



**STORMSHIELD**



**STORMSHIELD ENDPOINT SECURITY**

# RELEASE NOTES

Version 7.2

Document last updated: June 22, 2023

Reference: [ses-en-release\\_notes-v7.2.40](#)



# Table of contents

---

New behavior .....	3
Stormshield Endpoint Security 7.2.40 resolved vulnerabilities .....	5
Stormshield Endpoint Security 7.2.40 fixes .....	6
Compatibility between Windows versions and Stormshield Endpoint Security 7.2.40 ...	7
Recommendations .....	8
Known issues .....	9
Explanations on usage .....	13
Documentation resources .....	14
Downloading this version .....	15
Going to your MyStormshield personal area .....	15
Checking the integrity of the binary files .....	15
Information about Stormshield Endpoint Security 7.2 versions .....	16
Previous versions of Stormshield Endpoint Security 7.2 .....	18
Contact .....	136

In the documentation, Stormshield Endpoint Security is referred to in its short form: SES.  
This document is not exhaustive and minor changes may have been included in this version.



## New behavior

---

### Changes introduced in version 7.2.40

#### **OpenSSL update**

In the version 7.2.40 of SES, the OpenSSL library has been updated to version 3.0. It is used by the agent installer, the server and the SES agent.

However, limitations of the embedded SSL functions in Windows XP, Windows 2003 and Windows 7 make the installation of 7.2.39 or earlier agents and the 7.2.40 or higher server incompatible.

As a consequence, before updating the SES server in version 7.2.40, make sure you do not have any agents running on these former operating systems that are being installed and have not yet made their first connection to the server.

Once the server is updated, you will only need to use the *.msi* installation files generated by the 7.2.40 or higher server to install new agents.

This incompatibility does not affect agents already installed and connected to the SES server or agents running on Windows 10.



# Stormshield Endpoint Security 7.2.40 new features and enhancements

---

## **Support for SQL Server 2022 and Windows Server 2022**

SES now supports Microsoft SQL Server 2022 for the databases and Windows Server 2022 for the installation of the console and server.



# Stormshield Endpoint Security 7.2.40 resolved vulnerabilities

---

## **OpenSSL update**

A vulnerability with a medium level severity was fixed after the OpenSSL component was upgraded.

Details on this vulnerability can be found on our website

<https://advisories.stormshield.eu/2023-012>.



# Stormshield Endpoint Security 7.2.40 fixes

---

## Agent fix

### Access to files stored on a multiple mass storage USB device

Support reference 197901CW

SES no longer prevents users from accessing files stored on some USB devices which present several different mass storage devices to the Windows operating system. For example cameras could be concerned with this issue.



## Compatibility between Windows versions and Stormshield Endpoint Security 7.2.40

The Stormshield Endpoint Security agent 7.2.40 is compatible with the following Windows versions:

Windows version	Professional Edition	Secure Edition	Server-Side Edition
Windows XP SP3- 32 bits	✓	✓	-
Windows 7 SP1 - 32/64 bits, with updates <a href="#">KB4474419</a> and <a href="#">KB4490628</a>	✓	✓	-
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 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 <a href="#">KB4474419</a> and <a href="#">KB4490628</a>	-	-	✓
Windows Server 2012 R2 - 64 bits	-	-	✓



# Recommendations

## Information prior to an update of SES

The update of SES agents from versions 7.2.39 or earlier to version 7.2.40 requires the installation of a root certificate authority on all the agents running on operating systems from Windows 7 or Windows Server 2008 R2.

Please follow the steps in the Stormshield [Knowledge Base](#) article before updating. The article also provides the certificate and the necessary tools.

## Warning regarding the expiry of SHA-1 certificates in SES 7.2

SES 7.2 certificates signed in SHA-1 expired on October 25, 2022. Update your SES 7.2 agent pools as soon as possible by following the [procedure](#) in the Stormshield Knowledge base.

## Warning before migrating to Windows 10 22H2

Before you migrate your pool to Windows 10 22H2, ensure that the SES security policy you are using contains the trusted applications required for this migration.

The recommendations below apply only to agents without full disk encryption. Contact the Stormshield Technical Assistance Center (TAC) to migrate agents with full disk encryption.

SES version of your pool	Operations to perform before Windows migration
SES 7.2.36 to 7.2.39	<ul style="list-style-type: none"><li>Download the updated <i>Trust W10</i> rule group from your <a href="#">MyStormshield</a> personal area. This rule group is compatible with versions 7.2.36 to 7.2.39.</li><li>Import the rule group <i>Trust W10</i> in the <b>Application control</b> tab of the security policies applied to Windows 10 workstations. <i>Trust W10</i> now contains the file access permissions necessary.</li></ul>
SES 7.2.35 or previous versions	Windows 10 22H2 is not supported. Update your pool to the latest version of SES available beforehand.





## Known issues

The known issues are:

Id	Incompatibilities	Workaround
173536CW	<b>Description:</b> Incompatibility between Symantec Endpoint Security (SEP), Microsoft Internet Explorer 11 and the RCP protection.	You need to disable the RCP Protection on the Microsoft Internet Explorer 11 application.
	<b>Description:</b> Incompatibility between BitLocker To Go and the removable device control feature of the agent.	You need to disable the <b>Group management</b> parameter in the general settings of the device control to use BitLocker To Go.
	<b>Description:</b> Protection against forced reboot is not compatible with Windows 10 1703.	The problem is fixed in Windows 10 version 1709.
	<b>Description:</b> Incompatibility with IBM Trusteer Rapport under 64-bit Windows 7.	No solution for the moment.
87979 - 152138CW	<b>Description:</b> A blue screen appears whenever SES is used with Avast Endpoint 8.01609.	You need to disable the Avast Virtualization driver (aswSnx.sys). <b>Procedure:</b> <ol style="list-style-type: none"><li>1. Start the workstation in safe mode.</li><li>2. Disable the Avast driver found in <i>C:\Windows\system32\drivers\aswsnx.sys</i> by renaming it <i>C:\Windows\system32\drivers\aswsnx.sys.old</i>, for example.</li><li>3. Restart the workstation and check that it no longer presents a blue screen.</li></ol>
87998 - 152269PW	<b>Description:</b> During the installation of Avast Business version 17.2.2517 and SES, Windows processes are unable to start. The following error appears: <i>The application was unable to start correctly (0xc0000142). Click OK to close the application.</i>	No solution for the moment.



Id	Incompatibilities	Workaround
1645	<p><b>Description:</b> A bootable device cannot be created with the HP USB Disk Storage Format Tool. The following error message is displayed between [format end] and [start copy file] on the device: "FAILED TO MAKE THE DEVICE DOS-BOOTABLE".</p> <p><b>Cause:</b> When a device is removed from a computer, Stormshield Endpoint Security denies access to the latter as long as StormShield checks whether or not the device is encrypted. During this process, the HP software mounts and unmounts the device several times in a row.</p>	No solution for the moment. [#FKX-94147-408]
1846	<p><b>Description:</b> Incompatibility between StormShield and the Digital Persona smart-card authentication system. Files encrypted by Stormshield Endpoint Security cannot be accessed when using Windows authentication.</p> <p><b>Cause:</b> If Digital Persona is installed after Stormshield Endpoint Security, the former removes Stormshield Endpoint Security GINA dll and the authentication system.</p>	Install Stormshield Endpoint Security after Digital Persona. [#DNX-52479-415]



Id	Incompatibilities	Workaround
2137	<p><b>Description:</b> Incompatibility between StormShield and Sophos SafeGuard Enterprise (encryption tool). USB keys are displayed in Computer, but their content cannot be accessed. USB hard disks can only be accessed in read-only mode. <b>Cause:</b> The encryption tool is incompatible with the device control system. SafeGuard detects if another driver implements a filter and in this case, denies access to devices.</p>	<p>Modify the registry base in order to load the Stormshield Endpoint Security driver <code>odin-sys.sra</code> before the SafeGuard Enterprise driver.</p> <p><b>Procedure:</b></p> <ol style="list-style-type: none"><li>1. Stop the Stormshield Endpoint Security agent with <code>stopagent.exe</code></li><li>2. Go to registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder</code></li><li>3. Edit the <code>List</code> value and add an <b>Odin</b> entry above the <b>Primary Disk</b> entry (Safeguard Enterprise driver)</li><li>4. Go to registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\odin</code></li><li>5. Add the <code>Group</code> value (string type) and assign the value <code>Odin</code> in the <b>Value data</b> field.</li><li>6. Reboot.</li></ol> <p>[#BSX-16078-335]</p>
5180	<p><b>Description:</b> Incompatibility with BitLocker To Go (Stormshield Endpoint Security file encryption). <b>Cause:</b> BitLocker To Go and Stormshield Endpoint Security operations overlapping.</p>	<p>No solution for the moment. Stormshield Endpoint Security file encryption must be deactivated for removable devices.</p>
	<p><b>Description:</b> Incompatibility with F-Secure application on 64-bit operating systems. <b>Cause:</b> Incompatibility with auto-protection in Stormshield Endpoint Security.</p>	<p>Disable option <b>Use advanced process monitoring</b> in the DeepGuard settings in F-Secure.</p>
	<p><b>Description:</b> A BSOD occurs when using Stormshield Endpoint Security with a solution embedding Safenet aksfridge.sys, Aksdf.sys or Hardlock.sys drivers.</p>	<p>The version 6.62 or later of Safenet drivers (Sentinel HASP/LDK) includes a fix for this problem.</p>
	<p><b>Description:</b> MTP USB devices cannot be blocked.</p>	<p>No solution for the moment.</p>
	<p><b>Description:</b> SD card and eSata devices cannot be blocked.</p>	<p>No solution for the moment.</p>



Id	Incompatibilities	Workaround
9525	<b>Description:</b> A blue screen occurs when FortiClient Endpoint Protection is installed with Stormshield Endpoint Security.	Modify the registry base in order to load the SES driver <i>heimdall-sys.sra</i> after the FortiClient Endpoint Protection driver.  <b>Procedure:</b> <ol style="list-style-type: none"><li>1. Start the machine in safe mode or stop the SES agent with stopagent or with the challenge response <b>Complete stop</b>.</li><li>2. Go to registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\heimdall</code></li><li>3. Edit the <code>Group</code> value and replace the current value by <code>FSFilter Content Screener</code>.</li><li>4. Add the value <code>Tag</code> of the type <code>DWORD</code> and then edit the value and replace <code>0</code> by <code>1</code>.</li><li>5. Reboot.</li></ol> Side effects: removable devices protection (Bluetooth, Com, USB, etc.) does no longer work and must not be used.
	<b>Description:</b> A blue screen occurs when 360 Total Security Protection is installed with SES. <b>Cause:</b> Incompatibility with the driver 360Box64.	No solution for the moment.
9418	<b>Description:</b> Incompatibility with the extension "Office Editing for Docs, Sheets and Slides" for Google Chrome. Opening a document with this extension fails and displays either an error or a blank page.	No solution for the moment.
8397	<b>Description:</b> Whenever an NTFS compressed file is encrypted, data can be lost but no space is gained.	Disable compression of NTFS files before encrypting them.
9257	<b>Description:</b> Incompatibility with the EMET (Enhanced Mitigation Experience Toolkit) security EAF/EAF+. <b>Description:</b> Impossible to update workstations from Microsoft Windows 10 CBB 1511 to Windows 10 CBB 1607 with SES full disk encryption enabled.	No solution for the moment to be compatible with this EMET module.  <b>Workaround:</b> Disable encryption, migrate and enable encryption again after the migration.



## Explanations on usage

---

The following hardware and software are unsupported during disk encryption:

- Software RAID and dynamic disks.
- Partition management and disk cloning tools.
- Hard drives with sector size other than 512 bytes.
- Extended partitions (or secondary partitions) are not supported by full disk encryption. Only disks containing primary 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.



## Documentation resources

---

The following technical documentation resources are available on the [Stormshield Technical Documentation](#) website. We suggest that you rely on these resources for a better application of all features in this version.

### Guides

- Stormshield Endpoint Security Administration guide
- Stormshield Endpoint Security First Time Configuration guide
- SQL Server recommendations

### How to

- How to apply a security policy to your Active Directory
- How to unblock a user
- How to update workstations under Windows 10
- How to quarantine a workstation with the SES firewall
- How to renew the SES root certificate authority
- How to set up SQL Server



## Downloading this version

---

### Going to your MyStormshield personal area

You need to go to your [MyStormshield](#) personal area in order to download the 7.2.40 version of Stormshield Endpoint Security:

1. Log in to MyStormshield with your personal identifiers.
2. In the left panel, select **Downloads**.
3. In the right panel, select the relevant product and version.

### Checking the integrity of the binary files

To check the integrity of Stormshield Endpoint Security binary files:

1. Enter one of the following commands and replace `filename` by the name of the file you want to check:
  - Linux operating system: `sha256sum filename`
  - Windows operating system: `CertUtil -hashfile filename SHA256`
2. Compare with hashes provided on [MyStormshield](#) personal area, section **Downloads**.



## Information about Stormshield Endpoint Security 7.2 versions

The table below gives information about the Stormshield Endpoint Security 7.2 versions:

Version	Release date	Build
7.2.40	06/22/2023	1
7.2.39	10/20/2022	1
7.2.38	08/12/2022	1
7.2.37	04/07/2022	1
7.2.36	12/21/2021	1
7.2.35	10/26/2021	5
7.2.34	05/17/2021	4
7.2.33	12/21/2020	1
7.2.32	09/21/2020	1
7.2.31	08/10/2020	1
7.2.30	06/15/2020	1
7.2.29	01/30/2020	2
7.2.28	10/21/2019	2
7.2.27	09/23/2019	4
7.2.26	06/21/2019	3
7.2.25	03/22/2019	1
7.2.24	1/28/2019	2
7.2.23	9/13/2018	4
7.2.22	5/18/2018	b6
7.2.21	3/20/2018	3
7.2.20	2/28/2018	32002
7.2.19	11/30/2017	30808
7.2.18	8/28/2017	30367
7.2.17	6/19/2017	30056
7.2.16	5/18/2017	29988
7.2.15	2/9/2017	29261
7.2.14	11/30/2016	28738
7.2.13	10/21/2016	28446





7.2.12	9/29/2016	28180
7.2.11	9/22/2016	28114
7.2.10	7/29/2016	27616
7.2.09	6/10/2016	27184
7.2.08	5/27/2016	27072
7.2.07	5/9/2016	26972
7.2.05	1/22/2016	26324
7.2.04	10/30/2015	25798
7.2.03	7/31/2015	25366
7.2.01	5/11/2015	24884



# Previous versions of Stormshield Endpoint Security 7.2

In this section, you will find the features, resolved vulnerabilities and fixes from previous versions of Stormshield Endpoint Security 7.2.

7.2.39	New features		Bug fixes
7.2.38			Bug fixes
7.2.37	New features	Resolved vulnerabilities	Bug fixes
7.2.36	New features		Bug fixes
7.2.35			Bug fixes
7.2.34	New features	Resolved vulnerabilities	Bug fixes
7.2.33	New features		Bug fixes
7.2.32	New features		Bug fixes
7.2.31	New features		Bug fixes
7.2.30	New features	Resolved vulnerabilities	Bug fixes
7.2.29	New features		Bug fixes
7.2.28	New features		
7.2.27			Bug fixes
7.2.26	New features		Bug fixes
7.2.25		Resolved vulnerabilities	Bug fixes
7.2.24	New features		Bug fixes
7.2.23	New features		Bug fixes
7.2.22	New features		Bug fixes
7.2.21			Bug fixes
7.2.20	New features		Bug fixes
7.2.19	New features		Bug fixes
7.2.18	New features		Bug fixes
7.2.17	New features		
7.2.16	New features		Bug fixes
7.2.15	New features		Bug fixes
7.2.14	New features		Bug fixes
7.2.13	New features		Bug fixes
7.2.12		Resolved vulnerabilities	



7.2.11	New features		Bug fixes
7.2.10	New features		Bug fixes
7.2.09			Bug fixes
7.2.08		Updates	Bug fixes
7.2.07	New features	Updates	Bug fixes
7.2.06	New features	Updates	Bug fixes
7.2.05	New features	Updates	Bug fixes
7.2.04	New features	Updates	Bug fixes
7.2.03			Bug fixes
7.2.02		Updates	Bug fixes
7.2.01			Bug fixes
7.2	New features	Removed features	Bug fixes



## Stormshield Endpoint Security 7.2.39 new features and enhancements

---

### **Certificates update in the Basic template policy**

The certificates of the following applications have been updated in the application identifiers of the Basic template policy:

- Google Chrome
- Opera
- Mozilla Firefox
- Microsoft Edge
- Windows Defender
- Windows OneDrive
- Oracle Java



# Stormshield Endpoint Security 7.2.39 fixes

---

## Agent fix

### Loss of the trust inherited from parent applications

Support reference 170950PW

When applying a new policy, applications which were open and which inherited trust granted to their parent application could lose the trust (option **Application and children** of the attribute **Application scope** of **Trusted Rules**, in the tab **Application Control**). This issue occurred even if settings were the same in the new policy. This issue has been fixed.



# Stormshield Endpoint Security 7.2.38 fixes

## Console fix

### Reporting language

Support reference 192793CW

In the settings of some server configuration policies, the user would occasionally be unable to choose a language for logs other than the language of the administration console. This issue has been fixed.

## Agent fixes

### Microsoft .NET applications blocked when Symantec antivirus was enabled

Support reference 193667CW

When HoneyPot is enabled in security policies and Symantec antivirus is installed on workstations, Microsoft .NET applications are now no longer blocked when they are launched.

### Rules regarding trusted applications

Support reference 170649PW

In the **Application control** tab of a security policy, whenever a rule is created for a trusted application by selecting **Application and children** in the **Application scope** column, and by selecting the checkbox in the **Execution control** column, the configuration is now correctly applied and the processes that the trusted application created are no longer blocked.

## Server fix

### Certificate server logs

Occasionally, the certificate server would not save the latest error logs. This issue has been fixed and additional diagnostic data is now available.



## Stormshield Endpoint Security 7.2.37 new features and enhancements

---

### **Support for SQL Server 2019**

SES now supports Microsoft SQL Server 2019 for the databases.

### **Updates to the “Messaging tools” built-in rule group**

**Support reference 168429PW**

The new rules fix a compatibility issue between Microsoft Outlook and Adobe Acrobat Reader.



## Stormshield Endpoint Security 7.2.37 resolved vulnerability

---

### OpenSSL update

A vulnerability with a medium level severity was fixed after the OpenSSL component was upgraded in version 1.1.1n.

Details on this vulnerability can be found on our website

<https://advisories.stormshield.eu/2022-007>.





## Stormshield Endpoint Security 7.2.37 fix

---

### Agent fix

#### **Stopping and uninstalling the agent on Microsoft Windows 7**

In SES 7.2.36, stopping the agent by running the *stopagent.exe* program and uninstalling the agent did not work on the Microsoft Windows 7 operating system. This problem is fixed in version 7.2.37.



## Stormshield Endpoint Security 7.2.36 new features

### Support for Windows 10 21H2

SES now supports the Microsoft Windows 10 21H2 operating system.

Refer to the [Recommendations](#) section before you migrate your pool to Windows 10 21H2.

### Updates to the dedicated McAfee rule group

**Support references 186753CW and 187067CW**

New rules relating to trust have been added to the McAfee rule group to integrate McAfee Endpoint Security.



# Stormshield Endpoint Security 7.2.36 fixes

## Server fixes

### Agent connections to the SES server

Support reference 183642CW

On some high-traffic network infrastructures, phantom connections would sometimes persist on the SES server until they saturated the server. As a result, agents could no longer log in to the server. This issue has been fixed.

### Displaying the status of agents in the administration console

Support references 183671CW, 184976CW, 188406CW and 187806CW

The agent monitoring panel in the administration console would occasionally indicate that some agents in Warning or StandBy mode were invalid even though they were running properly. This issue has been fixed.

You must update SES from an updated administration console, using the Log and monitoring databases maintenance wizard in the DBInstaller utility, to benefit from this fix. The correct status of these agents will appear in the console when agents restart and log back in to the SES server.



# Stormshield Endpoint Security 7.2.35 fixes

## Console fix

### USB key enrollment

Support reference [SESMAINT-373](#)

USB keys with serial numbers exceeding 64 characters, such as 32 GB SanDisk Ultra USB 3.0, can now be enrolled.

## Agent fixes

### Freeze during agent uninstallation

Support reference [SESMAINT-333](#)

The entire workstation would occasionally freeze when uninstalling the SES 7.2 agent if an endpoint protection application other than Kaspersky was installed on the workstation. This issue has been fixed.

### Confirming agent uninstallation

Support reference [SESMAINT-302](#)

When the SES agent is being uninstalled from the Add/Delete programs panel, a dialog box now asks the user to confirm the operation.

### Access to encrypted USB keys with older versions of SES.

Support reference [SESMAINT-374](#)

Reading and writing is now possible on USB keys encrypted with older versions of SES.

### Improved persistence of SES network filters

Support reference [SESMAINT-231](#)

Third-party programs that hold administration privileges would sometimes delete Windows-registered SES network filters. As long as SES is installed, they will now be monitored and reinstalled whenever they are deleted.

## Server fixes

### Inserting new logs and updating agent status in databases

Support reference [SESMAINT-348](#)

When a database containing many agents and a large volume of logs has been installed for several years, inserting new logs and updating the status of agents could cause the SQL Server to consume much more CPU. The database has been improved and fixes this issue.



You must update the database with the Log and monitoring databases maintenance wizard of the DBInstaller utility, from a 7.2.35 administration console, to benefit from this fix.



## Stormshield Endpoint Security 7.2.34 new features

### Support for Windows 10 21H1

SES now supports the Microsoft Windows 10 21H1 operating system.

### Compatibility with local network proxies

The parameter *Compatibility with local network proxies* was added to the general settings in application control (Network activity protection) to guarantee compatibility with local network proxies that intercept outgoing UDP packets. This parameter makes it possible to change how stateful inspection of the SES firewall is managed so that the firewall can be more permissive and avoid blocking the return of redirected packets.

### Different binary signature

The binary signature scheme in SES 7.2.34 has been changed to comply with new Microsoft root certificates.

As a result, in Windows 7 and Windows Server 2008 R2, you must have [KB4474419](#) and [KB4490628](#) in order to install the SES 7.2.34 components. These updates usually exist on machines that are regularly updated.



# Stormshield Endpoint Security 7.2.34 resolved vulnerability

---

## OpenSSL update

Support reference **SESMAINT-299**

A vulnerability with a high level severity was fixed after the OpenSSL component was upgraded.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.



# Stormshield Endpoint Security 7.2.34 fixes

## Console fixes

### Updating an expired license

Support references SESMAINT-223 - 176453CW

When the SES license expires, it can now be updated in SES environments in which Active Directory groups have been declared.

### Duplicate rules in rule group *Trust W10*

Support reference SESMAINT-251

Rules no longer appear twice in the rule group *Trust W10*.

### Editing network rules

Support reference SESMAINT-297

Network rules in the *Base network* rule group from the *Basic template* policy can now be edited.

## Agent fixes

### BSOD during standby

Support reference SESMAINT-243

On an SES Secure Edition agent, a BSOD (blue screen of death) would sometimes occur under random conditions. This issue has been fixed.

### Uninstalling the firewall

Support reference SESMAINT-232

The firewall is now correctly uninstalled on operating systems in Windows 7 or higher.

### Compatibility with other firewalls

Support reference SESMAINT-203

Whenever several firewalls were enabled, including the SES firewall, some packets would occasionally be accepted or rejected by mistake. Compatibility with third-party firewalls has been enhanced.

### BSOD and unexpected shutdown of processes

Support reference SESMAINT-304

With Windows 10 2004 and 20H2, BSODs would sometimes occur when a machine was resuming after standby or shutting down. Processes have also been observed to shut down randomly. These issues have been fixed.





## Stormshield Endpoint Security 7.2.33 new feature

---

From version 7.2.20 upwards, SES no longer allows Avira antivirus to be managed. If you have this option, please refer to the [Recommendations](#) section before performing the upgrade.

### **Support for Windows 10 20H2**

SES now supports the Microsoft Windows 10 20H2 operating system.

Refer to the [Recommendations](#) section before you migrate your pool to Windows 10 20H2.



# Stormshield Endpoint Security 7.2.33 fixes

From version 7.2.20 upwards, SES no longer allows Avira antivirus to be managed. If you have this option, please refer to the [Recommendations](#) section before performing the upgrade.

## Console fix

### Accessibility and synchronization of the Active Directory environment

Support references T5146 - 175194CW

When users are being added, if an attempt to connect to an Active Directory domain or forest fails, the Active Directory environment will now remain accessible in the **Environment** tab of the administration console and can still be synchronized.

## Agent fixes

### Compatibility with VMware Horizon

Support references T5071 and 174810CW

Honeypot protection in SES is now compatible with VMware Horizon.

### Improved detection of UEFI firmware

Support reference T5077

UEFI firmware is now detected earlier during the installation of full disk encryption. A more explicit error log is also generated when it is detected.

### Uninstall Agent

Support reference T5025

Depending on the rules defined in the policy applied to a workstation, the SES agent would occasionally fail to uninstall. This issue has been fixed.



## Stormshield Endpoint Security 7.2.32 new feature

From version 7.2.20 upwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### Support of USB Attached SCSI removable disks (UAS)

Support references: T4919 - 173624CW - 171749CW

SES now supports the USB Attached SCSI protocol. This data transfer protocol is usually used by large capacity removable disks.



# Stormshield Endpoint Security 7.2.32 fixes

## Agent fixes

### Modifying the password of a workstation using full disk encryption

Support references: T4920 - 174326CW

In certain cases, modifying the password of workstations using full disk encryption would fail. This issue has been fixed.

#### IMPORTANT

Recovery removable media for encrypted disk must be updated with the 7.2.32 version of the SES recovery software, if they include Microsoft Windows PE 2004 version.

### Disabling Network applicative rules automatically when enabling temporary web access

Support references: T4897 - 174078CW

When enabling temporary web access, Network applicative rules automatically stop being evaluated. Previously they used to stay enabled and could prevent access to the company VPN portal.



## Stormshield Endpoint Security 7.2.31 new feature

From version 7.2.20 onwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### **Migration of an encrypted workstation to Microsoft Windows 10 2004**

We now support the migration of workstations using SES full disk encryption from Microsoft Windows 10 version 1909 to version 2004.

Be aware that if you created recovery removable media for encrypted disk before Windows migration, they will no longer work. You need to create a new one after the migration. For more information, see section *13.7.4 Recovering an encrypted disk on removable media* in the [Administration guide](#).



# Stormshield Endpoint Security 7.2.31 fix

---

## Server fix

### Deadlocks when inserting many logs in the database

Support reference 171218CW

When SES servers received many logs from the agents, their insertion in the database could be slowed down and sometimes even blocked. This issue has been fixed.

Warning: you must update log databases with the **Log and monitoring databases maintenance** wizard of the DBInstaller utility, from a 7.2.31 administration console, to benefit from this fix.



## Stormshield Endpoint Security 7.2.30 new features

From version 7.2.20 upwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### IPv6 communications control

Support reference 170965W

In the **Network Activity Control** tab of the security policy edition panel, the **IPv6 communications** option has been added to general settings. It makes it possible to allow or not IPv6 communications and to control every incoming or outgoing IPv6 flows.

### Compatibility with Microsoft Windows 10 2004

We have validated the SES agent was compatible with the new Windows 10 2004 operating system. The lowest version of the SES agent required is version 7.2.30.

#### **Restriction**

If you are using SES full disk encryption, the migration of the operating system from Windows 10 1909 or previous versions to the Windows 10 2004 version is not supported.

If you update the operating system, workstations could be permanently corrupted.



## Stormshield Endpoint Security 7.2.30 resolved vulnerability

---

### Libxml2 upgraded to version 2.9.6

**Support reference T4175**

The libxml2 version that Stormshield Endpoint Security uses to manage XML files has been upgraded to version 2.9.6. Version 2.9.4 contained security flaws.





# Stormshield Endpoint Security 7.2.30 fixes

---

## Console fix

### Network protocols lists updated

Support reference T4412

In the network rules edition panel, the lists of the network protocols allowing to complete the **Over IP** and **Over Ethernet** fields have been updated.

## Agent fixes

### HPP protection disabled

Support reference 170291CW

On 64-bit operating systems and in some situations, it could happen that the HPP protection does not apply to 32-bit processes. This issue has been fixed.



## Stormshield Endpoint Security 7.2.29 new features

From version 7.2.20 upwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### **New log when changing the disk encryption password**

Support references CF88953 - 160574PW

A log has been added to indicate a user has changed the full disk encryption password. If the old and the new passwords are the same, a Warning log is reported. If both passwords are different, an Information log is reported.

### **Compatibility with Windows 10 1909**

We have validated the SES agent was compatible with the new Windows 10 1909 operating system. The lowest version of the SES agent required is version 7.2.26.

### **Updating the security policies basic template**

The following certificates have been updated in the “basic template” policy:

- Oracle for Java
- Google for Chrome
- Opera for Opera
- Mozilla for Firefox
- Windows for Edge and Windows Defender



# Stormshield Endpoint Security 7.2.29 fixes

## Console fixes

### Error while connecting to the management console

Support references CF88966 - 166960CW

An issue in the database could result in the creation of corrupted users which would not be able to log on to the console. The error message "No environment assigned" would display. This issue only occurred when many users had been created and deleted from the console.

### Importing log filters

Support reference 168144CW

In the log manager, filters with only a difference on the status or the type of reporting are no longer considered as duplicates and can now be imported.

## Agent fix

### Application crashes since version 7.2.27 with the display of WerFault.exe

Support references CF88983 - 167682CW

When the RCP protection is enabled, random application crashes on browsers or other applications no longer occur.



## Stormshield Endpoint Security 7.2.28 new feature

From version 7.2.20 onwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### **Support of the Microsoft Windows Embedded Standard operating system**

The SES agent is now compatible with the Embedded version of the 32-bit Microsoft Windows 7 operating system, in order to protect the workstations under this version.



# Stormshield Endpoint Security 7.2.27 fixes

From version 7.2.20 onwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

## Console fix

### Backing up/restoring the administration database

Support references T3602, CF88926 - 165477CW

Whenever administration databases were backed up or restored, if a large number of these operations had been conducted in the past, registered console users would be deleted as index values were exceeded in database tables. This issue has been fixed.

## Agent fixes

### Installing agents through a deployment tool

Support references T3647, CF88934 - 165811CW

During the installation of the SES agent using a deployment tool run in command line, the asynchronous execution mode would cause workstations to restart too quickly even though the installation was still ongoing. The new installation synchronous execution mode now no longer causes workstations to unexpectedly restart and guarantees the proper installation of the agent.

### Blue screen when policies are changed in close succession

Support references T3639, CF88928 - 165624CW

Changing policies in some situations would cause a blue screen on workstations if such changes were carried out in close succession. This issue has been fixed.

### Action failure upon detection

Support references T3460, CF88859 - 163172CW

An issue with the synchronization of the agent would prevent some actions from being executed once the agent was detected on workstations. This issue has been fixed.

### SES and Schneider Electric compatibility

Support references T3562, CF88873 - 163654CW

Schneider's EcoStruxure Expert Unity V14 would be unable to open some projects whenever SES protection against memory corruption was enabled. This issue has been fixed.



## USB key enrollment

Support references T3597, CF88910 - 164844CW

Whenever a USB key was enrolled on an SES administration console that was also equipped with an SES agent, the agent would stop running and automatically restart after a minute. This issue has been fixed.



## Stormshield Endpoint Security 7.2.26 new features

From version 7.2.20 onwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### Renewing the root certificate authority

SES has a root certificate authority that authenticates links between SES servers, agents and consoles.

SES now makes it possible to:

- schedule the renewal of the authority before the expiration of its certificate,
- automatically distribute agent certificates that use the new root authority, while keeping the same agent IDs.

New certificates can start being distributed six months in advance, so that agents that are seldom online can be updated, and the increased server load can be spread out over a long period.

For further information, refer to the document *Renewing the SES root certificate authority* available on the [Stormshield technical documentation website](#).

### Compatibility with Windows 10 version 1903 May 2019 update

The operation of the SES agent has been validated on the new version of the Windows 10 version 1903 May 2019 update operating system. The lowest version of the SES agent required is version 7.2.26.

If you use a version of the SES agent lower than version 7.2.26 in Windows 10 version 1903, USB devices may not be properly detected and blocked.



# Stormshield Endpoint Security 7.2.26 fixes

## Console fix

### Modified agent merge

Support references T2609, CF88415 - 153940PW

The merging of agents by host name or by Active Directory name has been enhanced. They are now processed incrementally agent by agent instead of all agents at one go. Among other benefits, this makes it possible to:

- reduce the number of issues regarding competing access to the database,
- keep successful merges if users cancel processing or in the event of a processing timeout. The duration of a merge, previously set to two minutes, now times out after an hour.

Individual agent merges have not been modified.





## Stormshield Endpoint Security 7.2.25 resolved vulnerability

---

From version 7.2.20 onwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

Support reference T3064

### OpenSSL upgraded to version 1.0.2r

The vulnerability [CVE-2019-1559](#) has been fixed by upgrading the OpenSSL cryptographic library to version 1.0.2r. Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.



# Stormshield Endpoint Security 7.2.25 fixes

## Console fix

### Correction of version numbers in policies and configurations

Support references CF88585 - 158368CW

In the Agent Monitoring panel, policy and configuration versions may have been inconsistently numbered in cases where agents remained disconnected during and after a policy or configuration update. This anomaly has been fixed.

## Agent fixes

Support references CF88818 - 162361CW

### Workstation completely freezes when other security programs have been installed

The SES agent no longer causes the workstation to freeze completely when other security programs are present on the workstation, such as with McAfee ENS, for example.

Support references CF88823 - 162539CW

### Error message displayed with Adobe Acrobat Reader

A message indicating the error "The application was unable to start correctly (0xc0000022)" would appear whenever a PDF document was opened with Adobe Acrobat Reader on a workstation equipped with the SES agent. This issue has been fixed.

Support references T2910 - CF88863 - 163419CW

### BSOD occurring when the workstation goes into sleep mode or wakes up

In some cases, processing a list of pending network packets would cause a BSOD (blue screen). The BSOD would often occur when the workstation goes into sleep mode or wakes up. This issue has been fixed.



## Stormshield Endpoint Security 7.2.24 new feature

From version 7.2.20 upwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### **Compatibility with Windows 10 1809**

We have validated the SES agent was compatible with the new Windows 10 1809 SAC and LTSC operating system. The version 7.2.22 of the SES agent is the minimal version required.



# Stormshield Endpoint Security 7.2.24 fixes

## Server fix

**!** **Regeneration of the certificate for secure connections to the Apache server (HTTPS)**  
From January 20, 2019 onwards, SES agents will no longer be able to retrieve certificates from the embedded Apache server using a SES server older than version 7.2.24.

We recommend that you update your servers to version 7.2.24 in order to renew the Apache (HTTPS) certificate and allow new agents to download their certificates.

If you do not install version 7.2.24, you can manually regenerate this certificate on each SES server in the pool.

To manually regenerate the Apache server (HTTPS) certificate:

1. Stop the "Stormshield Endpoint Security Server" service on the SES server,
2. Run the `C:\Program files(x86)\Stormshield\Stormshield Endpoint Security Server\Apache\gen_new_Apache_cert.bat` file as an administrator,
3. Restart the SES server.

From version 7.2.24 of the SES server onwards, the Apache server (HTTPS) certificate will always be regenerated every time the SES server is updated.

You can stop this certificate from being renewed during the update of the SES server. To do so, before beginning the update, add a DWORD type of `DoNotGenerateCgiCert` value with its value set to 1 in the registry key:

- "HKEY\_LOCAL\_MACHINE\SOFTWARE Wow6432Node\Stormshield\Stormshield Endpoint Security Server" on a 64-bit operating system,
- "HKEY\_LOCAL\_MACHINE\SOFTWARE\Stormshield\Stormshield Endpoint Security Server" on a 32-bit operating system.

## Console fixes

### Creation of removable media for recovery: replacement of WinPE 8.1 with WinPE 10-1809

The help provided in the SES console in the Windows Preinstallation Environment (WinPE), allowing the creation of removable media when an encrypted disk needs to be recovered, has been updated. It is now based on WinPE version 10-1809.

### New trusted rule in the rule group regarding McAfee programs

Support references CF88643 - 156774PW

SES previously blocked the executable file `setuppcc.exe` run during the installation of McAfee Endpoint Threat Protection. A trusted rule has been added in order to allow this executable file to be run.



### Update of Windows certificates

The Basic template policy previously blocked the executable file *setupprep.exe* run during the migration from Windows 1803 to 1809. Windows certificates have been updated to allow this executable file to be run, and enable the migration from Windows 1803 to 1809.

### Improvement of performance when merging agents

Support references CF88415 - 153940PW

Merging agents in the console by host name or by Active Directory name would take more than two minutes whenever the database was particularly large. The length of this operation would cause an error in the console. Performance for this operation has been improved to speed up the merger.

## Agent fixes

### Correction of issues during migration from Windows 10 1709 to 1803

Support references CF88679 - 159197CW

On certain hosts with startup configurations stored on auxiliary FAT partitions instead of on the main NTFS partition, the startup configuration will no longer be lost during the upgrade to version 1803. Furthermore, Windows will no longer start up in troubleshooting mode.

### Correction of issues during the setup of HoneyPot protection

Support references CF88702 - 159852CW

In certain cases, the use of trusted applications together with HoneyPot protection enabled would cause errors during its setup. This in turn would slow down access to files and the registry database. The setup of HoneyPot protection is now operational in all cases and slowdowns no longer occur.

### Correction of latency issues when printing

Support references CF88777 - 161297CW

On some computers with the SES firewall enabled, printouts would be launched after several minutes. This issue has been fixed.



## Stormshield Endpoint Security 7.2.23 new feature

From version 7.2.20 onwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

### **Shutting down the agent from a workstation**

Whenever the dynamic configuration of the agent allows it, the user can now shut down the agent by clicking on the **Disable** link from the agent interface on the workstation. If the configuration does not allow shutting down the agent, clicking on this link will open the challenge window.



# Stormshield Endpoint Security 7.2.23 fixes

## Agent fixes

### Incompatibility with ArcGIS Explorer Desktop

Support references CF88610 - 158672CW

The RCP protection on the SES agent no longer causes the ArcGIS Explorer Desktop program to hang during startup.

### Configuration of temporary web access from the agent

Support references CF88593 - 158463CW

In cases where users have shortcuts on their workstations to request temporary web access, the options "/GrantWebAccess" and "/NoConfirm" to be added to the target of the *ssmon.exe* executable file shortcut have been corrected. The first option has since become case-sensitive and the second would cause the opposite effect.

### Incompatibility with the Symantec Endpoint Protection 'System lockdown' feature

Support references CF88327 - 154855CW

The cohabitation of SES agents with Symantec Endpoint Protection agents on which the "System lockdown" feature has been enabled no longer generates internal error messages in SES system protection logs.

## Console fixes

### Deployment of configuration changes in the environment

The name of the **Apply changes to the environment** button has been changed. The button is now called **Deploy to the environment**.

### Policy and configuration version number in the Agent Monitoring panel

Support references CF88585 - 158368CW

In the Agent Monitoring panel, the **Policy** and **Configuration** columns now indicate version numbers along with names.

### Update of the Agent Monitoring panel

Support references CF88260 - 154383CW

In the Agent Monitoring panel, whenever new policies or configurations were deployed in the environment, the **Config. Status** column would occasionally indicate a "valid" status for a while even though the new policies or configurations that were applied were not yet visible in the **Policy** and **Configuration** columns. The duration of this display has been reduced to 30 seconds. As soon as the status becomes valid again, the names and numbers of the policies and configurations will therefore be updated in the console within 30 seconds.



### Removal of the learning feature

The learning feature in the agent's dynamic configuration policy has been removed. As such, the **Application behavior control** section in the security policy has been modified. The **Registry access** protection has been removed, and the **File access** and **Execution control** protections now only have two possible settings left: enabled or disabled.

### Format of the application identifier hash

During the creation of an application identifier using a hash, it may contain spaces or dashes, which are deleted when the identifier is being confirmed.

### Adaptation of menus and buttons according to user role

The buttons for modifying a policy as well as the **Add internal directory** menu are no longer available to users who do not have the privileges to carry out these actions.

### Console reports

**Real-Time** reports are now consistent with the values shown in the **Monitoring > Agents** panel.

### Names of columns switched in the security policy

The names of the **Access to this application** and **Applications access** columns in the security policy, in the **Application control** tab, in the **Trusted applications** menu, had been switched. This error has been fixed.





# Stormshield Endpoint Security 7.2.22 new features

From version 7.2.20 onwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

## Modernizing SES console's user interface

SES console's interface has been modernized and simplified. Changes in graphics and menu names improve the interface's user-friendly design and facilitate the control and use of the console.

Likewise, the **Licenses** menu in the **Monitoring** section (which displays a report indicating information on your licenses) has been moved to the **Reports** menu so that it appears among the other types of reports.

## Support for SQL Server 2017

SES now supports SQL Server 2017.

## Compatibility with Windows 10 1803

The Windows 10 1803 April 2018 Update operating system is compatible with SES 7.2.22.

## Modifying information displayed in the agent monitoring panel

The **Agent Identifier** column has been added to the agent monitoring panel. It is hidden by default. It is now possible to sort and filter agents according to their identifier.

The **Last synchronization** column has been added and placed after the **Configuration** column. It is displayed by default. It indicates the date and time that the agent received and applied the latest policy and configuration file.

The **Last configuration** column has been removed.

## Displaying the SES icon on workstations

Support references CF88063, T1534, 152698PW

The new **Displaying icon in the status bar** option in the dynamic agent configuration makes it possible to select the agent monitor's icon display mode on the workstations. This option is selected by default. If this option is not selected, the monitor's icon is not visible in the status bar. Moreover, the notification display option is automatically unselected and grayed out.

## Activating the agent monitor in the Start menu

It is now possible to activate the agent monitor in the **Start** menu on workstations.

## Uninstalling the SES agent via the Windows control panel

On workstations, the Stormshield Endpoint Security Agent entry is now visible in the Windows control panel enabling a program to be uninstalled. It is therefore possible to uninstall the agent via this panel if stopping the agent is authorized in its policy.

## Integrating policies in the agent installation program

Support reference T1639

It is now possible to integrate current policies in the agent installation program. To do so, simply copy the file *sync/Agent.srz* in the folder *Apache/cgi-bin*, then restore the installation programs.



During the agent's installation, you will need to retrieve the agent's certificate for the agent to be operational, as indicated in the *Login and password for downloading certificates* section of the *Administration Guide*. In this way, it is possible to deploy functional agents even if they don't have access to the SES server



# Stormshield Endpoint Security 7.2.22 fixes

## Agent fixes

### Controlling a Terminal Server (TSE) session remotely

Support references CF 88448, T1515, 155784CW

It was not possible to take control of a TSE session remotely from a SES Server-Side Edition agent. A notification indicated that access was denied after confirming the transfer of control. This problem has been fixed.

### Decrypting the hard disk via recovery media

Support references CF 88413, T1578, 154773PW

When *NepRecovery.exe* is used from a recovery media file, the error message indicating that the password was wrong or that the *.srr* file was corrupted no longer appears if the *.srr* files are large.

### Machine freezes when launching an executable file on a DFS server

Support references CF 88133, T1388, 153165CW

Launching an executable file from a DFS server systematically caused the workstation equipped with the SES agent to freeze for two minutes. This problem has been fixed.

### Evolution of the log file format

Support reference T492

The log files now contain the process identifier (PID) that generated the log line.

### New log file after uninstalling the agent

Support reference T1477

After uninstalling a SES agent, the new log file *framework.log* is copied into the directory *%WINDIR%\Temp\Stormshield*.

### Incompatibility between Sophos Endpoint Protection and SES

Support references T1694, CF 88315, 154850CW

In certain cases, specifically when other security software programs like Sophos Endpoint Protection v10.7 were installed on the workstation, a blue screen could occur when protection against memory overflow was active. This problem has been fixed.

### Applying a corrupted configuration

Support references CF 88524, T1702, 155827CW

When the agent received a corrupted configuration, it would unsuccessfully try to interpret the configuration. Now the agent waits to receive a new configuration.



## Applying policies

Support references CF 88515, T1641, 157247CW

When a policy or a script was applied on a condition related to the Active Directory user and when the domain controller took a long time to respond, it took a long time for the policy to be applied. This problem has been fixed.

## Order used to apply Wi-Fi access point rules

Support reference T1465

Until now, Wi-Fi access point rules were applied in the order of their group, whereas all other rules are applied in the order of their rank, irrespective of their group. The Wi-Fi rules now behave like the others.

## Circular logging in the trace manager

Support references T1769, CF 88306, 153218PW

In the trace manager, it is now possible to choose circular logging to store traces and so restrict the size of the log file.

## Server fixes

### Evolution of the log file format

Support reference T492

The log files now contain the process identifier (PID) that generated the log line.

### New log file after uninstalling the server

Support reference T1477

After uninstalling the SES server, the new log file *framework.log* is copied into the directory `%WINDIR%\Temp\Stormshield`.

### Managing the migration

Support references T1073, CF 88528, 155829PW

Now, when a server gets a configuration and policies from a SES console, it disregards them if it already has a configuration and policies from a more recent console.

## Console fixes

### Changing the console's password

Support references T1715, CF 88546, 157780CW

The form to change the console's password limited its size to 20 characters. The limit is now 128 characters.



## Displaying the connection status of agents

Support references T1704, CF 88261, 154426CW

The console could display agents as being connected when they were no longer connected. This problem would occur when an agent was disconnected from the server (or outside the network) and the server was rebooted before registering that the agent had logged off.

## Displaying the version of the server and of SES agents

Support references T1627, T1477

In the console, the version of the server and agents is now displayed as 7.2.22 instead of 7.222. This change also applies to agents that are listed in the monitoring panel and have a previous version. It is also visible in the XML file exported from the agent monitoring panel.

## Importing and exporting log filters

Support reference T1488

The enabled/disabled status of each log filter in the log manager is now correctly exported and imported in the *lfxml* file.

## Saving the first operator of an advanced filter in the log display


Support reference T1490

In advanced log monitoring filters, the first operator was not saved. It was replaced by an active IF AND when an advanced filter was imported or after the console was closed and reopened. The first operator is now saved.

It should also be noted that when advanced filters are disabled, the filter is recalculated according to the operators available in non-advanced mode.

## Console administration logs

Support reference T1599, CF 88501, 157144CW

When an administrator changed the policy applied to an environment or to a user group via the drop-down list and not by the  button, the modification of the link of the policy to the environment would not be logged. This problem has been fixed.

## Copying and pasting rules

Support reference T1120

When an application rule was copied and pasted from another security policy, agents would not send a log to the server to signal the application of this rule. This problem has been fixed.



## Merging agents

**Support references T1760, CF 88415, 153940PW**

When the log database contained an extensive history of agent connection logs (several years' worth), merging agents in the console could take longer than two minutes and ultimately fail. In order to offer the possibility to reduce the size of this history, an option to clean agent history has been added to DbInstaller's **Log and monitoring database maintenance** menu.

However, if there is an extensive history of agent connection logs, updating the log and monitoring databases can take several minutes.



# Stormshield Endpoint Security 7.2.21 fix

## Agent fix

### Incompatibility with the Spectre/Meltdown fix for Windows 7 and 8.1 32 bits

Support references T1643, T1644

The Microsoft fix against Spectre and Meltdown vulnerabilities caused an incompatibility with SES on Windows 7 and 8.1 32 bits. This issue has been fixed. In the future, if another incompatibility of this type occurs, the SES protections impacted would be automatically disabled. The error message "Internal Error 17" would display.



# Stormshield Endpoint Security 7.2.20 new features

From version 7.2.20 upwards, SES no longer allows the administration of the Avira antivirus solution. If you have this option, please refer to the section [Recommendations](#) before performing the upgrade.

## Installing SES

Only one file is needed now to install SES (*setup.exe*). The *bin* folder containing the files *server.exe* and *console.exe* no longer exist. However, the installation program dedicated to only the server remains available.

## Encryption and enrollment of removable devices

Support reference T1322

It is now possible to encrypt enrolled removable devices or enroll encrypted devices. Warning: when a device is decrypted via the SES console on an agentless SES workstation, its contents will no longer be considered trustworthy.

## Supported versions of Microsoft SQL Server

Support reference T1309

An SES server can now be installed with a version of SQL Server that SES does not recognize. This will open a warning message.

## Getting started guide

A new *Getting started guide* is available in your [MyStormshield](#) area. It provides help and recommendations on how to deploy and operate SES 7.2.





# Stormshield Endpoint Security 7.2.20 fixes

## Agent fixes

### Incompatibility with the Spectre/Meltdown fix for Windows 10 32 bits

Support reference T1550

The Microsoft fix against Spectre and Meltdown vulnerabilities caused an incompatibility with SES on Windows 10 32 bits. This issue has been fixed. In the future, if another incompatibility of this type occurs, the SES protections impacted would be automatically disabled. The error message "Internal Error 17" would display.

### Windows disk repair tool

Support reference CF 88404

SES no longer prevents the Windows disk repair tool *chkdsk* from repairing a disk when the workstation starts.

### Improved stability

Support reference T1281

It is now no longer possible to lose the agent configuration file *conf.srx*. It is regenerated every time the workstation is restarted or when policies to be applied are reassessed.

### Uninstallation of the agent on Windows 10

Support reference T1424

When an agent is uninstalled on a Windows 10 operating system in version 1709 or higher, it no longer cause network connections to be lost when the operation is complete.

### New logs after the uninstallation of the agent

Support reference T1424

The log file *\log\updater.sro* is now split into three files:

- *\log\installer.sro*: logs relating to installation
- *\log\updater.sro*: logs relating to updates
- *\log\uninstaller.sro*: logs relating to uninstallation

After an agent has been uninstalled, the folder *%WINDIR%\Temp\Stormshield* will be created and the following log files will be copied into it:

- *install.log*
- *SRSservice.log*
- *installer.sro*
- *updater.sro*
- *uninstaller.sro*



## Console fixes

### User passwords

Support reference T1274  
Passwords longer than 20 characters can now be entered when users are logged on to a SES console. There is no longer a maximum limit on the number of characters.

### Number of connections to a server

Support reference CF 88335 - 154830CW  
The number of simultaneous connections to a SES server has been increased from 1000 to 2000, and the number of agents assigned to a server is no longer restricted.

### Exporting agents

Support reference T1282  
In the agent monitoring panel, agents to be exported can be selected in an *.xml* file. Three options are offered: the list of all agents, the list of selected agents or the list of agents displayed.

### Performance enhancement

Support reference T1316 CF 88157  
The **User Manager** panel appears more quickly than it used to, even when a large number of users has been configured.

Changes are applied to the environment more quickly when several SES servers have been configured.

### Policies in the agent monitoring panel

Support reference T862  
The policy displayed by agent in the **Agent Monitoring** panel would occasionally be wrong. It is now displayed correctly.



# Stormshield Endpoint Security 7.2.19 new features

## New trace manager

SES offers a new trace collection tool on workstations that are equipped with the agent. The trace manager makes it possible to gather various traces relating to the process of running the agent, the operating system, and the network. Trace collection can be activated directly from the agent, in command line or from a configuration file.

The trace manager is able to retrieve the following information:

- Agent logs,
- Agent traces,
- Information gathered by Msinfo32,
- Problem Steps Recorder (PSR),
- Device tracking,
- Windows event logs,
- IP configuration,
- Routing table,
- Network traces.

This new tool enables more accurate diagnoses in the event of any abnormality in the behavior of the SES agent. For more information on using the trace manager, refer to the *SES Administration guide*.

## Compatibility with 32- and 64-bit versions of Windows 10 1709

Support reference T1083

SES now runs on 32- and 64-bit Windows 10 1709 operating systems. As such, you can upgrade your Windows 10 1703 system to Windows 10 1709 without having to uninstall SES.

## Management of rule sequence on trusted applications

Support reference T948 (153682CW)

In a security policy, you can now select the evaluation mode of rules that apply to trusted applications. The new **Rules Evaluation** column, available in advanced mode, offers two possibilities for each rule:

- **Go to next rule:** the next rule that applies to the same application will be evaluated and applied accordingly.
- **Skip next rules:** as soon as the rule applies, the following rules that apply to the same application will be ignored.

Previous versions of SES did not offer this option. Up until version 7.2.11, only the first rule concerning an application would apply, while the following rules would be ignored. From version 7.2.12 to 7.2.18, all rules concerning an application would apply. From version 7.2.19 onwards, the default option is **Go to next rule**.



## Manual pre-enrollment of devices

Support reference T1155

Removable devices can now be pre-enrolled using their serial numbers without the need to plug them into the workstation that hosts the administration console. Whenever the device is plugged into a workstation on which the SES agent has been installed, enrollment will be automatic.

## Revocation of enrolled devices

Support reference T1017

Enrolled or pre-enrolled removable devices can now be revoked without the need to plug them into the workstation that hosts the administration console. Whenever a revoked device is plugged into a workstation hosting an SES agent, all traces of enrollment via SES will be deleted, preventing the device from contacting the SES agent. Revoked devices can be enrolled again in an administration console.

## Copying and pasting device serial numbers

Support reference T1133

The serial numbers of enrolled, pre-enrolled or revoked devices can now be copied and pasted from the enrollment panel to a security policy.



# Stormshield Endpoint Security 7.2.19 fixes

## Agent fixes

### Internet Explorer 11 usage

Support references: CF88112, 153057CW, T1054

Internet Explorer 11 now runs correctly with SES and Sophos Endpoint Security and Control (version 10.7).

### Application of a security policy containing hash-based identifiers

Support reference: T620

Whenever an agent with a policy that does not contain any hash-based application identifier receives a new policy that contains hash-based identifiers (for example, the standard policy template), the workstation will no longer freeze as it used to previously.

### Loss of USB device names

Support references: 153143PW, T1115

Whenever a policy with removable device enrollment is applied to an agent, the name of the volumes on USB devices will now appear in Windows Explorer and the autorun dialog box will now appear when such devices are plugged in.

### USB device enrollment in Windows 8.1 and 10

Support references: T845, 153084PW

Whenever USB drives formatted in Windows 8.1 or 10 are enrolled, they will now be given a trusted status.

## Console fixes

### Agents merger in the monitoring panel

Support references 15394PW

Agents merger by NetBIOS or AD name in the agent monitoring panel no longer fails in some cases.

### Updates to the dedicated McAfee rule group

Support references 151571CW, CF87829, T1075

New trusted rules have been added to the McAfee rule group in order to enable the installation and update of the McAfee HIPS module whenever SES has already been installed on the workstation.



# Stormshield Endpoint Security 7.2.18 new features

## Updating the security policies template

A new trusted rule for user account control (consent.exe) has been added to the template to allow application access to be controlled.

Similarly, the rules for Microsoft Office have been enhanced to include the rules for Microsoft Office 365.

## Support for multiple signature of applications

An application can be signed by several certificates. When creating an application ID for security policies, you can now choose the certificate that will be used to identify the application.

Support reference 152719CW

## Adding a new trusted domain in application rules

The new **Attachment Disabled** trusted domain has been added to the trusted applications rules in advanced mode. If this trusted domain is enabled in the rule, SES does not attach itself to the application in question and does not directly modify the memory of this application. This makes it possible to define rules so SES can coexist with other applications that do not tolerate this kind of attachment and avoid incompatibility issues. This trusted domain only applies to 64-bit systems.

## Configuring Syslog messages for Stormshield Visibility Center (SVC) in the installation wizard

In the table configuration maintenance of the SES installation wizard, a new functionality allows a script to be run that configures log messages so they can be read by the Stormshield Visibility Center product.

Support reference 152307PW

## SES file corruption prevention

A new mechanism on the agent and the SES server prevents SES configuration files from being corrupted as well as recovery from corrupted files.

## Addition of the %HOSTID% variable in the logs sent to a third-party server

You can now use the %HOSTID% variable in the logs sent to a third-party server via SMTP and Syslog protocols. This variable is replaced by the agent's certificate ID or by an empty string if the log is sent by the SES server.

## Memory overflow protection

On 64-bit operating systems, a log is now sent when the SES agent blocks stack pivot-type behavior from a 32-bit application.

## Physical memory access protection

A log is now sent by the SES agent when it blocks an attempt to directly access physical memory.

Support reference 153478CW

## Peripheral device protection

In the device group settings, the new **Read access** audit level has been added.



# Stormshield Endpoint Security 7.2.18 fixes

## Agent fixes

### Display USB devices in the explorer

Support reference 153143PW

In Windows Vista and later versions of the operating system, the names of FAT or NTFS volumes on USB devices were not displayed in Windows Explorer when an SES agent was connected. The AutoRun dialog box was also not displaying when these devices were connected. Both problems have been fixed.

### Incompatibility with IBM Trusteer Rapport

Support reference 152066CW

Using the Rapport software to protect banking web sites at the same time as SES on 64-bit operating systems was causing Internet Explorer and Google Chrome to crash. The issue has been fixed for Microsoft Windows 8.1 and 10.

### Full disk encryption

Support reference 152215CW

Some communication protocols between the operating system and the hard drives were not supported by SES. This made encrypting certain drives impossible. This problem has been fixed.

### Trusted applications

Support reference 152886CW

When an application identifier used a certificate, an application might not have been considered a trusted application right after it was launched. This problem has been fixed.

### Incompatibility with Atempo Live Backup

An incompatibility with Atempo Live Backup software has been fixed. This incompatibility caused work stations to freeze on the Windows startup screen.

### Incompatibility with Microsoft Edge

Support reference 153466CW - 153963CW - 153903CW

An incompatibility between the Honeypot Protection (HPP) and Microsoft Edge on Windows 10 version 1703 has been fixed. This incompatibility was blocking Edge for several seconds during launch, and then caused it to close.

## Server fixes

### Recovery session in the key database missing

Previously, you could not recreate an agent encryption session if it had been removed from the key database. Now, if the key is no longer in the database, it is recreated when the next workstation is started.

### Apache server component updated to version 2.4.27

The Apache web server has been updated to version 2.4.27.



## Console fixes

Support reference 152977CW

### Console interface freezes

In some cases, when the OS theme, screen resolution or user preferences changed, the console's user interface would freeze and become unresponsive. This problem has been fixed.

### Use of TLS 1.2 for exchanges between the console and the server

In some cases, the administration console used TLS 1.0 to exchange information with the SES server. Now TLS version 1.2 is systematically used.

Support reference 153321CW

### Order of rules in security policies

In some cases, such as when copying and pasting rules, two rules could have the same rank. This problem has been fixed.

Support reference 151939PW

### Corruption of the recovery media file

When creating a recovery media file with a large number of keys, the creation of the key registry would sometimes fail. This problem has been fixed.

Support reference 152719CW

### Adding McAfee ETP rule groups for import

The new McAfee ETP rule groups for import makes the use of McAfee Endpoint Security Platform and Threat Prevention products compatible with SES.





## Stormshield Endpoint Security 7.2.17 new feature

---

### **Pre-enrollment of removable devices**

It is now possible to pre-enroll many removable devices from the SES console by importing a .csv file listing all the devices to enroll. When a pre-enrolled device is connected to an SES agent, it is automatically enrolled.



# Stormshield Endpoint Security 7.2.16 new features

## New automatic enrollment mode

A new automatic enrollment mode makes it possible to enroll removable devices for Windows users other than the connected user. This mode can be enabled in the **Device Control** tab in a security policy.

After you have plugged in a removable device, a window will appear allowing you to enter the Windows login identifiers of the user for whom you wish to enroll the device.

## Hidden "Removable devices" menu on SES agents

The removable device management menu no longer appears on the SES agent if the encryption of removable devices has been disabled in the agent's security policy.

## Order in which rule groups are displayed in the console

In the administration console, rule groups in the **Device control**, **Network security control** and **Application control** tabs are now displayed in alphanumeric order instead of the order of their creation.

## Copying and pasting application identifier entries

In the administration console, a pop-up menu has been added to the list of application identifiers, and to identifier entries. Among other functions, it allows copying and pasting entries from one identifier to another, or copying entries from several identifiers at the same time.

## Accessing the 64-bit registry in script tests

A new parameter, **Registry redirection (on 64-bit systems)**, has been added to script tests that search for a registry key or the value of a registry key. 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. All registry tests that existed before the upgrade to version 7.2.16 will be assigned the value *Enabled* for this new parameter, corresponding to the behavior of versions prior to 7.2.16.

## Changes to password strength levels

Password strength levels in encryption policies have been modified. They are now **High**, **Standard** and **Low** and the value applied by default is **Standard**.

The criteria for password strengths have changed as well:

- **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.

A password strength checker has been added for the creation of recovery media. The strength of this password must now be High.



### **NepRecovery**

A message has been added to the NepRecovery tool shutdown process, reminding the user to remove the recovery medium.

A password strength checker has been added for the modification of the user's password, the strength of which must now be at least Standard.

### **New layout of windows for creating and importing policies**

In the administration console, the following changes have been made to the windows in which policies are created and imported:

- Policy files can now be imported without the need to create a blank policy beforehand,
- The policy file import feature now allows several files to be imported at once,
- Existing policies can now be used as templates during the creation of policies,
- Templates of existing rule groups can now be imported when importing policies.

### **Display of automatically enrolled keys in the console**

Keys that have been automatically enrolled are now shown in the console along with keys that have been manually enrolled by administrators. This display depends on logs sent by agents when users use automatic enrollment.

### **Signature certificates**

SES now recognizes SHA-256 signature certificates from Windows 7 upwards.

### **Changes to the names of file access privileges in application rules**

Privileges have been renamed in application rules, in the **Application control** tab, under the **Files** column. The following privileges, from the most to the least restrictive, are now available:

- Access denied
- Read Only - RX (execution allowed)
- Read/Write - RW (execution denied)
- Read/Write - RWX (creation denied)
- Full access - RWX

### **New signature certificate**

As the signature certificate of Stormshield products' code has been renewed, a new certificate has been deployed. To comply with the new name of the company, the certificate now bears the Stormshield name instead of SkyRecon.



# Stormshield Endpoint Security 7.2.16 fixes

## Agent fixes

Support reference #CF 87791

### Veeam Backup compatibility

The procedure for restoring the Veeam Backup solution would freeze on the action *Unmounting partition*, and the option offered by Veeam (*Cancel*) did not allow the database to be restored. This issue has been fixed.

Support reference #CF 87920

### Fixes in heap spray protection

False positives with heap spray protection would occasionally prevent the user from opening certain legitimate files. These false positives have been fixed and heap spray protection is now more accurate.

### Removal of DRIVER\_ERROR logs during new installations

*DRIVER\_ERROR* messages are no longer shown during new installations of SES as they are irrelevant in this case.

Support reference #CF 87797

### Update of the encryption driver in the Windows recovery image

During updates of the agent, the encryption driver would not be updated in the Windows recovery image. It would then be impossible to access data on the disk during attempts to restore the system.

To fix this issue, this driver will be updated at the same time as the agent from now on.

Support reference #CF 87829

### McAfee FRP compatibility

An incompatibility between SES and McAfee FRP (File and Removable media Protection) could cause the workstation to freeze and prevent USB drives from being plugged in. This issue has been fixed.

### Failure during agent update

The update of an agent could fail when the security policy contained rules which blocked the creation of system files. The upgrade process now correctly handles this use case.

Support reference #CF 87934

### Compatibility with Bromium

The SES agent in version 7.2.15 prevented Bromium software from being initialized on a workstation. This issue has been fixed.

Support reference #CF 87839

### Flows normally allowed by the security policy blocked

Outgoing flows normally authorized by the security policy were blocked by the SES firewall. The firewall could deny a connection in stateful mode under certain conditions. This behavior has been fixed.



## Console fixes

### **Incompatibility of full disk encryption with database servers older than version 7.2.15**

It is now possible to encrypt agent in versions older than 7.2.15 by using databases in 7.2.15.

### **Error during USB drive enrollment**

Whenever Active Directory users attempted to enroll a USB drive, the **Enrolled by** field in the enrollment window would remain empty if certain LDAP attributes were missing for the connected user. The console now correctly retrieves the current user in the LDAP directory.

### **Warning before overwriting a database backup**

Whenever databases are backed up using the database maintenance utility (DbInstaller), the program now asks the user to confirm before overwriting the file if it already exists.

### **Console monitoring**

As part of efforts to improve user comfort, the **Event Viewer** menu in the console interface is now called **Console Monitoring**.

### **NepRecovery launch fixed**

The NepRecovery tool no longer ran properly on Windows PE operating system since the SES 7.2.15 version. This issue has been fixed.



## Stormshield Endpoint Security 7.2.15 new features

### Detection and automatic repair of desynchronized recovery passwords

The SES agent now verifies the validity of recovery information with the server every time an encrypted workstation starts up. In the event that the agent's recovery information is not synchronized with the server's recovery information, an automatic repair process will be launched. This makes it possible to ensure that the recovery password can continue to be used without generating errors.

To take advantage of this feature, you will need to update the encryption key database with the databases' maintenance utility (DbInstaller).

### Upgrade to .NET Framework 4.6.1 for the management console and related tools

The management console and related tools previously used version 4.0 of the .NET Framework. As Microsoft no longer provides support on this version, SES now uses version 4.6.1. As a result of this upgrade, these components can no longer be installed and used on Windows XP and Windows Server 2003 systems.

### Device groups managed in the security policy

The **Group management** parameter has been added to the **Device control** tab of the security policy. This parameter makes it possible to enable or disable all features relating to removable device groups in the security policy: audit, device encryption, enrollment, etc.

If the **Group management** parameter is modified in the policy, we recommend that you restart your workstations so that the SES agents can correctly apply the new security policy.

For more information, refer to the Stormshield Endpoint Security *Administration guide*.

### Information on the configuration of the SES agent in the registry base

Information on the SES agent's configurations and current policies will now be stored in the registry base on users' workstations. Keys contain the names, versions and dates on which static and dynamic configurations, as well as security, encryption and antivirus policies were applied. They also contain the limit on the version of the agent update, the agent mode (Normal, Warning or Standby) and any potential "Disable Protections" and "Antivirus control" challenges in progress.

For more information, refer to the Stormshield Endpoint Security *Administration guide*.

### Display of logs for the current session on the SES agent

The SES agent now displays only logs for the current session by default, meaning since the last time Windows was restarted or since the last time the agent logged back on after a shutdown.

The other display options (all logs, 20, 50, 100 and 200) can still be selected from the drop down list at the bottom right of the log window.



# Stormshield Endpoint Security 7.2.15 fixes

## Agent fixes

### Policy application

In previous versions of SES, a lag would occur between the display of logs indicating the application of a policy and the functional application of the policy. Logs now indicate the effective application of a new policy. As for application control rules, learning rules have been disabled in order to avoid compromising performance. Exceptions must be explicitly indicated from now on in application rules.

Support reference 11877

### Blocked policy application during the update of the Avira antivirus license

SES agents installed with Avira antivirus may be prevented from applying policies during updates of Avira licenses. Such updates now no longer prevent the SES agent from running, as the agent continues to apply policy changes sent by the server. Furthermore, in the system logs of event logs, whenever the Avira license expires, a log entry will appear indicating the expiration.

Support reference #CF 87633

### Installation of the Stormshield VPN on Windows 10 1607 CBB

On workstations equipped with the SES agent and Windows 10 1607 CBB operating system, the Stormshield VPN would incorrectly install and its virtual network adapter would not appear in the control panel. The installation of this network adapter now runs properly.

### Irrelevant VOLUME\_DENIED log

A VOLUME\_DENIED log would appear in the *device.sro* file every time a user plugged a device into a workstation, even when the configuration did not block such devices. This log will now only appear when access to the device has been explicitly prohibited.

Support reference #CF 87626

### Incompatibility of SEP 14 with RCP protection

Whenever Symantec Endpoint Protection 14 was installed on a workstation and RCP protection was enabled on SES, certain applications would stop functioning, in particular Mozilla Firefox, Internet Explorer, and the Symantec Endpoint Protection service itself. This issue has been fixed.

### Unnecessary auto-protection logs

On the SES agent, many [AUTO-PROTECTION] [OPEN-PROCESS] logs would appear in the *heimdall.sro* file found in the SES agent's log folder. These logs would appear every time a process attempted to access information about SES processes. These logs have been removed as prohibiting access to SES processes is part of the product's usual behavior.

Support reference 151256CW (#CF 87724)

### Compatibility with 64-bit Microsoft Office 2013 and 2016

SES was incompatible with the 64-bit versions of Microsoft Office 2013 and 2016 products. All of these products now run correctly on supported operating systems.



### Microsoft Windows 10 application consoles

Whenever an application rule prohibited console applications from creating files in Windows 10, such applications would not be able to launch (even in Warning mode). This issue has been fixed.

### Incompatibility between SES control on running applications from removable devices and McAfee device encryption

The control feature on running applications from removable devices is now working on devices encrypted with the McAfee FRP feature: the warning window is displayed and the executable is blocked if any.

Support reference #CF 87789

### Windows session opening after an update of the agent

After the agent was updated on a workstation, when the computer restarted, the user's Windows session could not open again. The issue occurred when the agent applied at least one security policy containing one or more certificates. This issue has been fixed.

## Server fixes

### Simplification of the server's update mode

The parameter for changing the server's update mode via the console has been removed. The default update mode is now automatic mode. The server will continue to check for new updates when the SES service starts. Caution: if servers have been configured in manual update mode, they must be upgraded before the console to version 7.2.15 so that they do not remain frozen in manual update mode; otherwise, switch them to automatic update mode before upgrading to version 7.2.15.

### Simplified retrieval of updates by the server

SES servers' ability to retrieve their updates on remote servers will now be restricted to local folders and Windows shared folders. SES servers can no longer retrieve updates on FTP or HTTP servers. In the **Software Updates Settings** section in the server policy, the **Source type**, **Port**, **User name**, **Password** and **Remote path** parameters have been removed. The **URL/Local path** parameter has been renamed **Updates download folder**.

For more information, refer to the Stormshield Endpoint Security *Administration guide*.

## Console fixes

### Enhanced port searches

In network firewall rules and network application sub-rules, the only search criterion for ports was their names. It is now possible to search for a port either by its number, name or description. Furthermore, users can now resize windows.

Support reference 9542

### Backup and restoration functions on databases' maintenance utility (DbInstaller)

Errors occurred preventing databases from being restored. This issue has been fixed.

### Log Manager

Dans une démarche d'amélioration de l'ergonomie de l'interface de la console, le menu **Éditeur de logs** se nomme désormais **Configuration des logs**.





**Error in the report “Stormshield Endpoint Security Configuration Changes”**

In the console, when opening the report about the SES configuration changes, it displayed an error related to the database for policies storage. This issue has been fixed.



## Stormshield Endpoint Security 7.2.14 new features

Support reference 150843PW

### App-V 4.6 paths: dealing with backslash

It is now possible to specify paths starting with a single backslash “\” (in addition to drive letters « X:\ » and to UNC paths “\\”) in application identifiers paths, in the applicative rules. This feature allows writing paths for applications virtualized with App-V 4.6.

### Updating Windows 10 CBB 1511 to the "Anniversary Update" 1607 version

Updating a workstations environment to the Windows 10 1607 version is possible but requires some particular actions in the security policies. A document is available in the document base on [MyStormshield](#) to help you.



# Stormshield Endpoint Security 7.2.14 fixes

## Agent fixes

Support reference 11508

### ICMP filtering removed from network applicative rules

In the **Network** column of the applicative rules panel in the security policy, the parameter **By default** applied to ICMP, TCP and UDP protocols whereas it was not possible to write network rules about ICMP protocol in this window. Now, network applicative rules no longer apply to ICMP protocol.

Support reference 11639 (#CF 87512)

### Dealing with slashes ("/) in LDAP organizational units (OU)

When the complete Distinguished Name (DN) of a host included at least one slash (for example with an OU containing itself a slash), the agent installed on this machine could not retrieve a policy linked to this OU. Now, the agent is able to retrieve policies in this case.

Support reference 11578

### New format for auto-protection logs

In order to be more explicit, logs about SES auto-protection have changed format.

Support reference 11536 (#CF 87441 - 150724PW)

### Slow application of policies after a network modification

When the SES server was unavailable, applying conditional policies could take up to 20 seconds. Some improvements have been made in order to change policy as fast as possible, even if the SES server is unavailable. Latency can still occur with the display of policy application logs. This issue will be fixed in a future release.

Support reference 11811 (#CF 85877)

### TCP connections blocked when using the FastOpen option

In the **Network security control** tab in the security policy, when the parameter **TCP integrity check** was enabled, the firewall blocked TCP connections using the TCP FastOpen option. Now, this option is detected and is no longer blocked.

Support reference 11846 and 11920 (#CF 87614)

### Using the stopagent and ssusrlog tools with the Windows local System account

It is now possible to execute the SES stopagent and ssusrlog tools with the local System account. This account is used to execute processes in SES scripts, among other usages.

Support reference 150843PW

### Dysfunction of the agent's interface after an update

After updating the agent, in some cases, the agent's interface could indicate that it was disabled as long as the workstation did not restart. The agent worked properly however. The interface only did not answer.



## Server fix

Support reference 11531

### SES server version number in the Windows Control Panel

When updating the SES server, the version number displayed in the **Programs and features** menu in the Windows **Control Panel** did not switch to the latest version installed. This issue has been fixed.

## Console fix

Support reference 11816

### SES policies export

In the administration console, only the security policy is exported in SCZP format. This format is an archive containing the file of the security policy in SCEP format as well as the related application identifiers. All the other types of policies are exported directly in the SCEP format.

From the version 7.2.11, all policies were exported in SCZP format. To import a policy other than a security policy in the versions 7.2.11 to 7.2.13, it was necessary to extract first the SCEP file from the SCZP archive.

From version 7.2.14, the problem has been fixed: all policies except security policies are exported in SCEP format.

Support reference 11716 (#CF 87511)

### Traffic between the administration console and databases

The traffic between the console and databases could be very important when there were many agents and/or logs bases. The traffic has been optimized in order to reduce the volume of exchanged data. This issue mainly impacted environments with several logs databases.



## Stormshield Endpoint Security 7.2.13 new features

### **Avira antivirus update**

The version of Avira now deployed on SES 7.2.13 agents is Avira Antivirus Pro 2015. If you have an environment of agents using the Antivirus option, you should start by uninstalling the previous version of Avira (Avira Professional Security 2013) before proceeding with the upgrade of your agents. The new version of Avira will be automatically deployed when agents are upgraded.

The procedure to follow is explained in the *Stormshield Endpoint Security Administration guide*, under the section *Migrating to Avira 2015*.

The Antivirus option is now compatible with Microsoft Windows 10.

### **Synchronizing full disk encryption recovery data**

During an SES upgrade from a version earlier than 7.2.06, full disk encryption recovery data will now be verified and repaired where necessary. The agent will initiate this verification procedure during its upgrade. As such, recovery data between the agent and SES server will not be desynchronized due to errors while handling the database or network instability.



# Stormshield Endpoint Security 7.2.13 fixes

## Agent fixes

Support reference 11372

### Display of logs relating to the application of policies and configurations

Whenever the agent applied a new policy or configuration, the application log would appear several times consecutively in the event log window. This issue has been fixed.

Support reference 11080 (#CF 86971)

### Problems connecting to the server via a direct route

Whenever a direct route to the SES server was established in the network configuration, the SES agent would be unable to connect to the server. This problem arose with certain VPNs and policies could not be applied. Now, if a route can reach the server, the agent will no longer lose its connection.

Support reference 11444 (#CF 87417 and 87432)

### Blue screen whenever the *Ntdll.dll* file was compressed

On Microsoft Windows 10 and Windows 8.1, executable files on the operating system, including the *Ntdll.dll* file, can be compressed with the command `compact /compactos:always`. Whenever the SES agent was being installed on a machine on which this command had been run, or whenever this command was run after the agent was installed, a blue screen would appear whenever the machine started up. This issue has been fixed.

Support reference 11551 (#CF 87486)

### Random blue screen during kernel event monitoring

Certain verifications performed as part of kernel event monitoring in the security policy could randomly cause a blue screen. These actions have been reviewed and corrected.

Support reference 11350 (#CF 87349)

### Incompatibility of the SES agent with certain Intel graphics drivers

On Microsoft Windows XP or 2003 Server, a blue screen could occur whenever the SES agents and certain Intel graphics drivers were installed on the same workstation. This issue has been fixed.

Support reference 11645 (#CF 87509)

### Error with the built-in test on the active network interface in scripts

Ever since version 7.2.10, an error would occur during network tests on an active interface and would prevent the test from running. This issue has been fixed.

## Console fixes

Support reference 11079

### Incorrect permissions on the console

In some cases, certain features on the console (script duplication, for example) could not be accessed. This issue has been fixed.



Support reference 11365 (#CF 87355)

**Problems displaying the application rules of the security policy**

In the application rules applied to access to the registry database, whenever a row was added, if it was the last one displayed, a scroll bar would appear in the middle of the window. This issue has been fixed.

Support reference 10666

**System behavior settings in the security policy**

In the *System behavior* tab of the security policy, the "Low" setting on certain parameters meant that nothing would be blocked or protected. The "Low" setting has been renamed "Disabled".

Support reference 9955

**Lists and tables**

The "." edit button in lists and tables was not visible enough (right aligned) and was not adapted to drop-down lists. The button now appears whenever you roll the mouse over a row and how it appears corresponds to the action it performs (drop-down list or edit window).

Support reference 11440

**New actions added in Device logs**

In the log editor, the actions VOLUME\_MOUNT, VOLUME\_READWRITE, FILE\_CREATE, FILE\_READ and FILE\_WRITE have been added to Device logs.

Support reference 11512 (#CF 87443)

**Malfunction of the database installation wizard**

Whenever a Stormshield version 6.0.XX is migrated with a database restoration to an SES 7.2.XX version, the database installation wizard would suddenly stop running. This issue has been fixed.

Support reference 9171

**Rule groups enabled in the security policy**

Whenever a rule group was disabled in the security policy, the rules would not display a "Disabled" status. All rules in the group now display the "Disabled" status.

Support reference 11219

**Modification of a rule group's name when it is copied**

Whenever a rule group was copied from one security policy to another, its name would occasionally be truncated. This issue has been fixed.

Support reference 11541

**Correction of the "Invalid file" error when importing a policy**

During the import of a policy, whenever the encoding was not UTF-8, an error would stop the action. Imports now take place correctly, but in the event of unknown encoding, certain characters may be replaced.

Support reference 11216

**Deleting rule groups**

In a security policy in edit mode, rule groups concerning removable devices or the network firewall can now be deleted using the "Del" button on the keyboard.

Support reference 11381

**Enhancement of the "Restore" action in scripts**

The **Restore** action (in a policy/configuration) offered in scripts has been enhanced and a **Reevaluate** action has been added. For more information on both of these options, please refer



to the section *Scripts* in the *Administration guide*.

## Server fix

Support reference 9035 (#CF 86831)

### **Missing privileges when a server is deleted**

Despite a user possessing the permissions needed for deleting an SES server, it would not actually be deleted. The cause of this issue was an error in the assignment of privileges on the SQL server during installation. Servers are now properly deleted if the user has the necessary privileges.





# Stormshield Endpoint Security 7.2.12 resolved vulnerabilities

---

Support references 11522, 11524 and 11526

## OpenSSL upgraded to version 1.0.2j

Vulnerabilities ([CVE-2016-6304](#), [CVE-2016-6306](#) and [CVE-2016-2177](#)) have been fixed by upgrading the OpenSSL cryptographic library to version 1.0.2j. Details on the vulnerability CVE-2016-6304 (OCSP Status Request extension unbounded memory growth) can be found on our website <https://advisories.stormshield.eu/>.



## Stormshield Endpoint Security 7.2.11 new features

### **New "Update Agent" challenge**

The **Update Agent** challenge now makes it possible to update an SES agent without restricting it to the version defined in the agent's static configuration. It will take effect on versions of the agent higher than 7.2.11.

### **Moving rules in agent groups**

A new button in the IP configuration and Netbios toolbar for agent groups in the internal directory now allows moving entries from one group to another while it is being edited.

### **Modification of application identifiers for extensions and trusted applications**

One or several application identifiers may be added or deleted simultaneously from several rules on extensions and trusted applications.

### **User creation window in the console**

A full dialog box now allows adding new SQL or Active Directory users from the console. It allows specifying certain information about the user (login, password, role, environment) and configuring the console for this new user (initialized by default as the current user's configuration).

### **Support for MS SQL Server 2014 and MS SQL Server 2016**

SES now supports the MS SQL Server 2014 and MS SQL Server 2016 versions.

### **New log for the "Run process" script test when the program cannot be created**

When adding an integrated "Run process" test in a script, the log created in the *skybatch.sro* file will now take on the value [CHECK] [ERROR] when the program cannot be run (typo or nonexistent command for example).



# Stormshield Endpoint Security 7.2.11 fixes

## Agent fixes

Support reference 11163 (#CF 87346)

### Slow processes on 64-bit operating systems

On 64-bit operating systems, 32-bit processes would use 100% of a processor's (or a core's) resources. This issue would arise whenever buffer overflow protection was enabled. As a result, processes would slow down significantly and seem to hang. This problem has been fixed.

Support reference 11020

### Rule application scope on trusted applications in the security policy

The extension of the scope of an application's trusted rule (which can be selected in the **Application scope** column) did not function for the **Run on a removable device** trusted domain: when the rule's application scope was defined on **Application and children**, a notification window would continue to appear, asking for confirmation to run a process on the removable device. The extension of the rule's scope now functions for this domain.

For more information on the scope of a security rule's application, please refer to the *Stormshield Endpoint Security Administration guide*.

Support reference 11203 (#CF 87173)

### Blocking of traffic linked to port scan detection

In some cases, the SES agent would block ICMP frames (type 3, code 3) after it has detected a port scan with IDS set to low. Such traffic will now be blocked only with an IDS level set to high or critical.

Support reference 11086 and 11087 (#CF 87246)

### Logs regarding extension rules in the security policy

System logs relating to extension rules defined in the security policy with a Warning status were no longer generated. This problem has been fixed.

Likewise, such logs were not generated if an application identifier had not been entered in the rule. From now on, logs will be generated even in the absence of an identifier.

Support reference 11185

### Aggregation of trusted rules

When several trusted rules applied to the same identifier, only the first trusted rule would be taken into account. All trusted rules will now be applied and aggregated.

Support reference 11370 (#CF 87350/87373/150043CW/150079CW)

### Correction of a BSoD on 64-bit Microsoft Windows operating systems

A BSoD would occasionally appear in version 7.2.10 on 64-bit Microsoft Windows operating systems when certain applications like GoToMeeting are used, requiring tools such as a webcam and USB microphone. This problem has been fixed.

Support reference 11127 (#CF 87200 and 86916)

### Performance enhancement

SES performance has been enhanced across all versions of Windows, in particular for 64-bit versions of Windows when RCP protection has been enabled.



## Server fix

Support reference 11035 (#CF 87237)

### Server updates

When the SES server's installation directory did not have a short Windows name, or when short Windows names were disabled, the update of the server would fail. Updates now function even when short Windows names are absent or disabled.

## Console fixes

Support reference 10595

### Removal of the "read-only" option from application rules

The **Read only** option, which prevented content on an executable file from being modified, has been removed from the application rule panel in the security policy.

Support reference 11186

### Security policy exports

When exporting a security policy, by default only the policy itself would be exported. From now on, the default option is to export the policy with its resources.

Support reference 10860 (#CF 87185 and 87227)

### Display of Active Directory groups in a script

The window for selecting groups or users in script resources did not display all the items present. This window has been replaced with a search window allowing searched items to be filtered.

Support reference 11241 (#CF 87044)

### Display of the agent's icon in Active Directory mode

In Active Directory view, computers on which agents have been installed display a specific icon. In some cases, the icon was not displayed. This problem has been fixed.

Support reference 11256 (#CF 86923)

### Sequence of rules when importing security policies

When security policies from version 6.0 of SES were imported, application control rules (application rules, extensions and trusted applications) would lose their position. Positions are now kept during imports.

Support reference 8583

### Display mode for kernel components

In the *System behavior* tab in the security policy, the **Kernel components** item would appear in red when protection was disabled and in green when it was enabled.

When protection is disabled, it will now be grayed out. A tool tip will indicate that protection has been disabled and the item can no longer be selected.

If protection has been enabled, the item will be displayed like a normal item.

Support reference 9553

### Privileges on CD/DVD/Blu-Ray extension rules

In the *Device control* tab in the security policy, when extension rules were copied and pasted or imported into a CD/DVD/Blu-Ray group, the possible privileges shown in the list were incorrect. The possible privileges now take into account the type of device.



Support reference 11265

**Exception when shutting down the console**

An exception could occur during the shutdown of the console when the dashboard was displayed. This problem has been fixed.

Support reference 8824

**Improvements to the script editor**

When script policies or script resources were being edited, the ":" character would be replaced with a "::" in the display of the script tree. This problem has been fixed.

Support reference 10398

**Pop-up menu for logs in Test mode**

The log monitoring pop-up (right-click) menu would not appear whenever logs reported in the console came from a rule in Test mode.

Now, logs reported by rules in Test mode can be copied and sorted using the pop-up menu.

Support reference 7248

**Short messages for ARP networks changed**

Short messages for ARP logs would display content for PORTDST and PORTSRC variables, even though ports are irrelevant in an ARP attack. This problem has been fixed.

Support reference 10854

**ssuslog.exe**

Whenever logs are successfully sent to the server via ssuslog.exe, error messages will no longer be displayed and a confirmation message will appear. Furthermore, the executable file is now able to manage incorrect parameters.

Support reference 11162

**Domains in an Active Directory changed**

A console would take some time to open if it ran in Active Directory mode. Several enhancements have been made when changing domains in an Active Directory forest. For example, sub-domains now load in the background.

Support reference 11250

**Standardized LDAP searches in the console**

Several features in the console require running LDAP queries: script resources, Active Directory searches, user searches for device enrollment, addition of users to the console with Windows authentication. When users entered a character string, in some cases, the console would automatically add the "\*" character before and after the string. This character would include items that contained the search string instead of performing an exact search, thereby significantly increasing the search duration.

Searches are now conducted on the exact string. The "\*" character will now need to be added manually where necessary.

In addition, user searches can now be performed on more attributes: the Windows connection name or the DNS name.



# Stormshield Endpoint Security 7.2.10 new features

## Support for Windows 10 CBB

Stormshield Endpoint Security now supports Microsoft Windows 10 CBB operating systems. All of the Stormshield Endpoint Security security features and devices are available on these new platforms.

### WARNING

Stormshield Endpoint Security does not apply any protection for processes that are part of the WSL (Windows Subsystem for Linux) feature available with the Windows 10 update released in July 2016. These processes could therefore compromise the integrity of the Stormshield Endpoint Security product as well as the workstation if they were misused. You are therefore advised to enable this feature only when needed and on occasion.

## Display of the serial numbers of new licenses in the SES console

For licenses that have serial numbers, they are now displayed in the license manager and in the license update menu.

## Shared servers

A single SES server can now manage an internal directory and an Active Directory at the same time. The product must be installed beforehand in Active Directory mode. In the event an agent belongs to two directories, a new parameter allows managing the priority of directories (**Environment** menu, *Parameters* tab)

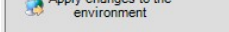
## Protection against privilege escalation

The SES agent now protects workstations from spoofing and the fraudulent modification of a process's security context. This new mechanism is integrated into protection against privilege escalation. Furthermore, the SES console now allows choosing between three levels of protection against privilege escalation: Disabled/High/Critical. If the option was enabled before the update, the Critical level will be selected in 7.2.10.

For details on each level, please refer to Chapter 9 of the *Administration guide 7.2*, section *System Behavior*.

## Synchronizing environments

In the SES console, the button formerly named **Synchronize**  which allowed deploying the server's policies and configurations to SES agents has been replaced with a new button called

**Apply changes to the environment**  in order to be clearer and more visible.

## Adding actions when events are detected

It is now possible to set up actions to be run whenever a particular event occurs on an SES agent, thanks to scripts associated with logs in the SES console's Log Manager. As soon as an agent reports a specified type of log, the associated script will be run.

## Console user comfort

In the SES console, the editable area of a field is now white and framed in blue to enhance visibility.

**Priority of policies applied by script**

The agent's dynamic configuration policies and security policies configured in scripts will now be applied in a new order according to their application source. The new order of application is as follows, from the highest to lowest priority: challenges (in the agent's static configuration), actions upon detection (in the Log Manager), scripts and policies linked (in an environment).

**Encryption policy management**

In the SES console, deleting an encryption policy applied to agents could accidentally decrypt workstations. To prevent this from happening, agents now keep their current encryption policies until the explicit application of a new policy. Therefore, in order to decrypt a machine that uses full disk encryption, an encryption policy on which full disk encryption has been disabled needs to be applied to it.

**New parameter for trusted applications**

In the SES console, for a security policy's trusted applications, a new field named Application scope now allows choosing whether to extend trust to the application only or to the application and its children. This parameter is accessible only in advanced mode.



# Stormshield Endpoint Security 7.2.10 fixes

## Agent fixes

Support reference 10546

### Compatibility of the SES agent with the Stormshield Data Security for Cloud & Mobility product

Whenever an SES agent was uninstalled from a workstation that was also equipped with Stormshield Data Security for Cloud & Mobility, the latter would become unstable. This problem has been fixed.

Support reference 10756 (#CF 87031)

### Uninstalling the SES agent in safe mode with networking

The system would stop running (blue screen) whenever the SES agent was uninstalled in safe mode with networking. This problem has been fixed.

Support reference 10495 (#CF 86854)

### Compatibility of the SES agent with Sophos antivirus

Whenever the SES agent was installed on the same workstation as Sophos, certain applications would stop running. This random occurrence was caused by competing access between Stormshield Endpoint Security and Sophos during the installation of protection. This problem has been fixed.

Support reference 10635

### Automatic validation of temporary web access

Whenever you create a shortcut on the user's desktop to request temporary web access ("/GrantWebAccess" argument added in the target of the shortcut to the executable file ssmon.exe), you can now add the option "/NoConfirm" in order to disable the web access confirmation window. Access will then be effective immediately.

Support reference 10458

### False positives on the protection (read only) of registry keys

Whenever a registry key was in read-only access in the application rules in the SES console, a log would be generated for each access to the key on the workstation. Logs will now be generated only for access attempts in write mode.

Support reference 10594

### Deleting implicit protection from renaming

Whenever a path-based application identifier was linked to an application rule, a file corresponding to the application identifier could no longer be renamed or deleted. This problem has been fixed.

Support references 10701 and 10862

### Compatibility with the Firefox browser in versions 47 and higher

The Firefox browser in versions 47 and higher did not run correctly on workstations equipped with an SES agent. This problem has been fixed.

Support reference 10863

### Accessing a value of a protected registry key

Whenever a program attempted to modify the "UpperFilters" value of the registry key "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E967-E325-11CE-BFC1-





08002BE10318}", access was denied. It is now possible to write values compatible with the operation of SES.

Support reference 10877 (#CF 87170)

### **Corruption of the main.srx file on the workstation**

On a workstation equipped with the SES agent, whenever the *main.srx* file was corrupted, invalid or nonexistent, the agent would be unable to apply current policies. This problem has been fixed. If an *srx* file from the Batch folder is corrupted, invalid or nonexistent, the agent will download all policies again.

Support reference 10724

### **Libxml2 upgraded to version 2.9.4**

The libxml2 version that Stormshield Endpoint Security uses to manage XML files has been upgraded to version 2.9.4. Version 2.9.3 contained security flaws.

## **Server fixes**

Support references 10740 and 10345

### **Agent/server connection time**

Communication between agents and the SES server has been improved, thereby cutting down connection time. Communication was indeed slow whenever small amounts of data were exchanged. The server could also become saturated as agents that logged off and on again could have been counted several times.

Support reference 10782 (#CF 86613)

### **Server connection management**

Whenever many SES agents logged on simultaneously to the server, it would not succeed in processing all connection requests. Agents would then no longer be able to log on and the server would be unavailable. This problem has been fixed.

Support reference 10705 (#CF 87063)

### **Unavailable HTTP web server**

Depending on the software environment available on the workstation that hosted the SES server, version 2.4 of the Apache web server provided from SES version 7.2.07 upwards could encounter instability and deny almost all incoming connections.

## **Console fixes**

Support references 9062 and 10763

### **Selecting the language of the console during installation**

The first time the SES console was run, the default language was English even though a different language was chosen during the installation of the product (French, Spanish, Portuguese or German). This problem has been fixed.

Support reference 10698

### **Go to rule menu in logs**

In the SES console's log panel, the **Go to rule** pop-up menu accessible by right-clicking on a particular log could cease to run in automatic refresh mode. This problem has been fixed.



Support reference 10672

**Copying a group in the security policy**

In the *Device control* and *Network security control* tabs of security policies in the SES console, the group copying function no longer worked. This problem has been fixed.

Support reference 10400

**Copy cell menu in logs**

In the SES console's log panel, the **Copy cell** pop-up menu accessible by right-clicking on a particular log did not work correctly. This problem has been fixed.

Support reference 10011

**Display of the version of a 7.1 agent's operating system in a 7.2 console**

In the Agent Monitoring panel of an SES 7.2 console, the version of the operating system displayed for each agent could be incorrect if the version of the agent was lower than 7.2. This problem has been fixed.

Support reference 10636

**Using filters in logs**

An error would appear whenever too many simple filters were selected in the SES console's log panel. The size of the filter display area will now be restricted and a scroll bar will appear if necessary.

Support reference 10537

**Help panel for date format**

In the SES console's control panel, whenever you enter a date display format, help at the bottom of the panel will now translate the value of the field to a date. For example, "G" equals "15/06/2009 13:45:30 PM".

Support reference 10812

**Built-in test on an Active Directory group**

While setting up a built-in test on an Active Directory group in the SES console, the domain name could no longer be entered in the test's properties. This problem has been fixed.

Support reference 10202

**Priority of logs in the Log Manager**

Changes to the priority of logs in the SES console's Log Manager were not applied whenever a filter on the display of logs was enabled. This problem has been fixed. Changes to priority only took into account logs displayed at the moment.

Support reference 10896

**Reorganization of the Role Manager**

The permissions panel in the Role Manager of the SES console has been reworked. Permissions are now sorted in the same order as the console's categories, and the permissions "Create and modify certificates" and "Create and modify security policies" have been merged.



# Stormshield Endpoint Security 7.2.09 fixes

## Agent fixes

Support reference 10805 (#CF 87125)

### **Some Windows updates could not be installed on the workstation**

The SES agent could prevent Windows updates from being installed if the updates needed to access sensitive keys of the registry base. This problem is fixed.

Support reference 10803

### **Compatibility with TheGreenBow VPN Client**

The SES firewall and TheGreenBow VPN Client could be incompatible when the option of the VPN client **Disable Split Tunneling** was enabled. This problem is fixed.



# Stormshield Endpoint Security 7.2.08 fixes

---

## Server fix

Support reference #CF 87063

### **HTTP Web server unavailable**

According to the software environment available on the workstation hosting the SES server, the version 2.4 of the Apache web server provided since SES 7.2.07 could deny almost all incoming connections. This problem is fixed.



# Stormshield Endpoint Security 7.2.08 updates

Support reference 10685

## OpenSSL update

A vulnerability ([CVE-2016-2107](#) - Attack against an AES CBC session implemented with AES-NI) has been fixed by upgrading the OpenSSL cryptographic library to version 1.0.2h. Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.



# Stormshield Endpoint Security 7.2.07 new features

## Support for Windows 10 LTSC

Stormshield Endpoint Security now supports Microsoft Windows 10 LTSC operating systems. All of the Stormshield Endpoint Security security features and devices are available on these new platforms.

## Selecting logs to be sent over an SMTP or Syslog server

Previously, all logs were sent either over an SMTP server or a Syslog server. You can now choose to use both server types simultaneously and select the types of logs to be sent over either server. This option has to be configured in the agent's dynamic configuration policy and in the log manager.

### WARNING

After upgrading your console to version 7.2.07, check the **Enable self-protection logs** parameter in the agents' dynamic configuration. The newly separate management of SMTP and Syslog servers may modify your settings. The recommended configuration is "fpdIm" (all options disabled). For more information, refer to the *7.2 Administration guide*.

## Notification of the imminent expiry of the full disk encryption password

Warning messages will now appear on the user's workstation 20 days, 10 days, 5 days and the day before the expiry of his encryption password. These messages will allow the user to directly modify his password and be warned the next time it expires.

## Shortcut for temporary web access

A shortcut can now be created on the user's desktop to quickly request temporary access to the web. You will need to create a shortcut to the executable file of the agent's graphical interface `ssmon.exe` on the desktop, then add the argument `"/GrantWebAccess"` as the target of the shortcut. This shortcut allows avoiding from going through the Stormshield Endpoint Security menu accessible from the system's status bar. For more information, refer to the *7.2 Administration guide*.

## Search field in the Agent Monitoring panel

A search field in the **Agent Monitoring** panel now allows finding agents more easily. Searches automatically cover the **Machine name, AD name, IP address**, etc columns.

## Panel that allows viewing server assignment locations

A sub-panel has been added to the **Stormshield Endpoint Security Servers** panel. During the selection of a server, all locations at which the selected server has been assigned will be listed.

## Parameters **Minimum agent version allowed** and **Maximum agent version allowed**

Two parameters in the configuration of the server now allow servers to block communication with agents in versions different from theirs. For more information, refer to the *7.2 Administration guide*.



# Stormshield Endpoint Security 7.2.07 fixes

## Agent fixes

Support reference 9661

### HoneyPot protection in Warning mode

Whenever Warning mode was enabled on the SES agent, logs indicating that HPP protection had been blocked would not appear. This problem is fixed.

Support reference 9836 (#CF 86559)

### SES agent execution error

Under certain circumstances, the corruption of the file *Sigs.srn* could cause an error during the execution of the SES agent (*framework.exe*). This problem is fixed. A `SIG_ERROR` system log will be recorded in such cases.

Support reference 9127

### Protection of SES files in Warning and StandBy mode

SES files (*\*.sra, \*.srn, \*.sro, \*.srx, \*.srxml*) are now protected by their extensions in Warning and StandBy modes. Protection is effective under the same conditions as in Normal mode, i.e., as long as the agent is enabled and 20 seconds after it has been disabled.

Support reference 8903

### Generating logs when the first connection to the Active Directory server fails

Whenever an SES agent in Active Directory mode connects for the first time to the AD server and the connection fails, a log will now be generated.

Support reference 8905

### Applying policies when the SES server cannot be contacted

When the SES agent is logged off from the server, the conditions for applying policies in a group of agents will now be evaluated during each attempt to reconnect to the server in order to find out which policies should be applied.

Support reference 9970

### Deleting the *sr* footprint file after the revocation of a USB key

Whenever a USB key was revoked from a management console installed on a workstation equipped with an SES agent, the file *sr footprint* would not be deleted. This problem is fixed. After a key is revoked, it will now be ejected as well by the console.

Furthermore, a warning will now appear when the console does not detect the USB key during its revocation.

Support reference 10118 (#CF 86724)

### Compatibility with ESET

ESET Endpoint Antivirus could not be installed on a workstation equipped with an SES Professional Edition agent. This problem is fixed.

Support reference 10190 (#CF 86466)

### Compatibility with TheGreenBow VPN client

TheGreenBow VPN client (version 5.22 and upwards) did not run correctly when the SES Firewall feature was enabled on the agent. This problem is fixed.



Support reference 10324 (#CF 86833 and 86856)

### **Connecting to a StormShield 6.0 server during a partial migration**

During a partial migration from version 6.0 to version 7.2, 7.2 agents may occasionally continue to log on to the former 6.0 server. This problem is fixed.

Support references 10100 and 10103

### **SES agent freezing when the network connection is unstable**

Whenever the connection between the agent and SES server was unstable due to the loss of network packets, latency, etc., the agent (framework.exe) would stop running. This problem is fixed.

## Server fixes

Support reference 10346

### **Agents unable to connect to the SES server**

Agents could no longer communicate with the SES server whenever it could no longer communicate with its own logs and monitoring database server. This problem is fixed.

Support reference 10505

### **SES agents logging on to the server without synchronization**

After installing SES server and agents, the server may occasionally stop working whenever an agent logged on whereas the synchronization never had been launched from the management console. This problem is fixed.

## Console fixes

Support reference 10137 (#CF 86753)

### **Inability to synchronize SES servers from the console**

The synchronization of SES servers would fail when the administration console took too long to retrieve configuration information from the database and generate the files to be sent to servers. This problem is fixed.

Support reference 9894 (#CF 86233)

### **Managing disjoint namespaces to add users**

It is now possible to add Active Directory users whose DNS name on the domain and NetBIOS name on the domain are different (disjoint namespaces) to users of the console.

Support reference 5252

### **Filing script resources in alphabetical order**

Tests and actions in script resources are now arranged in alphabetical order and no longer in the order of their creation.

Support reference 8394

### **Configurations and policies not retrieved by agents defined by a NetBios name**

Agents defined by a NetBios name containing lowercase letters could not retrieve configurations and policies on the SES server. This situation only arose in internal directory mode with a configuration of agent groups by NetBios name. This problem is fixed.





Support reference 10323

**Inability to start the management console with an expired license**

Only in internal directory mode, whenever the SES license reached its expiry date, an error message would appear and the administration console would not start. This problem is fixed.

Support reference 10354 (#CF 86759)

**Slowdown when loading the management console's dashboard**

The system would slow down when loading the dashboard. The patch provided enhances the console's performance without resolving the issue on very large databases.



## Stormshield Endpoint Security 7.2.07 updates

Support reference 9947

### Variables added in logs

The variables %CERT%, %MD5% and %SHA1% have been added to System logs in order to provide more details about the source. Refer to the *Administration guide 7.2* to look up examples of the use of the log manager.

Support reference 10150

### OpenSSL update

OpenSSL has been updated to version 1.0.2g.



## Stormshield Endpoint Security 7.2.06 new features

### Warning

The 7.2.06 version is currently being through the Common Criteria certification process and has not been publicly released yet.

### **Random generation of encryption keys**

A new step has been added in the Stormshield Endpoint Security server installation procedure. The user must randomly move the mouse in order to increase random for the generation of encryption keys for full disk encryption.



# Stormshield Endpoint Security 7.2.06 fixes

## Agent fixes

Support reference 9286

### Logs sent from the agent to the server during computer shutdown

When a computer was shutting down, some logs concerning events in progress could not be sent to the server. This problem has been fixed: during shutdown, all logs are now stored in a file which will be sent to the server next time the computer starts.

Support references 9285, 9708

### Full disk encryption: issue with the creation of the guest account on the agent

It was not possible to create the GUEST account from the SES agent if the password of the USER and ADMIN encryption accounts had been changed. Also, it was not possible to create the GUEST account from the USER account if its validity was only one hour. The possibility to create the GUEST account now only relies on the rights granted in the encryption policy.

Support reference 9543

### Error during data recovery

After recovering data from an encrypted computer thanks to the recovery media, the workstation could become unusable. This issue could occur if the option **Partition encryption** in the encryption policy had been changed over time. Data recovery through the media is now fully functional and the disk is properly decrypted.

Support reference 9883

### Improvement of the encryption password expiration window

The renewal request for the encryption password after it has expired is now more explicit for the user. The **Cancel** button in this window has also been grayed out in order to force the user to change the password.

Support references 8938, 9366, 9222, 9224, 9367, 9654, 9223

### New logs about full disk encryption

The following software logs concerning full disk encryption have been added:

- Encrypted partitions: when full encryption or decryption of the disk is completed, a log indicates the partitions which have been encrypted or decrypted.
- Authentication failures and successes when a workstation which disk is encrypted starts.
- Creation/deletion of a guest account: a log reports the type of the encryption account (user, administrator or guest) connected when the guest account was created or deleted.
- Postponement of full disk encryption
- Modification of the user password with the recovery media.
- Update of recovery elements
- Disk decryption: a log reports that disk decryption through the recovery media is completed.



## Server fixes

Support reference 9688

### Automatic update of the Apache configuration

When installing a new version of the SES server, Apache configuration files were not generated again and this prevented the Apache server from properly starting. This had to be done manually with the *skyapache.exe* tool. Apache configuration files will be automatically generated the next time the SES server 7.2.06 is updated to a higher version.

Support reference 8556

### Certificate download web page

The certificate download web page was accessible through HTTPS (secure) and HTTP (not secure). Now the secure access only is available.

Support reference 9601

### New log reporting that policies have been sent from the server to the agents

In the *output.sro* file on the server, a new log now reports that the SES server has just sent configurations and policies to an agent.

## Console fix:

Support reference 9599

### New log reporting the generation of recovery elements

A new log now reports that recovery elements have been generated by the server for an agent. This log displays by default in the Software logs of the console.



# Stormshield Endpoint Security 7.2.06 updates

Support references 8556, 9857, 9895

## OpenSSL and Apache update

The OpenSSL component has been updated to version 1.0.2e and the Apache component has been updated to version 2.4.18.

The configuration of the Apache server is not updated when the SES server is updated from a version previous to 7.2.06. You need to manually apply updates by executing the command «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*. The SES server must be restarted to take modifications into account.

Moreover it is no longer possible to use Internet Explorer 8 on Windows XP to download a certificate ([https://ip\\_du\\_serveur/ssl/cgi](https://ip_du_serveur/ssl/cgi)). A more up-to-date browser must be used to access this page.

Support reference 8889

## Improvement of the security of recovery data

The recovery data for full disk encryption are now authenticated with the algorithm PBKDF2-HMAC-SHA512 and encrypted with a key generated with PBKDF2-HMAC-SHA512.

Support reference 8504

## Cipher suites

The SES server now supports the cipher suites ECDHE-RSA-AES256-SHA and ECDHE-RSA-AES256-SHA384.

Support reference 9626

## Improvement of the security of authentication on an encrypted disk

The authentication protocol now uses the algorithm PBKDF2 in order to improve the security of the authentication step. When updating SES from a version not using this protocol, the USER password will have to be changed in order to implement this new process. The disk is not decrypted during the update process.



## Stormshield Endpoint Security 7.2.05 new features

---

### **Execution tracing**

Traces can now be recorded when issues are encountered while using the SES agent, providing Stormshield Endpoint Security support with useful information for analyzing issues via the Trace manager.

Refer to the *Administration Guide* for more details about the Trace manager.



# Stormshield Endpoint Security 7.2.05 fixes

## Agent fixes

Support reference 9420

### Repetitive request to reboot

During the installation of a Secure Edition agent, rebooting is mandatory. After rebooting, the agent would repeatedly offer to reboot the workstation. This problem has been fixed.

Support reference 8979

### Network filtering with several IP addresses

In a configuration with a network interface bearing several IPv4 addresses, network filtering may fail to function correctly. This problem is fixed.

Support reference 6010

### Date/time in logs sent via Syslog

External logs sent via Syslog contained a date and time (timestamp) corresponding to the date and time they were sent by the SES server. They now correspond to the date and time the agent generated the log.

Support reference 9097

### Improved self-protection of the agent in warning mode

The self-protection of the agent's registry keys when the agent is in warning mode has been improved.

Support reference 9580

### Blue screen when renaming a registry key in warning mode

Whenever the agent was in warning mode, a blue screen could appear when registry keys were being renamed. This problem has been fixed.

Support reference 8827

### Description of the *ssmon.exe* application identifier changed

The description of the *ssmon.exe* application identifier was "Stormshield Monitor". It has been changed to "Stormshield Endpoint Monitor".

Support reference 9016

### Removal of LDAP latencies before the agent applies policies

When the agent downloads policies, it applies them directly then updates its LDAP information. The latency of the connection to the LDAP server is reduced as such.

Support reference 9571 (#CF 86480)

### Opening RDP connections on Windows XP and Windows Server 2003

Enabling certain types of buffer overflow protection prevented the workstation from being controlled remotely with the Microsoft tool (*mstsc.exe*) on Windows XP and Windows Server 2003. This problem has been fixed.





## Server fix

Support reference 9329 (#CF 86052)

### Wrong version of the server in the Programs and Features panel after an update

The version of the server in the Programs and Features panel is now correct after an update.

## Console fixes

Support reference 9329 (#CF 86052)

### Wrong version of the console in the Programs and Features panel after an update

The version of the console in the Programs and Features panel is now correct after an update.

Support reference 9314

### Default value of the encryption key size modified

When creating a new encryption policy, the size of the encryption key is now 256 by default instead of the previous 128.

Support reference 9293

### Display of modifications to policies in the event viewer

In the console's event viewer, whenever a policy was modified, only the icon would appear in the columns of modified values. The text accompanying the icon was missing.

Whenever a modification to a policy is validated, the icon and text relating to this icon will now appear correctly in the event viewer.

Support reference 9427

### Editing a role in the console

When a role is being edited in the console, if the role was validated without any changes being made or by quitting the console, an exception would occur. This problem has been fixed.

Support reference 9237

### Application of changes to information on agent groups in the internal directory after validation

The first validation did not apply the changes made. The validation and synchronization of information with the database have been fixed.

Support reference 8962

### Installation and update of the console on a workstation with an SES agent

An error occurred during the installation, update and uninstallation of a console whenever there was an agent on the workstation. This problem has been fixed.

Support reference 9199

### Button for selecting an Active Directory element in script resources

In script resources, Active Directory users or groups could no longer be selected when a "Domain" built-in test was added. This problem has been fixed.

Support reference 9302

### Wrong SRService error logs

During the installation of an agent, SRService error logs were generated when the machine rebooted. These errors appeared even when the installation took place correctly and no errors were detected. These error logs have been deleted and no longer appear when the agent has been successfully installed.



Support reference 9465

**Error message during the update of the console used by several Windows sessions**

Whenever several users logged on to the console on the same workstation, the console could not be updated. An error message would be generated without specifying that the user had to check whether other users were logged on to the console. The error message will now ask the user to check whether other Windows sessions are using the console or whether the database installer is running on the workstation.

Support reference 9484

**Agent configuration graph**

The agent configuration graph in the dashboard did not take into account the trend scale. This problem has been fixed.

Support reference 9577

**Selection of the value for the active network interface in script resources**

Ever since version 7.2, certain graphics editors were no longer available in the script resources. These editors have been reintegrated.

Support reference 9582

**Installation of SES in an internal directory with an expired license**

During the installation of an SES environment, if the evaluation license used has expired, the installation would fail without stating reasons. This problem has been fixed.

Support reference 9585

**Translation error in the pop-up menu Show logs in the AD**

In a console in Spanish or Portuguese, the pop-up menu that allows displaying logs from a selected AD object would display the same option four times without indicating the type of log to select. This problem has been fixed.

Support reference 8753

**Selecting the node in scripts and script resources by right-clicking**

The wrong pop-up menu would open by right-clicking with a mouse on a condition, test, result {true/false} or action. This problem has been fixed.

Support reference 7294

**Adding an environment variable |programfilesnative|**

Up until now, there had only been the environment variable |programfiles| to reference an application identifier for application control.

|programfiles| only allowed pointing to 32-bit "Program Files" paths. The |programfilesnative| variable now allows referencing the native "Program Files" path. This will continue to be "C:\Program Files" regardless of whether it is a 32 or 64-bit operating system.

Support reference 9680

**Exception in the console when copying an empty cell**

In system logs, the console would return an exception whenever an empty cell was copied. This problem has been fixed.

Support reference 9696

**Interpretation of regular expressions defined in the Log Manager.**

Regular expressions that allow choosing the log messages defined in the Log Manager were not interpreted in the same way by the console and agent. This problem has been fixed.



Support reference 8410

**Synchronization statuses in a multi-server environment**

In certain cases, during a synchronization with several servers, the **Servers** window would display for all servers except one the status "Synchronization failed", even when all servers were correctly synchronized.

Support reference 8826

**Search behavior in AD**

When an AD search returns too many results, only the first 50 will now be shown. Furthermore, a status icon will be displayed next to the root node of the search and a tooltip will indicate the need to refine the search.

Support reference 9705

**Tracking modifications to log messages in the event viewer**

The addition and deletion of log messages in the Log Manager were not correctly reflected in the event viewer. New logs are now shown in italics until they are first validated in order to recognize them more easily when editing logs.

Support reference 9482

**Reappearance of deleted application rules**

After application rules have been deleted from the main node, they could reappear during the selection of a group or during the validation of the policy. This problem has been fixed.

Support reference 9621

**Adding identifiers to application rules in a policy that is not being edited**

Application identifiers could be added to application rules even when the policy was not being edited, but this is no longer the case.

Support reference 9502

**Defining an application identifier that begins with "\*" :**

Application identifiers that do not take into account the letter of the drive ("\* : ") can be defined once again. "

Support reference 8467

**Adding application or firewall rules to the main node of groups**

Rules can no longer be added to the main nodes of various rules in the security policy.

Support reference 9734

**Dragging and dropping for script resources**

Ever since version 7.2, elements of scripts (tests, action, conditions) could no longer be dragged and dropped. The panels affected were script resources and script policies. This problem has been fixed.

Support reference 9651 (#CF 86289)

**Blue screen due to application control**

A blue screen could appear on the workstation when launching binary files if there had been too many application rules in the security policy. This problem has been fixed.



# Stormshield Endpoint Security 7.2.05 updates

Support reference 9749

## Integration of new AVIRA configuration functions

- The **Show warning messages** parameter has been added for the 'Scanner', 'Real-time Protection' and 'Web Protection' components in the antivirus configuration.
- The **Quarantine directory** parameter has been added to the general settings in the antivirus configuration.
- There is no longer the need to be an administrator in order to start an Avira scan.

Support reference 8237

## Stack pivot protection for 64-bit processes

Protection from stack pivot attacks has been strengthened to protect 64-bit processes as well.

Support reference 9753

## Libxml2 upgraded to version 2.9.3

The version of libxml2 previously used (2.9.2) for managing XML files contained security flaws. The version used on SES is the most recent version to date (2.9.3).

Support reference 9710

## OpenSSL upgraded to version 1.0.1q

The version of OpenSSL previously used (1.0.1p) contained a vulnerability that would potentially allow an attacker to cause a denial of service attack on the SES server. The version used by SES has been upgraded to version 1.0.1q.



# Stormshield Endpoint Security 7.2.04 new features

## Dashboard

The SES management console home screen now displays a dashboard. It includes four charts providing an overview of the state of the agents. Each chart can be undocked from the main window and displayed on another screen.

The dashboard can also be accessed from the **Management and Monitoring Tools** panel.

Refer to the *Administration Guide* for more details about the dashboard.

## Display of logs improved in the SES management console

The previous **Log Monitoring** panel has been replaced by the main menu **Dashboard** in the **Management and Monitoring Tools** panel, and by the sub menus **Software logs**, **System logs**, **Network logs** and **Device logs**.

This improvement allows searching relevant data in logs thanks to simple and advanced filters.

Refer to the *Administration Guide* for more details about the display of logs.

## Full support for Windows Server 2003 SP2 and R2 SP2

Stormshield Endpoint Security now supports Microsoft Windows Server 2003 SP2 and R2 SP2 operating systems. All of the Stormshield Endpoint Security security features and devices are available for the installation Stormshield Endpoint Security Server-Side Edition 32 bits on these new platforms.

## Updating whitelisting templates

It is now possible to update whitelisting templates used by Stormshield Endpoint Security through the menu **Tools > Updating whitelisting templates**.

By default, the file *Templates.scwt* is in the **Templates** directory of the SES management console. You can also request an up-to-date version of the file to the Technical support.

### WARNING

Significant changes have been made to the log databases. Thus updating alert databases with the DBInstaller tool may take a long time. To ensure the update runs correctly, the available space on the disk where the bases are stored must be at least equal to the size of the biggest table of the log databases (db\_SoftwareLog, db\_systemLog, db\_networkLog or db\_MediaLog).



# Stormshield Endpoint Security 7.2.04 fixes

## Known issue

Support reference 8962

### Installing the SES management console and a SES agent on the same workstation

It is currently not possible to install or uninstall a SES management console on a workstation on which a agent is already installed.

The only workaround solution in this version is to disable the SES agent or to set the Warning mode in the console.

## Agent fixes

Support reference 9190 (#CF 85863)

### Home screen configuration lost when encrypting files

On Windows 8 operating system, when encrypting files on the system disk, the configuration of the home screen was lost. The issue also occurred when Sticky notes were configured. These problems are fixed.

Support reference 9181 (#CF 85358)

### The agent cannot be installed on Hungarian Windows XP

It was not possible to install the SES agent on the Hungarian version of Windows XP. The problem could also occur on versions of the operating system in other languages. This problem is fixed.

Support reference 8954

### Error message when applying a file encryption policy

When applying a file encryption policy, an error log was displayed if no letter was linked to a partition. This problem is fixed.

Support reference 8907

### Rights management improved to access the SES installation folder

The protection against an irrelevant change of the rights to access Stormshield Endpoint Security folder by an administrator or a program with administrator rights has been improved.

Support reference 8701

### Installing the antivirus program after a restart

It was not possible to properly install the antivirus program just after the machine had restarted. Some elements were missing. These elements are now retrieved properly.

Support reference 8806 (#CF 84878)

### Bad policies application when the connection to the Active Directory was lost

In Active Directory mode and if the connection to the Active Directory server was lost, if a policy was applied on an organizational unit (OU) or on a group of SES agents which name included a special character (accent, etc.), the agent did not apply the policies assigned to this OU.

Support reference 8715

### Installing the antivirus program

When installing the antivirus program, an error log was displayed because of an error of file copy. This problem is fixed.



Support reference 9067 (#CF 85838)

**Incompatibility with McAfee**

On 64-bit operating systems, a BSOD occurred if McAfee Viruscan 8.8 Patch 6 was installed with Stormshield Endpoint Security. This problem is fixed.

On 32-bits operating systems, McAfee applications stopped unexpectedly. This problem is fixed.

Support reference 8976 (#CF 85826)

**Use of the LDAP port to retrieve the computer name**

Until now the port used to retrieve the computer name on the agent side was the port 135 but this port is not considered as a valid LDAP port. The port used now is a standard LDAP port.

**i NOTE**

For outgoing communication, the remote ports TCP 88, TCP 389, UDP 389, UDP 53 and TCP 3268 must be opened between the workstation and the Active Directory server.

Support reference 8974

**Exception on *ntdll.dll* when loosing the connection to the Active Directory on Windows XP**

On Windows XP, when the connection to the Active Directory server was lost and a policy was modified in the SES management console, the reconnection of the agent to the server caused an exception in *ntdll*. This problem is fixed.

Support reference 9039

**Renaming of SES update file names**

When updating Stormshield Endpoint Security, the names of the update files downloaded by the agent are now in lowercase.

Support reference 8832

**Firewall logs and Ethernet filtering**

In the Firewall module, the log type displayed was false when a network connection was blocked at the Ethernet level (via source or destination MAC address). Now the adequate log of the type 'FW\_MAC' is displayed.

Support reference 9111

**MAC address in the Firewall logs**

In the Firewall module, the MAC address specified in the log was false when a network connection was blocked at the Ethernet level. This problem is fixed.

Support reference 9178 (#CF 85872)

**Slow workstation when opening the Windows session**

The workstation could be very slow because of the crash of one of the svchost processes.

Support reference 9289

**Installation path of the SES agent in lowercase**

Since the version 7.2, the installation path of the SES agents included folder names beginning with a lowercase letter. Installation paths have been normalized and are written now "Stormshield" instead of "stormshield". The 7.2 agent is now installed in the folder **C:\Program Files\Stormshield\Stormshield Endpoint Security Agent\**.



Support reference 9294

**Random BSOD**

When the SES agent prevented a registry key from being opened, a BSOD could occur. This problem is fixed.

Support reference 8970 (#CF 85869)

**Chrome 64 bits does not work with Stormshield Endpoint Security**

The 64-bit version of Chrome displayed an error message when it was installed with the SES agent. The issue occurred on all the supported 64-bit platforms (Windows 7 64 bits and Windows 8.1 64 bits). This problem is fixed.

Support reference 8211

**Avast 64 bits does not work with Stormshield Endpoint Security**

The 64-bit version of Avast caused a BSOD when it was installed with the SES agent. The issue occurred on all the supported 64-bit platforms (Windows 7 64 bits and Windows 8.1 64 bits). This problem is fixed.

## Server fixes

Support reference 8930 (#CF 85501)

**Compliance of Syslog TCP with the RFC 6587**

Some commercial Syslog servers including the RSA server could perform a bad interpretation of logs because of a non-compliance of the Syslog emission on TCP. This problem is fixed.

Support reference 8503

**Memory leak issue in the conversion engine on the server side**

An error when synchronizing the policies on the server side caused a memory leak and a log was displayed. This problem is fixed.

Now the version of security policies is verified both on server side and agent side.

Support reference 9236

**Generation of a certificate from an up-to-date server**

The installation program of Stormshield Endpoint Security 7.2 no longer allowed generating certificates on a 7.2 server which had been updated since a version 7.1 or 6.0.

## Console fixes

Support reference 9169

**Accessing a rule from the dashboard**

The **Go to Rule** feature in the dashboard now points to the rule corresponding to the selected log.

Support reference 8833

**Restart of the SES management console and license change**

It is now possible to add an expired license and then to replace it with a valid license without restarting the SES management console.

Support reference 8828

**Changes made on security policies displayed in the Event Viewer**

When adding or modifying an application identifier, the log in the Event Viewer did not display enough information. Also, the changes made in the general settings of the **Application Control**





tab in the security policy were not all listed in the Event Viewer. The Event Viewer now lists all changes made on security policies from the SES management console.

Support reference 8553

### **Logs duplicated in the Log Manager**

When logs were imported several times in the Manager, multiple copies were displayed. This problem is fixed. A previous version of a log is now replaced by the new import.

Support reference 8946

### **Synchronizing tests and actions after migrating**

When tests and actions were migrated on Stormshield Endpoint Security 7.2.03, there were not synchronized if the administrator had not viewed them before synchronizing the SES management console. This problem is fixed.

Support reference 9119

### **Detection of USB devices**

In some cases, starting the detection of USB devices could close unexpectedly the SES management console. These cases are now properly managed and do not suspend the use of the console.

Support reference 9149 (#CF 85554)

### **Policy or configuration settings lost**

If many modifications had been made in a policy or configuration, errors could occur when selecting the check out mode in the SES management mode. All the settings of the policy or configuration were lost because of these errors. This problem is fixed.



## Stormshield Endpoint Security 7.2.04 updates

Support reference 8857

### **libxml2 library update**

There was a security vulnerability in the libxml2 library used for XML files management (configuration, policies, etc.). It has been updated to fix this issue.

Support reference 8304

### **Apache server component updated to version 2.2.31**

The Apache server component installed with the SES server has been updated to version 2.2.31 in order to counter the vulnerability allowing an attacker to cause a denial of service.



# Stormshield Endpoint Security 7.2.03 fixes

---

## Agent fix

Support reference 8897

### **Crash of Internet Explorer 11 when the RCP protection was enabled**

The RCP protection made some 32-bit applications crash when running on the Windows 7 64-bit operating system. This was the case for Internet Explorer 11 which is a 32-bit application. This problem has been fixed.



# Stormshield Endpoint Security 7.2.02 fixes

## Agent fixes

Support reference 8547 (#CF 85247)

### Blue screen occurring when the workstation goes into sleep mode

In the Network security control tab of the security policy, when some Network Firewall rules were filtering on the MAC address, some workstations did not go properly into sleep mode. The shutdown could also be unusually long: a blue screen occurred and the computer stopped. This problem is fixed.

If you use filtering rules on MAC address, we recommend you to update Stormshield Endpoint Security to version 7.2.02.

Apply the following procedure on the impacted computers:

1. Deactivate all Network Firewall rules with MAC address filtering. You can create a "temporary" policy without MAC address filtering for these agents.

#### NOTE

If filtering on MAC address is defined in some Network Firewall accepting rules, some network services may not be accessible during the update process. You can then add additional accepting "IP address" rules.

2. Wait for all the machines to receive the new policy.
3. Restart the machines.
4. Update Stormshield Endpoint Security.
5. Activate the deactivated rules.

If the procedure is not properly applied, a blue screen may occur during the update. In this case, restart the computer twice. The update will still be applied and the issue will be definitely fixed. If Microsoft Windows prompts to choose between normal restart, safe mode or system recovery, select normal restart.

#### NOTE

Workstations under Windows XP are not impacted. They can be normally updated.

Support reference 8427 (#CF 84778)

### Deadlock on synchronization mechanisms

When applications used synchronization mechanisms on the workstation, a deadlock could occur when threads using these mechanisms stopped (for example applications using Mono or Unity3D). This problem is fixed.

Support reference 7133

### Random blue screen occurring when resuming from sleep mode

A blue screen could occur when 32-bits operating systems resumed from sleep mode. This problem is fixed.

Support reference 8478

### New restart log added to notifications

When updating or installing SES agents, a restart log now displays in the event log.



Support reference 8407

**Running applications from removable devices**

When the agent was disabled, running applications from a removable device was not possible. This problem is fixed.

Support reference 8338

**DirectX keylogging method**

Keylogging using the Directx method was not blocked when the protection was set to the "critical" level. This problem is fixed.

Support reference 8295

**Different Network Firewall and WiFi Access Points configurations between console and agent**

The deactivation of Network Firewall and WiFi Access Points groups in the *Network security control* tab of the security policy could not be taken into account by the SES agent. This problem is fixed.

Support reference 8434

**Improvement of logs related to tokens**

Error logs displayed when exchanging tokens between the server and SES agents have been improved.

Support references 6596 and 8494

**Enhancement of the agent self-protection**

The protection of SES agent components on the workstation has been enhanced in order to ban right modifications on these components.

Support reference 8441

**Compatibility with Oracle VM VirtualBox**

The compatibility with Oracle VM VirtualBox has been improved.

Support reference 8535 (#CF 85050)

**No Execute rules displayed in ssmom**

When the protection against executable file creation was enabled, messages relating blocking processes were no longer displayed in the SES agent event log but only in log files. This problem is fixed.

Support reference 8521

**Correction of the display of the executable file creation blocking log**

When the protection against executable file creation is enabled, now no log is sent when modifying the content of an executable file.

Support reference 8581 (#CF 84542)

**Installing Avira antivirus on a Spanish operating system**

Now the Avira antivirus program is installed in English by default on workstations which system language is other than French.

Support reference 8584

**Protection against executable files creation**

Protection against the creation of executable files has been strengthened.

Support reference 8633 (#CF 85259)

**Correction of a IRQL\_NOT\_LESS\_OR\_EQUAL blue screen at machine startup**

A blue screen could happen randomly on some workstations under Windows XP.



Support reference 8678 (#CF 85675)

**Correction of Root registry keys management**

Management of the Root registry keys has been enhanced. A bug could cause an unexpected shutdown of applications.

Support reference 8727 (#CF 85696)

**Compatibility between a VPN IPSec client and the SES firewall under 64-bit Windows 7**

Using the SES agent firewall (driver "thor3") and a VPN IPSec client at the same time on the same workstation under 64-bit Windows 7 could not always work. The SES firewall incorrectly filtered incoming packets such as UDPENCAP (encapsulation of the ESP protocol in UDP packets source/destination ports 4500). As a consequence, network flows routed by a VPN IPsec tunnel were not functional. This problem is fixed.

## Server fixes

Support reference 6596

**Enhancement of the server self-protection**

The protection of SES server components on the workstation has been enhanced in order to ban right modifications on these components.

Support reference 8716 (#CF 85597)

**Management of log cache files enhanced**

Log cache files incorrectly formatted are now properly managed on the SES server.

## Console fixes

Support reference 8329

**Incorrect search in a log filter**

When filtering software, system, network or device logs in the **Log Monitoring** panel with the method "contains" in the **Comparison** field, the search did not find logs if the filter "Value" contained the character [ ]. This problem is fixed.

Support reference 8428

**Checking the parent relationship of servers certificate**

When synchronizing the SES administration console and servers, the root authority of the servers certificate is now compared to the root authority of the administration console certificate in order to check the parent relationship.

Support reference 8451

**Error in the console when sorting certificates according to the validity date**

In the security policy, sorting certificates according to the validity date works now properly.

Support reference 8486

**Error in the console when sorting policies if there is no inherited policy**

In the **Policies linked** panel available from the **Environment Manager**, sorting works now properly for policy categories which do not contain inherited policy.

Support reference 8426

**Inconsistent ranks after deleting security rules**

In the **Application Control** tab of the security policy, when the focus was set on **Applicative rules**, **Extension Rules** or **Trusted Rules** and when the user deleted one or more lines, the ranks



numbering became inconsistent. This problem is fixed.

Support reference 8327

### **Creation of applicative rules / sub-rules Network**

Since the IP parameter was introduced in version 7.2.00 in the sub-rules Network in the applicative rules of the security policy, it was impossible to create two rules with the same network modes and ports. This problem is fixed.

Support reference 8478

### **New restart log added to notifications**

A restart log has been added in the console event log to indicate an update or installation of Stormshield Endpoint Security.

Support reference 6910

### **Support of special characters in the antivirus policy**

The antivirus policy now supports special characters in the **Paths to scan** and **Files to scan** fields.

Support reference 8549 (#CF 85629)

### **Check in of the log manager impossible after importing .LFXML file**

In the log manager, an error prevented imported elements from being saved in the database. This problem is fixed.

Support reference 7298

### **Copying rules of a security policy in the same order**

It is now possible to paste the rules of a security policy in another policy in the same order.

Support reference 8625

### **Enrolling a removable device via an Active Directory Windows user**

In the device enrollment manager, it was not possible to add a USB device if the console user had been created from a Windows account. The **Enrolled by** field remained empty because the user was not found in the Active Directory. This problem is fixed.



# Stormshield Endpoint Security 7.2.02 updates

Support reference 8202

## New contextual menu from application identifiers

In the SES administration console, a contextual menu has been added to application identifiers in the **Application Control** tab of the security policy. It allows assigning or removing identifiers to the current rule or going directly to the selected identifier in the application identifiers management panel.

Support reference 8448

## New Stormshield SignTool shortcut in the Start menu

A shortcut to run Stormshield SignTool is now available in the Windows Start menu since Stormshield Endpoint Security 7.2.02.

Support reference 8455

## Filtering extensions when importing certificates

When importing certificates in the SES administration console, it is now possible to filter certificates extensions (\*.cert, \*.crt, \*.der, \*.pem, \*.p7b et \*.p7c).

Support reference 8666

## Multiline display in the SES administration console

In the security policy, the rules editor can now be customized. Network rules, applicative rules, extension rules and trusted rules can now be displayed on several lines.

Support reference 8775

## OpenSSL update

OpenSSL has been updated to version 1.0.1p.

Support reference 8498

## cURL update

cURL has been updated to version 7.42.1.

Support reference 8309

## SQLite update

Security vulnerabilities have been disclosed about SQLite. SQLite has been updated to version 3.8.10.2 in order to block these vulnerabilities.





# Stormshield Endpoint Security 7.2.01 fixes

---

## Agent fix

Support reference 8446

### **Policies could not be migrated from version 7.1 to 7.2**

When updating from StormShield version 7.1 to Stormshield Endpoint Security version 7.2, the new 7.2 agent was not able to apply 7.2 policies downloaded from the server before being updated. Resynchronizing policies on the server from the SES console was first required to make the agent able to retrieve and apply them. This problem has been fixed and is described in the STORM-2015-03 security advisory.



# Stormshield Endpoint Security 7.2 fixes

## Agent fixes

### USB devices blocked when the agent is shut down

Support reference 7228

The Stormshield Endpoint Security agent may block access to USB devices if it has been shut down. This problem has been fixed.

### Anticipated booting of the agent's service

Support reference 7035

The agent's service always boots first on the workstation so that the agent would have an active status as soon as possible.

### New configuration file for kernel protection

Support reference 7523

A new file *dumpconf.srn* has been created at the root of the system partition. This enables the separation of the configuration from the policy for Stormshield Endpoint Security protection.

### Integrity of configuration files for kernel protection

Support reference 7550

The files *dumprules.srn* and *dumpconf.srn* stored at the root of the system partition are now covered by an integrity test to detect corruption.

### Poor initialization of RCP protection

Support reference 7643

RCP protection would occasionally fail to function correctly on certain processes due to the poor initialization of the internal mechanism. This problem has been fixed.

### HPP protection may fail to function without RCP protection.

Support reference 6454

Under Windows 7 in 32 bits, HPP protection did not function when RCP protection was disabled. This problem has been fixed.

### HPP protection may fail to function without KRP protection.

Support reference 7141

Under Windows XP, HPP protection did not function when KRP protection was disabled. This problem has been fixed.

### Poor initialization of HPP protection

Support reference 7142

Under 32-bit systems, HPP protection would occasionally fail to function correctly due to the poor initialization of the internal mechanism. This problem has been fixed.

### BSOD in Thor3 and Meili

Support reference 7789

A blue screen involving network filtering drivers (Thor3 and Meili) could occur whenever the workstation lacked physical memory. This problem has been fixed.



## Console fixes

Support reference 6861

### Resizing of columns in the Policies linked panel

Columns in the **Policies linked** panel in the management console can now be resized.

Support reference 6829

### Removal of the "Server configuration" category

In the Active Directory tree in the management console, whenever an agent was selected, the "Server configuration" category would appear. This is no longer the case. Likewise, if a server is selected in the same tree and it is linked to an organizational unit in AD, the Stormshield Endpoint Security server panel would appear.

Support reference 7239

### Improved firewall logs

The readability of Stormshield Endpoint Security firewall logs has been improved.

Support reference 7165

### Update of a console immediately after its installation

Whenever the management console was updated immediately after it had been installed, the database installation program instead of the update program would execute. This problem has been fixed.

Support reference 7065

### Editing multiple application rules

The collective status of a selection of several application rules can now be edited in the management console.

Support reference 7306

### Problem selecting panels in the console

The wrong tab would appear in the management console whenever the selected policy was changed, causing random behavior. This problem has been fixed.

Support reference 7130

### Pop-up menus in the management console

Pop-up menus in the management console could appear on elements that should not be having them. This problem has been fixed.

Support reference 7412

### Reorganization of firewalls rules through keyboard shortcuts

An error could occur whenever firewall rules were reorganized using the keyboard shortcuts intended for such purposes. This problem has been fixed.

Support reference 7435

### Path validation

Invalid paths in application rules or extensions on removable devices could be accepted in the management console. This problem has been fixed.

Support reference 7544

### Stack corruption

Stack corruption could occur in the management console during the creation of a recovery CD, for example. This problem has been fixed.



Support reference 7422

**Random display of DbInstaller**

A bug in DbInstaller has been fixed. The bug would occasionally display its main panel after a migration of the database during an update of the management console. Likewise, the panel that summarizes the product installation could continue to be displayed if the import of older policies was selected.

**Graphical fixes in the console**

The graphical aspect of the console has been standardized. Icons and the size of certain columns have been revised. The **Rename** option was added to certain pop-up menus.

Support reference 7622

**Fixes in the console**

The display of page numbers in log monitoring has been corrected: the first page now bears the number "1" instead of "0".

Support reference 7563

**Changed environment variables**

|systemroot| and |programfiles| have been removed from the list of environment variables allowed for file encryption. The agent never encrypts these locations.

Support reference 8013

**Generation of Firewall / Network filtering rules**

During the generation of "Network firewall" rules in the security policy file, the order of rules was not kept. Indeed, instead of generating rules according to the "Rank" setting ('#' in the console display), the order of groups of "Network firewall" rules in the security policy would be used instead. This issue has been fixed. Rules now follow the order specified in the "Rank" setting. Caution: this fix may have a signification operational impact on your network filtering policy. When migrating from an earlier version of Stormshield Endpoint Security, the administrator must check that the order of network filtering rules indeed follows the desired type of filtering.

Support reference 7533

**Changed policy link system**

A new policy link editing panel has replaced the existing panel. Links can now be created there without dragging and dropping.

Support reference 8207

**Backwards compatibility of policies**

A mechanism has been added to improve the reliability of the behavior of recently updated agents that have not yet received the policies corresponding to their version.

Support reference 8025

**Management of CSV separators**

A new parameter has been added to the management console's options to manage the various separators in CSV format. This parameter affects how the contents of agent groups and hash files are imported.

Support reference 8059

**Modification of the SES installer**

The Stormshield Endpoint Security installed has been modified: the optional "Console settings" step has been removed. The default name of the database's instance is now SES and no longer EDDAS. Several strings have been modified to make them clearer.



## Stormshield Endpoint Security.7.2 new features

### Enhanced heap spray detection engine

Stormshield Endpoint Security includes a new heap spray detection algorithm. This new engine now replaces the previous one when the **Protection against memory overflow** option is set to "High" or "Critical" in the security policy. When set to "Low", the former algorithm will continue to be used.

This new engine improves the detection of heap spray attacks.

### New update process

The process of updating from an older version of StormShield to the new Stormshield Endpoint Security 7.2 version has changed. There is no risk of compromising security on the workstation the next time it is rebooted following the installation of the new version.

### Full support for Windows 8.1 and Server 2012 R2

Stormshield Endpoint Security now supports Microsoft Windows 8.1 Update 1 and Windows Server 2012 R2 Update 1 operating systems. All of the Stormshield Endpoint Security security features and devices are available on these new platforms.

### Full support for Windows Server 2003 SP2 and R2 SP2

Stormshield Endpoint Security now supports Microsoft Windows Server 2003 SP2 and R2 SP2 operating systems. All of the Stormshield Endpoint Security security features and devices are available for the installation Stormshield Endpoint Security Server-Side Edition 32 bits on these new platforms.

### Application filtering by hash or certificate

Certificates or MD5 or SHA-1 hashes can now be used for identifying applications in application rules in the administration console. Furthermore, application filtering can now be configured in blacklist or whitelist mode.

Older policies in version 7.1 can be imported. Details on how to use this new feature are provided in the Stormshield Endpoint Security *administration guide*.

### Enhanced security in kernel memory allocation

Privileges allowing Stormshield Endpoint Security kernel components to execute memory allocation have been removed. This enhancement is possible from Microsoft Windows 8 / Windows 2012 upwards.

### Cancellation of a lock in the management console.

Locks can now be broken in the Stormshield Endpoint Security management console. Administrators holding the "User Management" privilege can indeed impose editing of a policy. Administrators can therefore override users who are currently editing the policy without having validated it.

### Reinforced protection against memory overflow

Protection against memory overflow now checks "stack pivot" attacks. The Stormshield Endpoint Security agent now blocks such attacks.

### Enhanced Stormshield Endpoint Security driver logs

Debug logs of Stormshield Endpoint Security kernel modules have been enhanced.



### **Upgrade to framework .NET 4.0**

Stormshield Endpoint Security now uses the NET 4.0 framework instead of version 2.0.  
Stormshield Endpoint Security will automatically install this new prerequisite if necessary.



## Features removed from Stormshield Endpoint Security 7.2

---

**Removal of the "Protection against CPU overload" feature.**

This feature was removed from the product as its rate of false positives was too high.

**Removal of the "Copy/Paste" feature.**

This feature was removed from version 7.2 of Stormshield Endpoint Security onwards.



## Contact

---

To contact our Stormshield Technical Assistance Center (TAC):

- <https://mystormshield.eu/>

All requests to technical support must be submitted through the incident manager in the private-access area [https://mystormshield.eu](https://mystormshield.eu/), under **Technical support > Manage cases**.

- +33 (0) 9 69 329 129

In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on <https://mystormshield.eu>.





# STORMSHIELD

*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.*