the data recorded is in the archive.

8. Forward this archive to technical support.

Tracing from the command line interface

Traces can be collected via the command line interface without any interaction with the user.

To start tracing:

1. Open a command prompt in the agent's or server's installation folder.

2. Run the command `EirCmd.exe start resultFilePath="path\example.zip"` to start tracing and define the name and location of the trace archive.

3. Use the command `EirCmd.exe stop` to stop tracing.

4. Use the command `EirCmd.exe status` to find out the current status of the tracing operation.

> **ℹ NOTE**
> The trace manager cannot be used from the command line interface if simultaneously, items to be collected require administrator privileges, and if the tracing operation requires the workstation to be rebooted.

Saving and importing the configuration of the trace manager

- Once you have selected items from the left panel in the trace manager's graphical interface, and you have defined your preferences in the section on the right, you can save your configuration by clicking on **Save this configuration**.
  It will be saved in *.econf* format.

- To use a configuration that was saved earlier:
  - Double-click on a *.econf* file to open the trace manager's graphical interface
    -or-
  - Click on **Import a configuration** from the trace manager's graphical interface
    -or-
  - Indicate the *.econf* file un the `configFilePath` parameter in the command line in order to start tracing : `EirCmd.exe start resultFilePath="path\example.zip" [configFilePath="path\example.econf"]`.

Tracing on the Stormshield Endpoint Security agent in Windows XP

The tracing tool cannot be used at startup on Microsoft Windows XP clients.

To use the tool:

1. Right-click on the Stormshield Endpoint Security agent icon in the taskbar and select **Other operations** > **Start trace manager**.
2. Click the settings icon and select the traces you want to save. By default all traces are checked and tracing will be done immediately only once.
3. Start tracing.
4. Repeat the actions which caused the unexpected behavior of the agent.
5. Stop tracing.
6. Write a comment if needed.
7. Wait for the process to end: various commands will be running to retrieve all the information required about the machine as well as network configuration data. The technical support teams needs them to analyze the problem.
8. When the archive is created, the save window opens. Save the archive. All the data recorded is in the archive.
9. Forward this archive to technical support.

> **ℹ NOTE**
> Only the technical support team can work on the trace file (extension *.etl*).

Appendix A. Protocols

Here is the protocol correspondence table:

Code	Meaning
[0x0004]	"0004/IEEE 802.3 packet"
[0x0101]	"0101-1FF/Experimental"
[0x0200]	"0200/Xerox PUP protocol - see 0A00"
[0x0200]	"0200/PUP Address Translation - see 0A01"
[0x0500]	"0500/Protocol Unavailable"
[0x0400]	"0400/Nixdorf"
[0x0600]	"0600/XNS"
[0x0601]	"0601/XNS Address Translation (3Mb only)"
[0x0660]	"0660/DLOG (?)"
[0x0661]	"0661/DLOG (?)"
[0x0800]	"0800/IP protocol"
[0x0801]	"0801/X.75 Internet"
[0x0802]	"0802/NBS Internet"
[0x0803]	"0803/ECMA Internet"
[0x0804]	"0804/CHAOSnet"
[0x0805]	"0805/X.25 Level 3"
[0x0806]	"0806/Address resolution protocol"
[0x0807]	"0807/XNS Compatibility"
[0x0808]	"0808/Frame Relay ARP (RFC1701)"
[0x081C]	"081C/Symbolics Private"
[0x0888]	"0888-088A/Xyplex"
[0x0900]	"0900/Ungermann-Bass network debugger"
[0x0A00]	"0A00/Xerox IEEE802.3 PUP"
[0x0A01]	"0A01/Xerox IEEE802.3 PUP Address Translation"
[0x0BAD]	"0BAD/Banyan VINES"
[0x0BAE]	"0BAE/Banyan VINES Loopback"
[0x0BAF]	"0BAF/Banyan VINES Echo"
[0x1000]	"1000/Trailer packet"
[0x1234]	"1234/DCA - Multicast"
[0x1600]	"1600/VALID system protocol"
[0x1989]	"1989/Artificial Horizons (\"Aviator\" dogfight simulator [on Sun])"

Code	Meaning
[0x1995]	"1995/Datapoint Corporation (RCL lan protocol)"
[0x3C00]	"3C00/3Com NBP virtual circuit datagram (like XNS SPP) not registered"
[0x3C01]	"3C01/3Com NBP System control datagram not registered"
[0x3C02]	"3C02/3Com NBP Connect request (virtual cct) not registered"
[0x3C03]	"3C03/3Com NBP Connect response not registered"
[0x3C04]	"3C04/3Com NBP Connect complete not registered"
[0x3C05]	"3C05/3Com NBP Close request (virtual cct) not registered"
[0x3C06]	"3C06/3Com NBP Close response not registered"
[0x3C07]	"3C07/3Com NBP Datagram (like XNS IDP) not registered"
[0x3C08]	"3C08/3Com NBP Datagram broadcast not registered"
[0x3C09]	"3C09/3Com NBP Claim NetBIOS name not registered"
[0x3C0A]	"3C0A/3Com NBP Delete Netbios name not registered"
[0x3C0B]	"3C0B/3Com NBP Remote adaptor status request not registered"
[0x3C0C]	"3C0C/3Com NBP Remote adaptor response not registered"
[0x3C0D]	"3C0D/3Com NBP Reset not registered"
[0x4242]	"4242/PCS Basic Block Protocol"
[0x424C]	"424C/Information Modes Little Big LAN diagnostic"
[0x4321]	"4321/THD - Diddle"
[0x4C42]	"4C42/Information Modes Little Big LAN"
[0x5208]	"5208/BBN Simnet Private"
[0x6000]	"6000/DEC Unassigned, experimental"
[0x6001]	"6001/DEC MOP dump/load"
[0x6002]	"6002/DEC MOP remote console"
[0x6003]	"6003/DEC DECNET Phase IV route"
[0x6004]	"6004/DEC LAT"
[0x6005]	"6005/DEC diagnostic protocol (at interface initialization?)"
[0x6006]	"6006/DEC customer protocol"
[0x6007]	"6007/DEC LAVC, SCA"
[0x6008]	"6008/DEC AMBER"
[0x6009]	"6009/DEC MUMPS"
[0x6010]	"6010-6014/3Com Corporation"
[0x6558]	"6558/Trans Ether Bridging (RFC1701)"
[0x6559]	"6559/Raw Frame Relay (RFC1701)"
[0x7000]	"7000/Ungermann-Bass download"

Code	Meaning
[0x7001]	"7001/Ungermann-Bass NIUs"
[0x7002]	"7002/Ungermann-Bass diagnostic/loopback"
[0x7003]	"7003/Ungermann-Bass ??? (NMC to/from UB Bridge)"
[0x7005]	"7005/Ungermann-Bass Bridge Spanning Tree"
[0x7007]	"7007/OS/9 Microware"
[0x7009]	"7009/OS/9 Net?"
[0x7020]	"7020-7029/LRT (England) (now Sintrom)"
[0x7030]	"7030/Racal-Interlan"
[0x7031]	"7031/Prime NTS (Network Terminal Service)"
[0x7034]	"7034/Cabletron"
[0x8003]	"8003/Cronus VLN"
[0x8004]	"8004/Cronus Direct"
[0x8005]	"8005/HP Probe"
[0x8006]	"8006/Nestar"
[0x8008]	"8008/AT&T/Stanford (local use)"
[0x8010]	"8010/Excelan"
[0x8013]	"8013/SGI diagnostic type"
[0x8014]	"8014/SGI network games"
[0x8015]	"8015/SGI reserved type"
[0x8016]	"8016/SGI bounce server"
[0x8019]	"8019/Apollo DOMAIN"
[0x802E]	"802E/Tymeshare"
[0x802F]	"802F/Tigan, Inc."
[0x8035]	"8035/Reverse addr resolution protocol"
[0x8036]	"8036/Aeonic Systems"
[0x8037]	"8037/IPX (Novell Netware?)"
[0x8038]	"8038/DEC LANBridge"
[0x8039]	"8039/DEC DSM/DDP"
[0x803A]	"803A/DEC Argonaut Console"
[0x803B]	"803B/DEC VAXELN"
[0x803C]	"803C/DEC DNS Naming Service"
[0x803D]	"803D/DEC Ethernet Encryption"
[0x803E]	"803E/DEC Distributed Time Service"
[0x803F]	"803F/DEC LAN Traffic Monitor"

Code	Meaning
[0x8040]	"8040/DEC PATHWORKS DECnet NETBIOS Emulation"
[0x8041]	"8041/DEC Local Area System Transport"
[0x8042]	"8042/DEC Unassigned"
[0x8044]	"8044/Planning Research Corp."
[0x8046]	"8046-8047/AT&T"
[0x8048]	"8048/DEC Availability Manager for Distributed Systems DECamds (but someone at DEC says not)"
[0x8049]	"8049/ExperData"
[0x805B]	"805B/Stanford V Kernel exp."
[0x805C]	"805C/Stanford V Kernel prod."
[0x805D]	"805D/Evans & Sutherland"
[0x8060]	"8060/Little Machines"
[0x8062]	"8062/Counterpoint Computers"
[0x8065]	"8065-8066/Univ. of Mass @ Amherst"
[0x8067]	"8067/Veeco Integrated Auto."
[0x8068]	"8068/General Dynamics"
[0x8069]	"8069/AT&T"
[0x806A]	"806A/Autophon"
[0x806C]	"806C/ComDesign"
[0x806D]	"806D/Compugraphic Corporation"
[0x806E]	"806E-8077/Landmark Graphics Corp."
[0x807A]	"807A/Matra"
[0x807B]	"807B/Dansk Data Elektronik"
[0x807C]	"807C/Merit Internodal (or Univ of Michigan?)"
[0x807D]	"807D-807F/Vitalink Communications"
[0x8080]	"8080/Vitalink TransLAN III Management"
[0x8081]	"8081-8083/Counterpoint Computers"
[0x8088]	"8088-808A/Xyplex"
[0x809B]	"809B/AppleTalk"
[0x809C]	"809C-809E/Datability"
[0x809F]	"809F/Spider Systems Ltd."
[0x80A3]	"80A3/Nixdorf"
[0x80A4]	"80A4-80B3/Siemens Gammasonics Inc."
[0x80C0]	"80C0-80C3/DCA (Digital Comm. Assoc.) Data Exchange Cluster"

Code	Meaning
[0x80C4]	"80C4-80C5/Banyan Systems"
[0x80C6]	"80C6/Pacer Software"
[0x80C7]	"80C7/Applitek Corporation"
[0x80C8]	"80C8-80CC/Intergraph Corporation"
[0x80CD]	"80CD-80CE/Harris Corporation"
[0x80CF]	"80CF-80D2/Taylor Instrument"
[0x80D3]	"80D3-80D4/Rosemount Corporation"
[0x80D5]	"80D5/IBM SNA Services over Ethernet"
[0x80DD]	"80DD/Varian Associates"
[0x80DE]	"80DE-80DF/TRFS (Integrated Solutions Transparent Remote File System)"
[0x80E0]	"80E0-80E3/Allen-Bradley"
[0x80E4]	"80E4-80F0/Datability"
[0x80F2]	"80F2/Retix"
[0x80F3]	"80F3/AppleTalk AARP"
[0x80F4]	"80F4-80F5/Kinetics"
[0x80F7]	"80F7/Apollo Computer"
[0x8100]	"8100/IEEE 802.1Q VLAN tagging (XXX conflicts)"
[0x80FF]	"80FF-8101/Wellfleet Communications (XXX conflicts)"
[0x8102]	"8102/Wellfleet BOFL (Breath OF Life) pkts [every 5-10 secs.]"
[0x8103]	"8103/Wellfleet Communications"
[0x8107]	"8107-8109/Symbolics Private"
[0x812B]	"812B/Talaris"
[0x8130]	"8130/Waterloo Microsystems Inc. (XXX which?)"
[0x8130]	"8130/Hayes Microcomputers (XXX which?)"
[0x8131]	"8131/VG Laboratory Systems"
[0x8132]	"8132-8137/Bridge Communications"
[0x8137]	"8137/Novell (old) NetWare IPX (ECONFIG E option)"
[0x8138]	"8138/Novell, Inc."
[0x8139]	"8139-813D/KTI"
[0x813F]	"813F/M/MUMPS data sharing"
[0x8145]	"8145/Vrije Universiteit (NL) Amoeba 4 RPC (obsolete)"
[0x8146]	"8146/Vrije Universiteit (NL) FLIP (Fast Local Internet Protocol)"
[0x8147]	"8147/Vrije Universiteit (NL) [reserved]"
[0x8148]	"8148/Logicraft"

Code	Meaning
[0x8149]	"8149/Network Computing Devices"
[0x814A]	"814A/Alpha Micro"
[0x814C]	"814C/SNMP over Ethernet (see RFC1089)"
[0x814D]	"814D-814E/BIIN"
[0x814F]	"814F/Technically Elite Concepts"
[0x8150]	"8150/Rational Corp"
[0x8151]	"8151-8153/Qualcomm"
[0x815C]	"815C-815E/Computer Protocol Pty Ltd"
[0x8164]	"8164-8166/Charles River Data Systems"
[0x817D]	"817D/Protocol Engines XTP"
[0x817E]	"817E/SGI/Time Warner prop."
[0x8180]	"8180/HIPPI-FP encapsulation"
[0x8181]	"8181/Scheduled Transfer STP, HIPPI-ST"
[0x8182]	"8182-8183/Reserved for HIPPI-6400"
[0x8184]	"8184-818C/SGI prop."
[0x818D]	"818D/Motorola"
[0x8191]	"8191/PowerLAN NetBIOS/NetBEUI (PC)"
[0x819A]	"819A-81A3/RAD Network Devices"
[0x81B7]	"81B7-81B9/Xyplex"
[0x81CC]	"81CC-81D5/Apricot Computers"
[0x81D6]	"81D6-81DD/Artisoft Lantastic"
[0x81E6]	"81E6-81EF/Polygon"
[0x81F0]	"81F0-81F2/Comsat Labs"
[0x81F3]	"81F3-81F5/SAIC"
[0x81F6]	"81F6-81F8/VG Analytical"
[0x8203]	"8203-8205/QNX Software Systems Ltd."
[0x8221]	"8221-8222/Ascom Banking Systems"
[0x823E]	"823E-8240/Advanced Encryption Systems"
[0x8263]	"8263-826A/Charles River Data Systems"
[0x827F]	"827F-8282/Athena Programming"
[0x829A]	"829A-829B/Inst Ind Info Tech"
[0x829C]	"829C-82AB/Taurus Controls"
[0x82AC]	"82AC-8693/Walker Richer & Quinn"
[0x8390]	"8390/Accton Technologies (unregistered)"

Code	Meaning
[0x852B]	"852B/Talaris multicast"
[0x8582]	"8582/Kalpana"
[0x8694]	"8694-869D/Idea Courier"
[0x869E]	"869E-86A1/Computer Network Tech"
[0x86A3]	"86A3-86AC/Gateway Communications"
[0x86DB]	"86DB/SECTRA"
[0x86DD]	"86DD/IP protocol version 6"
[0x86DE]	"86DE/Delta Controls"
[0x86DF]	"86DF/ATOMIC"
[0x86E0]	"86E0-86EF/Landis & Gyr Powers"
[0x8700]	"8700-8710/Motorola"
[0x8739]	"8739/Control Technology Inc. RDP Without IP"
[0x873A]	"873A/Control Technology Inc. Mcast Industrial Ctrl Proto."
[0x873B]	"873B-873C/Control Technology Inc. Proprietary"
[0x876B]	"876B/TCP/IP Compression (RFC1701)"
[0x876C]	"876C/IP Autonomous Systems (RFC1701)"
[0x876D]	"876D/Secure Data (RFC1701)"
[0x8808]	"8808/802.3x flow control packet"
[0x880B]	"880B/PPP (obsolete by PPPOE)"
[0x8820]	"8820/Hitachi Cable (Optoelectronic Systems Laboratory)"
[0x8847]	"8847/MPLS Unicast"
[0x8848]	"8848/MPLS Multicast"
[0x8856]	"8856/Axis Communications AB proprietary bootstrap/config"
[0x8863]	"8863/PPP Over Ethernet Discovery Stage"
[0x8864]	"8864/PPP Over Ethernet Session Stage"
[0x8888]	"8888/HP LanProbe test?"
[0x9000]	"9000/Loopback: used to test interfaces"
[0x9001]	"9001/3Com (Formerly Bridge Communications), XNS Systems Management"
[0x9002]	"9002/3Com (Formerly Bridge Communications), TCP/IP Systems Management"
[0x9003]	"9003/3Com (Formerly Bridge Communications), loopback detection"
[0xAAAA]	"AAAA/DECNET? Used by VAX 6220 DEBNI"
[0xFAF5]	"FAF5/Sonix Arpeggio"
[0xFF00]	"FF00/BBN VITAL-LanBridge cache wakeups"
[0x0]	"HOPOPT/IPv6 Hop-by-Hop Option"

Code	Meaning
[0x1]	"ICMP/Internet Control Message"
[0x2]	"IGMP/Internet Group Management"
[0x3]	"GGP/Gateway-to-Gateway"
[0x4]	"IP/IP in IP encapsulation"
[0x5]	"ST/Stream"
[0x6]	"TCP/Transmission Control"
[0x7]	"CBT/CBT"
[0x8]	"EGP/Exterior Gateway Protocol"
[0x9]	"IGP/any private interior gateway"
[0xa]	"BBN-RCC-MON/BBN RCC Monitoring"
[0xb]	"NVP-II/Network Voice Protocol"
[0xc]	"PUP/PUP"
[0xd]	"ARGUS/ARGUS"
[0xe]	"EMCON/EMCON"
[0xf]	"XNET/Cross Net Debugger"
[0x10]	"CHAOS/Chaos"
[0x11]	"UDP/User Datagram"
[0x12]	"MUX/Multiplexing"
[0x13]	"DCN-MEAS/DCN Measurement Subsystems"
[0x14]	"HMP/Host Monitoring"
[0x15]	"PRM/Packet Radio Measurement"
[0x16]	"XNS-IDP/XEROX NS IDP"
[0x17]	"TRUNK-1/Trunk-1"
[0x18]	"TRUNK-2/Trunk-2"
[0x19]	"LEAF-1/Leaf-1"
[0x1a]	"LEAF-2/Leaf-2"
[0x1b]	"RDP/Reliable Data Protocol"
[0x1c]	"IRTP/Internet Reliable Transaction"
[0x1d]	"ISO-TP4/ISO Transport Protocol Class 4"
[0x1e]	"NETBLT/Bulk Data Transfer Protocol"
[0x1f]	"MFE-NSP/MFE Network Services Protocol"
[0x20]	"MERIT-INP/MERIT Internodal Protocol"
[0x21]	"SEP/Sequential Exchange Protocol"
[0x22]	"3PC/Third Party Connect Protocol"

Code	Meaning
[0x23]	"IDPR/Inter-Domain Policy Routing Protocol"
[0x24]	"XTP/XTP"
[0x25]	"DDP/Datagram Delivery Protocol"
[0x26]	"IDPR-CMTP/IDPR Control Message Transport Proto"
[0x27]	"TP++/TP++ Transport Protocol"
[0x28]	"IL/IL Transport Protocol"
[0x29]	"IPv6/"
[0x2a]	"SDRP/Source Demand Routing Protocol"
[0x2b]	"IPv6-Route/Routing Header for IPv6"
[0x2c]	"IPv6-Frag/Fragment Header for IPv6"
[0x2d]	"IDRP/Inter-Domain Routing Protocol"
[0x2e]	"RSVP/Reservation Protocol"
[0x2f]	"GRE/General Routing Encapsulation"
[0x30]	"MHRP/Mobile Host Routing Protocol"
[0x31]	"BNA/"
[0x32]	"ESP/Encap Security Payload"
[0x33]	"AH/Authentication Header"
[0x34]	"I-NLSP/Integrated Net Layer Security TUBA"
[0x35]	"SWIPE/IP with Encryption"
[0x36]	"NARP/NBMA Address Resolution Protocol"
[0x37]	"MOBILE/IP Mobility"
[0x38]	"TLSP/Transport Layer Security Protocol using Kryptonet key management"
[0x39]	"SKIP/SKIP"
[0x3a]	"IPv6-ICMP/ICMP for IPv6"
[0x3b]	"IPv6-NoNxt/No Next Header for IPv6"
[0x3c]	"IPv6-Opts/Destination Options for IPv6"
[0x3d]	"any host internal protocol"
[0x3e]	"CFTP/CFTP"
[0x3f]	"any local network"
[0x40]	"SAT-EXPAK/SATNET and Backroom EXPAK"
[0x41]	"KRYPTOLAN/"
[0x42]	"RVD/MIT Remote Virtual Disk Protocol"
[0x43]	"IPPC/Internet Pluribus Packet Core"
[0x44]	"any distributed file system"

Code	Meaning
[0x45]	"SAT-MON/SATNET Monitoring"
[0x46]	"VISA/VISA Protocol"
[0x47]	"IPCV/Internet Packet Core Utility"
[0x48]	"CPNX/Computer Protocol Network Executive"
[0x49]	"CPHB/Computer Protocol Heart Beat"
[0x4a]	"WSN/Wang Span Network"
[0x4b]	"PVP/Packet Video Protocol"
[0x4c]	"BR-SAT-MON/Backroom SATNET Monitoring"
[0x4d]	"SUN-ND/SUN ND PROTOCOL-Temporary"
[0x4e]	"WB-MON/WIDEBAND Monitoring"
[0x4f]	"WB-EXPAK/WIDEBAND EXPAK"
[0x50]	"ISO-IP/ISO Internet Protocol"
[0x51]	"VMTP"
[0x52]	"SECURE-VMTP/SECURE-VMTP"
[0x53]	"VINES"
[0x54]	"TTP"
[0x55]	"NSFNET-IGP/NSFNET-IGP"
[0x56]	"DGP/Dissimilar Gateway Protocol"
[0x57]	"TCF"
[0x58]	"EIGRP"
[0x59]	"OSPFIGP"
[0x5a]	"Sprite-RPC/Sprite RPC Protocol"
[0x5b]	"LARP/Locus Address Resolution Protocol"
[0x5c]	"MTP/Multicast Transport Protocol"
[0x5d]	"AX.25/AX.25 Frames"
[0x5e]	"IPIP/IP-within-IP Encapsulation Protocol"
[0x5f]	"MICP/Mobile Internetworking Control Pro."
[0x60]	"SCC-SP/Semaphore Communications Sec. Pro."
[0x61]	"ETHERIP/Ethernet-within-IP Encapsulation"
[0x62]	"ENCAP/Encapsulation Header"
[0x63]	"any private encryption scheme"
[0x64]	"GMTP"
[0x65]	"IFMP/Ipsilon Flow Management Protocol"
[0x66]	"PNNI/PNNI over IP"

Code	Meaning
[0x67]	"PIM/Protocol Independent Multicast"
[0x68]	"ARIS"
[0x69]	"SCPS"
[0x6a]	"QNX"
[0x6b]	"A/N/Active Networks"
[0x6c]	"IPComp/IP Payload Compression Protocol"
[0x6d]	"SNP/Sitara Networks Protocol"
[0x6e]	"Compaq-Peer/Compaq Peer Protocol"
[0x6f]	"IPX-in-IP"
[0x70]	"VRRP/Virtual Router Redundancy Protocol"
[0x71]	"PGM/PGM Reliable Transport Protocol"
[0x72]	"any 0-hop protocol"
[0x73]	"L2TP/Layer Two Tunneling Protocol"
[0x74]	"DDX/D-II Data Exchange DDX"
[0x75]	"IATP/Interactive Agent Transfer Protocol"
[0x76]	"STP/Schedule Transfer Protocol"
[0x77]	"SRP/SpectraLink Radio Protocol"
[0x78]	"UTI"
[0x79]	"SMP/Simple Message Protocol"
[0x7a]	"SM"
[0x7b]	"PTP/Performance Transparency Protocol"
[0x7c]	"ISIS over IPv4"
[0x7d]	"FIRE"
[0x7e]	"CRTP/Combat Radio Transport Protocol"
[0x7f]	"CRUDP/Combat Radio User Datagram"
[0x80]	"SSCOPMCE"
[0x81]	"IPLT"
[0x82]	"SPS/Secure Packet Shield"
[0x83]	"PIPE/Private IP Encapsulation within IP"
[0x84]	"SCTP/Stream Control Transmission Protocol"
[0x85]	"FC/Fibre Channel"
[0x86]	"RSVP-E2E-IGNORE"
[0x87]	"Mobility Header"
[0x88]	"UDPLite"

Appendix B. Files Exempted from Encryption

Some files that are automatically initialized upon computer start-up will never be encrypted, namely Windows system files and Stormshield Endpoint Security files.

Here is the list of files that will never be encrypted:

Files exempted from encryption
*.386
*.a
*.bat
*.cab
*.com
*.cpl
*.cur
*.dat
*.desklink
*.dev
*.dll
*.drv
*.exe
*.ico
*.job
*.jod
*.la
*.lib
*.lnk
*.log
*.o
*.ocx
*.p12
*.pdb
*.pfx
*.reg
*.scf
*.sra
*.srk

Files exempted from encryption
*.srn
*.sro
*.srx
*.sys
*\boot.ini
*\bootfont.bin
*\bootmgr
*\bootsect.dos
*\desktop.htt
*\desktop.ini
*\ntldr
*\ntuser.ini
*\ntuser.pol
System Volume Information
temporary internet files
|programfiles|*
|systemdrive|\Boot*
|systemdrive|\BOOTSECT.BAK
|systemdrive|\Documents and Settings\All Users*
|systemdrive|\Documents and Settings\Default User*
|systemdrive|\Documents and Settings\LocalService*
|systemdrive|\Documents and Settings\NetworkService*
|systemdrive|\programdata*
|systemdrive|\progra~1*
|systemdrive|\recovery*
|systemroot|*
|userprofile|\application data\microsoft\crypto*
|userprofile|\application data\microsoft\protect*
|userprofile|\application data\microsoft\systemcertificates*
|userprofile|\appdata\roaming\microsoft\crypto*
|userprofile|\appdata\roaming\microsoft\protect*
|userprofile|\appdata\roaming\microsoft\systemcertificates*
|userprofile|\appdata\roaming\microsoft\sticky notes*
|userprofile|\appdata\local\microsoft\windows\appsfolder.*

Files exempted from encryption
|userprofile|\appdata\local\microsoft\windows\usrclass.*
|userprofile|\appdata\local\microsoft\windows\caches*
|users|\all users*
|users|\default user*
|userprofile|\ntuser.dat*

Appendix C. Date and time format strings

This appendix shows the list of standard and custom date and time format strings used in the console.

The option **Date format** is in the **Configuration** menu of the **Console Manager** section.

C.1 Standard date and time format strings

Format specifier	Description	Examples
d	Short date pattern	6/15/2009
D	Long date pattern	Monday, June 15, 2009
f	Full date/time pattern (short time)	Monday, June 15, 2009 1:45 PM
F	Full date/time pattern (long time)	15/06/2009 1:45:30 PM
g	General date/time pattern (short time)	15/06/2009 13:45
G	General date/time pattern (long time)	6/15/2009 1:45:30 PM
M, m	Month/day pattern	June 15
O, o	Round-trip date/time pattern	2009-06-15T13:45:30.0900000
R, r	RFC1123 pattern	Mon, 15 Jun 2009 20:45:30 GMT
s	Sortable date/time pattern	2009-06-15T13:45:30
t	Short time pattern	1:45 PM
T	Long time pattern	1:45:30 PM
u	Universal sortable date/time pattern	2009-06-15 20:45:30Z
U	Universal full date/time pattern	Monday, June 15, 2009 8:45:30 PM
Y, y	Year/month pattern	June, 2009
Any other single character	Unknown specifier	The console displays the "Invalid format" error

C.2 Custom date and time format strings

Format specifier	Description	Examples
d	The day of the month, from 1 through 31	6/1/2009 1:45:30 PM -> 1 6/15/2009 1:45:30 PM -> 15
dd	The day of the month, from 01 through 31	6/1/2009 1:45:30 PM -> 01 6/15/2009 1:45:30 PM -> 15
ddd	The abbreviated name of the day of the week	6/15/2009 1:45:30 PM -> Mon (en-US)

Format specifier	Description	Examples
dddd	The full name of the day of the week	6/15/2009 1:45:30 PM -> Monday
h	The hour, using a 12-hour clock from 1 to 12	6/15/2009 1:45:30 AM -> 1 6/15/2009 1:45:30 PM -> 1
hh	The hour, using a 12-hour clock from 01 to 12	6/15/2009 1:45:30 AM -> 01 6/15/2009 1:45:30 PM -> 01
H	The hour, using a 24-hour clock from 0 to 23	6/15/2009 1:45:30 AM -> 1 6/15/2009 1:45:30 PM -> 13
HH	The hour, using a 24-hour clock from 00 to 23	6/15/2009 1:45:30 AM -> 01 6/15/2009 1:45:30 PM -> 13
K	Time zone information	With DateTime values: 6/15/2009 1:45:30 PM, Kind Unspecified -> 6/15/2009 1:45:30 PM, Kind Utc -> Z 6/15/2009 1:45:30 PM, Kind Local -> -07:00 (depends on local computer settings) With DateTimeOffset values: 6/15/2009 1:45:30 AM -07:00 --> -07:00 6/15/2009 8:45:30 AM +00:00 --> +00:00
m	The minute, from 0 through 59	6/15/2009 1:09:30 AM -> 9 6/15/2009 1:09:30 PM -> 9
mm	The minute, from 00 through 59	6/15/2009 1:09:30 AM -> 09 6/15/2009 1:09:30 PM -> 09
M	The month, from 1 through 12	6/15/2009 1:45:30 PM -> 6
MM	The month, from 01 through 12	6/15/2009 1:45:30 PM -> 06
MMM	The abbreviated name of the month	6/15/2009 1:45:30 PM -> Jun (en-US) 6/15/2009 1:45:30 PM -> juin (fr-FR)
MMMM	The full name of the month	6/15/2009 1:45:30 PM -> Jun
s	The second, from 0 through 59	6/15/2009 1:45:09 PM -> 9
ss	The second, from 00 through 59	6/15/2009 1:45:09 PM -> 09
t	The first character of the AM/PM designator	6/15/2009 1:45:30 PM -> P (en-US) 6/15/2009 1:45:30 PM -> (fr-FR)
tt	The AM/PM designator	6/15/2009 1:45:30 PM -> P
y	The year, from 0 to 99	1/1/0001 12:00:00 AM -> 1 1/1/0900 12:00:00 AM -> 0 1/1/1900 12:00:00 AM -> 0 6/15/2009 1:45:30 PM -> 9
yy	The year, from 00 to 99	1/1/0001 12:00:00 AM -> 01 1/1/0900 12:00:00 AM -> 00 1/1/1900 12:00:00 AM -> 00 6/15/2009 1:45:30 PM -> 09
yyy	The year, with a minimum of three digits	1/1/0001 12:00:00 AM -> 001 1/1/0900 12:00:00 AM -> 900 1/1/1900 12:00:00 AM -> 1900 6/15/2009 1:45:30 PM -> 2009

Format specifier	Description	Examples
yyyy	The year as a four-digit number	1/1/0001 12:00:00 AM -> 0001 1/1/0900 12:00:00 AM -> 0900 1/1/1900 12:00:00 AM -> 1900 6/15/2009 1:45:30 PM -> 2009
yyyyy	The year as a five-digit number	1/1/0001 12:00:00 AM -> 00001 6/15/2009 1:45:30 PM -> 02009
z	Hours offset from UTC, with no leading zeros	6/15/2009 1:45:30 PM -07:00 -> -7
zz	Hours offset from UTC, with a leading zero for a single-digit value	6/15/2009 1:45:30 PM -07:00 -> -07
zzz	Hours and minutes offset from UTC	6/15/2009 1:45:30 PM -07:00 -> -07:00
:	The time separator	:
/	The date separator For more information: The "/" Custom Format Specifier	/
"string" 'string'	Literal string delimiter	("arr:" h:m t) -> arr: 1:45 P
%	Defines the following character as a custom format specifier	(%h) -> 1
\	The escape character	(h \h) -> 1 h
Any other character	The character is copied to the result string unchanged	(arr hh:mm t) -> arr 01:45 A

Appendix D. White list

This appendix contains the list of processes allowed to execute when the agent is in whitelist mode (application control). Stormshield Endpoint Security processes will be allowed by default.

Windows XP SP3
%WINDIR%\Explorer.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\crss.exe
%WINDIR%\system32\logonui.exe
%WINDIR%\system32\lsass.exe
%WINDIR%\system32\rundll32.exe
%WINDIR%\system32\services.exe
%WINDIR%\system32\smss.exe
%WINDIR%\system32\svchost.exe
%WINDIR%\system32\userinit.exe
%WINDIR%\system32\winlogon.exe

Windows 7 SP1
%WINDIR%\Explorer.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\conhost.exe
%WINDIR%\system32\consent.exe
%WINDIR%\system32\csrss.exe
%WINDIR%\system32\DllHost.exe
%WINDIR%\system32\logonui.exe
%WINDIR%\system32\lsm.exe
%WINDIR%\system32\runonce.exe
%WINDIR%\system32\services.exe
%WINDIR%\system32\smss.exe
%WINDIR%\system32\svchost.exe
%WINDIR%\system32\taskhost.exe
%WINDIR%\system32\userinit.exe
%WINDIR%\system32\wininit.exe
%WINDIR%\system32\winlogon.exe

%WINDIR%\SysWOW64\Autochk.exe

%WINDIR%\SysWOW64\DllHost.exe

%WINDIR%\SysWOW64\Explorer.exe

%WINDIR%\SysWOW64\runonce.exe

%WINDIR%\SysWOW64\svchost.exe

%WINDIR%\SysWOW64\userinit.exe

%WINDIR%\SysWOW64\wininit.exe

Windows Server 2008 R2.

%WINDIR%\Explorer.exe

%WINDIR%\system32\Autochk.exe

%WINDIR%\system32\Autochk.exe

%WINDIR%\system32\conhost.exe

%WINDIR%\system32\consent.exe

%WINDIR%\system32\csrss.exe

%WINDIR%\system32\DllHost.exe

%WINDIR%\system32\logonui.exe

%WINDIR%\system32\lsm.exe

%WINDIR%\system32\runonce.exe

%WINDIR%\system32\services.exe

%WINDIR%\system32\smss.exe

%WINDIR%\system32\svchost.exe

%WINDIR%\system32\taskhost.exe

%WINDIR%\system32\userinit.exe

%WINDIR%\system32\werfault.exe

%WINDIR%\system32\WerFaultSecure.exe

%WINDIR%\system32\wermgr.exe

%WINDIR%\system32\wininit.exe

%WINDIR%\system32\winlogon.exe

%WINDIR%\SysWOW64\Autochk.exe

%WINDIR%\SysWOW64\DllHost.exe

%WINDIR%\SysWOW64\Explorer.exe

%WINDIR%\SysWOW64\runonce.exe

%WINDIR%\SysWOW64\svchost.exe

%WINDIR%\SysWOW64\userinit.exe

%WINDIR%\SysWOW64\werfault.exe

%WINDIR%\SysWOW64\WerFaultSecure.exe

%WINDIR%\SysWOW64\wermgr.exe

%WINDIR%\SysWOW64\wininit.exe

Windows 8.1

%WINDIR%\Explorer.exe

%WINDIR%\system32\Autochk.exe

%WINDIR%\system32\conhost.exe

%WINDIR%\system32\consent.exe

%WINDIR%\system32\csrss.exe

%WINDIR%\system32\DllHost.exe

%WINDIR%\system32\dwm.exe

%WINDIR%\system32\logonui.exe

%WINDIR%\system32\lsm.exe

%WINDIR%\system32\runonce.exe

%WINDIR%\system32\services.exe

%WINDIR%\system32\smss.exe

%WINDIR%\system32\svchost.exe

%WINDIR%\system32\taskhost.exe

%WINDIR%\system32\userinit.exe

%WINDIR%\system32\werfault.exe

%WINDIR%\system32\WerFaultSecure.exe

%WINDIR%\system32\wermgr.exe

%WINDIR%\system32\wininit.exe

%WINDIR%\system32\winlogon.exe

%WINDIR%\SysWOW64\Autochk.exe

%WINDIR%\SysWOW64\DllHost.exe

%WINDIR%\SysWOW64\Explorer.exe

%WINDIR%\SysWOW64\runonce.exe

%WINDIR%\SysWOW64\svchost.exe

%WINDIR%\SysWOW64\userinit.exe

%WINDIR%\SysWOW64\werfault.exe

%WINDIR%\SysWOW64\WerFaultSecure.exe

%WINDIR%\SysWOW64\wermgr.exe

%WINDIR%\SysWOW64\wininit.exe

Windows Server 2012 R2

%WINDIR%\Explorer.exe

%WINDIR%\system32\Autochk.exe

%WINDIR%\system32\conhost.exe

%WINDIR%\system32\consent.exe

%WINDIR%\system32\csrss.exe

%WINDIR%\system32\DllHost.exe

%WINDIR%\system32\dwm.exe

%WINDIR%\system32\logonui.exe

%WINDIR%\system32\lsm.exe

%WINDIR%\system32\runonce.exe

%WINDIR%\system32\services.exe

%WINDIR%\system32\smss.exe

%WINDIR%\system32\svchost.exe

%WINDIR%\system32\taskhost.exe

%WINDIR%\system32\userinit.exe

%WINDIR%\system32\werfault.exe

%WINDIR%\system32\WerFaultSecure.exe

%WINDIR%\system32\wermgr.exe

%WINDIR%\system32\wininit.exe

%WINDIR%\system32\winlogon.exe

%WINDIR%\SysWOW64\ DllHost.exe

%WINDIR%\SysWOW64\ wininit.exe

%WINDIR%\SysWOW64\Autochk.exe

%WINDIR%\SysWOW64\Explorer.exe

%WINDIR%\SysWOW64\runonce.exe

%WINDIR%\SysWOW64\svchost.exe

%WINDIR%\SysWOW64\userinit.exe

%WINDIR%\SysWOW64\werfault.exe

%WINDIR%\SysWOW64\WerFaultSecure.exe

%WINDIR%\SysWOW64\wermgr.exe

Windows 10 LTSB and CBB

|systemroot|\Explorer.EXE

|systemroot|\System32\autochk.exe

|systemroot|\System32\conhost.exe

|systemroot|\System32\consent.exe

|systemroot|\System32\csrss.exe

|systemroot|\System32\dllhost.exe

|systemroot|\System32\dwm.exe

|systemroot|\System32\logonui.exe

|systemroot|\System32\lsass.exe

|systemroot|\System32\runonce.exe

|systemroot|\System32\services.exe

|systemroot|\System32\sihost.exe

|systemroot|\System32\smss.exe

|systemroot|\System32\svchost.exe

|systemroot|\System32\userinit.exe

|systemroot|\System32\werfault.exe

|systemroot|\System32\werfaultsecure.exe

|systemroot|\System32\wermgr.exe

|systemroot|\System32\wininit.exe

|systemroot|\System32\winlogon.exe

|systemroot|\System32\upfc.exe

|systemroot|\SysWOW64\autochk.exe

|systemroot|\SysWOW64\dllhost.exe

|systemroot|\SysWOW64\Explorer.EXE

|systemroot|\SysWOW64\runonce.exe

|systemroot|\SysWOW64\svchost.exe

|systemroot|\SysWOW64\userinit.exe

|systemroot|\SysWOW64\werfault.exe

|systemroot|\SysWOW64\werfaultsecure.exe

|systemroot|\SysWOW64\wermgr.exe

Appendix E. Logs Tables Schema

Stormshield Endpoint Security logs are stored in four tables of the Stormshield Endpoint Security database:

- Software logs table
- System logs table
- Network logs table
- Device logs table

This appendix shows a SQL database user how to write SQL scripts in order to extract and use logs.

The file *Stormshield Endpoint Security - Log Format.xls* is available on the SkyRecon support website and gives all the possible values for each entry of the database.

E.1 Main tables of the Stormshield Endpoint Security database

Table dbo.db_identification

This table contains agent identifiers.

Name	Type	Comment/Example
Index	int	Index
IP	nvarchar(50)	IPv4 address of the agent, in numeric format. Example: 192.168.128.108
MAC	nvarchar(50)	MAC address of the agent/not used
HostId	nvarchar(50)	Identifier of the agent certificate Example: AwKiAbIctFVWVhhq/ This string is unique.
Hostname	nvarchar(255)	Name of the machine, as defined in the **Computer Name** section of the advanced system properties. Example: C7-FSO-W81-64
LDAP	nvarchar(1024)	Full name of the machine in the domain. Example: C7-FSO-W81-64.Computers.sshield1.test Usually the first part of this variable is the hostname.

Table dbo.db_username

This table contains user names.

Name	Type	Comment/Example
Id	bigint	User Identifier
User	nvarchar(1024)	User name/login Example: John Doe

Table dbo.db_SystemLog

This table contains logs describing processes blocked by the agent. It is related to the **System Logs** in the Stormshield Endpoint Security console.

Name	Type	Comment/Example
Id	bigint	Log Id
Index	int	Index
Ltimestamp	bigint	Time in seconds since 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Action type Action type performed by Stormshield Endpoint Security. Example: OVERFLOW: Overflow
Status	nvarchar(50)	Action status
Source	nvarchar(1024)	The meaning of these fields depends on the codes "action" and "status". See logs table for more details
Dest	nvarchar(1024)	
Option	nvarchar(1024)	
Rid	int	Rule number
Userid	nvarchar(1024)	User identifier. Used to find the name in the db_username table
Cnx_state	tinyint	Connection status

Table dbo.db_SoftwareLog

This table contains logs about the agent and the policies received.

Name	Type	Comment/Example
Id	bigint	
Index	int	
Ltimestamp	bigint	Time in seconds since 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Severity of the event: • INFO • WARN • ERROR
Status	nvarchar(50)	Nature of the event
Log	nvarchar(1024)	Message the user can read Example: An error occurred when communicating with driver
Type	nvarchar(50)	Type of the event
Modname	nvarchar(50)	Module which sent the log
UserID	bigint	Used to find the user in the db_username table
Cnx_state	tinyint	Connection status

Table dbo.db_MediaID

This table describes Plug and Play identifiers of removable devices. They come from the Windows Plug and Play enumeration.

Name	Type	Comment/Example
MD5	nvarchar(50)	MD5 of the various fields. Information stored in the logs table db_MediaLog
VendorID	bigint	Device PnP Vendor ID
ProductID	bigint	Device PnP Product ID
SerialID	nvarchar(1024)	Serial number of the device
VendorName	nvarchar(1024)	Name of the device vendor.
ProductName	nvarchar(1024)	Name of the device model.

Table dbo.db_MediaLog

This table describes operations on removable devices.

Name	Type	Comment/Example
MD5	nvarchar(50)	MD5 of the various PnP fields. Used to find the description of the device in the table db_MediaID.
Index	int	
ltimestamp	bigint	Time in seconds since 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Description of the type of event
Status	nvarchar(50)	Action status
Source	nvarchar(1024)	Source of the event
Dest1	nvarchar(1024)	First object of the event
Dest2	nvarchar(1024)	Second object of the event
Size	bigint	Size assigned
Type	nvarchar(50)	Bus type assigned
ClassID	nvarchar(50)	Device class
Rid	int	Rule number
Userid	igint	Used to find the user in the db_username table
Cnx_state	tinyint	Connection status
Enrollmentstate	nvarchar(50)	Enrollment status
Ownername	nvarchar(1024)	Enrolled devices owner

Table dbo.db_NetworkLog

This table contains network access logs (Thor and Meili drivers).

Name	Type	Comment/Example
Id	bigint	
Index	int	
ltimestamp	bigint	Time in seconds since 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Description of the type of event
Status	nvarchar(50)	Action status
Metadata	nvarchar(255)	Various information, refer to the file *Stormshield Endpoint Security - Log Format.xls* available on the SkyRecon support website.
Ipdst	nvarchar(255)	Destination IP address
Ipsrc	nvarchar(255)	Source IP address
Code	nvarchar(255)	Attack sub-type
Proto1	nvarchar(50)	Ethernet/MAC level protocol
Proto2	nvarchar(50)	Other protocol
Rid	int	Rule number
Cnx_state	tinyint	Connection status

E.2 Examples of how to use tables

This section provides examples of SQL queries to get some information about the logs tables.

Retrieving all system logs and searching machines and users identifiers

```
select [user],[status],

CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-
01-01', 20) ), 13) tick,

SUBSTRING(source,0, CHARINDEX('<>',source)) Source

from [stormshield].[dbo].[db_SystemLog] s WITH (NOLOCK)

join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Retrieving all software logs and searching machines and users identifiers

```
select [user],[action],[status],[modname],[log],

CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-
01-01', 20) ), 13) tick

from [stormshield].[dbo].[db_SoftwareLog] s WITH (NOLOCK)
```

```
join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Retrieving all network logs and searching machines and users identifiers

```
select [user],[action],[status],[ipdst] IpSrcToIpDst,[ipsrc] Port,
[proto1],[proto2],
```

```
CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-
01-01', 20) ), 13) tick
```

```
from [stormshield].[dbo].[db_NetworkLog] s WITH (NOLOCK)
```

```
join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Retrieving all device logs and searching machines and users identifiers

```
select [user],[ownername],[Action],[status] ,[ClassID],
```

```
CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-
01-01', 20) ), 13) tick,
```

```
SUBSTRING(source,0, CHARINDEX('<>',source)) Source
```

```
from [stormshield].[dbo].[db_MediaLog] s WITH (NOLOCK)
```

```
join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Appendix F. WiFi authentication modes

The table below gives the correspondence between the names given to the WiFi authentication modes in the SES security policies and the names of the corresponding modes in the Microsoft Windows operating systems.

For more information on these authentication modes, refer to the Microsoft documentation:

- Windows XP
- Other operating systems

SES	Windows XP	Other operating systems
open	Ndis802_11AuthModeOpen	DOT11_AUTH_ALGO_80211_OPEN
WEP	Ndis802_11AuthModeShared	DOT11_AUTH_ALGO_80211_SHARED_KEY
open or WEP	Ndis802_11AuthModeAutoSwitch	not supported
WPA	Ndis802_11AuthModeWPA	DOT11_AUTH_ALGO_WPA
WPA (PSK)	Ndis802_11AuthModeWPAPSK	DOT11_AUTH_ALGO_WPA_PSK
WPA (ADHOC)	Ndis802_11AuthModeWPANone	DOT11_AUTH_ALGO_WPA_NONE
WPA2	Ndis802_11AuthModeWPA2	DOT11_AUTH_ALGO_RSNA
WPA2 (PSK)	Ndis802_11AuthModeWPA2PSK	DOT11_AUTH_ALGO_RSNA_PSK
Other authentication modes	Others (excludes the 8 values above)	Others (excludes the 7 values above)

STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2023. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.