STORMSHIELD ENDPOINT SECURITY EVOLUTION

RELEASE NOTES

Version 2

Document last update: September 27, 2021

Reference: ses-en-release_notes-v2.1.1

Table of contents

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

This document is not exhaustive and minor changes may have been included in this version.

SES Evolution 2.1.1 fixes

Installation

Support references: SESNG-7486

You can now launch an update a second time via the Installation Center if it was canceled the previous time.

Support references: SESNG-7842

The Installation Center now correctly verifies the backend component password.

Stormshield default policy

Support references: SESNG-7714

When keylogging protection is enabled, KeePass Password Safe is no longer prevented from automatically entering passwords

Support references: SESNG-7865

Wi-Fi rules that were initially in the *Protection baseline* rule set have been outsourced to an independent rule set that is not included by default in policies. In this way, the software security policy can be kept separate from the hardware component usage policy. In addition, Wi-Fi and general device rules no longer generate incidents systematically.

Support references: SESNG-8105

By adding a new root certificate that Google Chrome uses, the browser can be started again when a user clicks on a hypertext link in an e-mail in Microsoft Outlook.

Support references: SESNG-8399

The SQL Server VSS Writer identification mode has been changed. Now it no longer freezes when it writes information to the Shadow Copies registry.

Support references: SESNG-8444

Microsoft Office applications that write *.js* extension files no longer raise alarms.

To reduce the occurrence of false positives, some heuristic rules that detect password-stealing malware were removed from the policy, and two Microsoft programs known to access raw volumes were added to the policy.

Rule sets

Support references: SESNG-8335

Links to policies in the panel of a rule set are now kept when the **Update all** action is used.

Protection rules

Support references: SESNG-8345

In file rules or application identifiers, file paths containing errors could previously be entered. These are now verified.

OSSEC rules

Support references: SESNG-8345

Some of the file paths that must be monitored in OSSEC rules prevented the policy from being applied. This issue has been fixed.

Logs

Support references: 183722CW

Rules created when an exception is added from a log are now configured correctly.

Support references: 167478PW

SES Evolution no longer generates errors when there is a large volume of context logs.

SES Evolution agent

Support references: 184781CW

When events are exported in the SES Evolution agent interface, a list of technical errors is no longer displayed.

Compatible Microsoft Windows versions

SES Evolution 2 is compatible with the following Windows versions. For more information, refer to the System requirements for SES Evolution section in the *Installation guide*.

Administration console
Windows 7 in 32 and 64 bits
Windows 8.1 update - August 2014 - 32 and 64 bits
Windows 10 Enterprise 2015 LTSB - 32 and 64 bits Windows 10 Enterprise 2016 LTSB - 32 and 64 bits Windows 10 1809 – 32 and 64 bits Windows 10 1909 – 32 and 64 bits Windows 10 2004 – 32 and 64 bits Windows 10 20H2 – 32 and 64 bits Windows 10 21H1 – 32 and 64 bits
Windows Server 2008 R2
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Backend
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Agent handler
Windows 10 Enterprise 2015 LTSB – 64 bits Windows 10 Enterprise 2016 LTSB – 64 bits Windows 10 1809 – 64 bits Windows 10 1909 – 64 bits Windows 10 2004 – 64 bits Windows 10 20H2 – 64 bits Windows 10 21H1 – 64 bits
Windows Server 2008 R2*
Windows Server 2012 R2*
Windows Server 2016
Windows Server 2019

* On these newly installed operating systems, Framework .NET 4.6.2 must be installed beforehand to enable the SES Evolution Installation center to run.

Agent
Windows 7 in 32 and 64 bits
Windows 8.1 update 3 (August 2014) - 32 or 64 bits
Windows 10 Enterprise 2015 LTSB - 32 and 64 bits Windows 10 Enterprise 2016 LTSB - 32 and 64 bits Windows 10 1809 – 32 and 64 bits Windows 10 1909 – 32 and 64 bits Windows 10 2004 – 32 and 64 bits Windows 10 20H2 – 32 and 64 bits Windows 10 21H1 – 32 and 64 bits
Windows Server 2008 R2
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Recommendations

Before updating an existing environment to SES Evolution version 2.1:

- Read the section **Known issues** in the StormshieldKnowledge base carefully (use the same login credentials as those for your MyStormshield client area),
- Read the section Explanations on usage carefully,

Updating built-in security policies

During the update from SES Evolution 2.0.x to 2.1, built-in security policies and built-in rule sets will also be updated.

Updated policies will not overwrite existing built-in policies, which will simply be renamed with the suffix *(Before update)*. If you are using built-in policies and want to apply the enhancements that come with the update, there are two ways to do so:

If you have kept the initial policies without modifying them:

1. Change the policy in the configuration of the agent groups in question, to choose the newly updated policy, i.e., the one that does not have the *(Before update)* suffix.
2. Delete your older *(Before update)* policies.

If you have customized the built-in policies:

1. Make your changes in the new policies.
2. Change the policy in the configuration of the agent groups in question, to choose the newly updated policy, i.e., the one that does not have the *(Before update)* suffix.
3. Delete your older *(Before update)* policies.

Known issues

The up-to-date list of the known issues related to this version of SES Evolution is available on the Knowledge Base Stormshield (English only). To connect to the Knowledge base, use the same identifiers as for MyStormshield.

Explanations on usage

SES Evolution installation
If a Windows update is in progress during a full installation of SES Evolution server or of the backend component, the installation will fail. It is recommended to disable Windows update before installing SES Evolution, and to enable it again afterwards.

Bluetooth Low Energy devices
The SES Evolution agent does not filter Bluetooth Low Energy devices; only standard Bluetooth devices are recognized.

Documentation resources

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

Guides

- Installation guide
- Administration guide

Please refer to the Knowledge base for specific technical information and to watch videos that the TAC (Technical Assistance Center) has created.

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 2.1.1 version of Stormshield Endpoint Security Evolution:

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 Evolution 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**.

Previous versions of SES Evolution v2

In this section, you will find the features and fixes from previous versions of SES Evolution v2.

2.1	New features	Resolved vulnerabilities	Bug fixes
2.0.2			Bug fixes
2.0.1		Resolved vulnerabilities	Bug fixes
2.0.0	New features		

SES Evolution 2.1 new features

New protections

Advanced protections

Advanced protections make it possible to protect your pool from malicious operations such as the theft of authentication credentials, malicious use of Windows tools, persistent techniques, etc.

Find out more

New built-in policy: Protection of backoffice components

A built-in security policy is now equipped to increase the security of SES Evolution backoffice components. This policy must be applied to agent groups that contain agent handlers, backends and the administration console.
In addition to the security features in the default policy, it includes several modular rule sets, each of which corresponds to a backoffice component. The policy consists of the following rule sets:

- Audits of attack contexts,
- Backend protection (new),
- Agent handler protection (new),
- Administration console protection (new),
- Advanced protections (new),
- Protection baseline.

Find out more

Changes to existing policies

The default policy has been enriched with new rule sets that provide advanced protections and protection from theft of sensitive information.

It now consists of the following rule sets:

- Audits of attack contexts,
- Advanced protections (new),
- Data leak prevention (new),
- Protection baseline.

When updating from SES Evolution 2.0.x to version 2.1, refer to the Recommendations to find out the steps to take with regard to policy updates.

New built-in rule sets

The following rule sets have been added:

Backend protection	Protects the IIS application server (programs, settings, injection, etc.), database and SES Evolution Installation Center.
Agent handler protection	Protects the agent handler (programs, settings, injection, etc.), database and SES Evolution Installation Center.

Administration console protection	Protects the SES Evolution administration console (programs, settings, injection, etc.), database and SES Evolution Installation Center.
Advanced protections	Unlike protections that react to a strong individual event, advanced protections react to a pattern of several weak events, which when combined, represent a threat.
Data leak prevention	Protects some specific applications used frequently in organizations, e.g., web browsers, file transfer tools, vaults, Windows security authorities and remote control tools. This protection mode covers unauthorized access to files, registry locations and keylogging attempts to deter the theft of sensitive assets. Windows security authorities are also protected from interprocess access, which prevents the extraction of Windows passwords. Special attention is given to programs that allow external code to run (e.g., script engines, DLL loaders, etc.), so that their operations will always be blocked. Likewise, programs provided by default with Windows (LOLBIN) that allow indirect access to information, are blocked.
Windows Defender event forwarding	Consolidates in the administration console security alerts of interest that Windows Defender raises on protected workstations in the SES Evolution pool. It is not included in built-in policies, so it must be added manually to your policies.

Changes to existing rule sets

The following rule sets have been modified:

Audits of attack contexts	• Operations by programs that allow external code to run (e.g., script engines, DLL loaders, etc.) are now always logged, even when they are signed. • The list of certificates that the rule set recognizes has been enriched. • Rule severity levels have been revised so that no rule is below the agent group's default threshold (*Notice* level being the lowest) • Advanced detection of ARP Spoofing has been added to this rule set to detect Man In The Middle attacks. • Optimization to minimize impact on system performance without compromising audit quality. This will also reduce the possibility of losing logs during intense activity.
Protection baseline	This rule set has been enriched and hardened: • Settings cannot be changed in safe mode, • BCD (Boot Configuration Data) is now protected, • Applications recognized as hacking tools have been enriched, • Script engines can no longer be run from browsers, • System configuration files (hosts, services and network) are now protected from unwanted changes, • Third-party programs are monitored and not allowed to run from MS Office applications, • Heuristic analysis of malicious data theft programs, based on the name of the accessed file, has been improved • Unsigned services are monitored and prevented from running.

Agent management

Agent groups based on Active Directory criteria

Agents can be automatically assigned to an agent group according to the Active Directory groups or organizational units to which they belong. This feature saves time and lowers the risk of error when creating agent groups.

Find out more

Uninstalling agents

You can now prevent the local administrator of a workstation from uninstalling the SES Evolution agent. In this case, the agent can still be uninstalled via a challenge.

Find out more

Agent filtering

New filters now make it possible to show the list of agents by criteria such as operating system, status, security policy, etc.

Find out more

Dashboard

A new diagram now appears in the dashboard of the administration console and shows the number of agents in the pool for each version of SES Evolution.

Find out more

Database

Log retention in the database

The duration of log retention in the log database can be configured, either when SES Evolution is installed, or at any time through the new **System** menu in the administration console. When logs reach the end of their retention period, they will be deleted by a task that runs regularly.

Find out more

Versions of policies and rule sets

The versions of policies and rule sets are now better managed to optimize storage space in the administration database.

Find out more

Removable devices

The list of known USB devices (vendor and product) has been updated in the administration console.

Activity monitoring

Windows event monitoring

Windows events of your choice can be forwarded to SES Evolution so that security information about your environment can be displayed.

Find out more

Logging of user activity

User activity in the SES Evolution administration console is now logged through a full audit of operations performed.

Find out more

Backoffic component logs

A new menu in the administration console, **System logs**, shows the activity of agent handlers, backend servers and the SES Evolution administration console.

Find out more

OSSEC analysis engine

OSSEC rules can now be imported into security policies from the administration console. This allows agents to subscribe to text-based logs or Windows events, and report them as SES Evolution logs in the log database or an SIEM.

Find out more

Exporting to syslog servers

Logs can now be exported to several syslog servers and the export formats IDMEF and CEF have been added to facilitate their integration into your solutions.

Find out more

Resolved vulnerabilities for SES Evolution 2.1

Agent

Loading DLLs

A vulnerability would occasionally cause some processes on the agent to load DLLs located elsewhere than in the agent's installation folders. This vulnerability has been fixed.

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

Backend

Access to custom scripts

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

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

Changes to unused scripts

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

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

Removal of unused scripts

A low severity vulnerability was fixed after the SES Evolution backend component was upgraded.

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

Removal of application identifiers

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

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

Changes to security policies

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

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

Duplication of security policies

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

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

SES Evolution 2.1 bug fixes

Installation

In the Installation Center, *Minimum installation* has been renamed *Demo installation* to indicate that it must not be used in a production environment, only for testing or demos. *Advanced installation* has been renamed *Standard installation*.

Support references: SESNG-6898

The Installation Center no longer shuts down unexpectedly when the SQL user is unknown. A clear message now informs the user of the issue.

Support references: 182618CW

The language of the Installation Center is now the same as the language of the operating system when it is either French, English, Spanish or German. The Installation Center appears in English for operating systems in other languages.

SES Evolution Agent

Support references: 183130CW

In some cases during startup, the SES Evolution agent would wrongly detect an integrity issue, which would then require a restart. This issue has been fixed.

Support references: SESNG-7184

A compatibility issue between the SES Evolution and the CCleaner application has been fixed.

Support references: SESNG-5426

A blue screen (BSOD) would sometimes occur when the host switched to standby mode. This issue has been fixed.

Security rules

Support references: 181886CW

Exception rules can now be created from logs containing UNC paths.

Support references: 182180CW

Rules can now be copied/pasted or cut/pasted within the same rule set.

Support references: SESNG-5365

Process hollowing protection has been improved.

Support references: SESNG-7226

Privilege escalation rules in an audit rule set no longer prevent the evaluation of rules found in the rule sets that follow.

Support references: SESNG-5295

The *Detect only* action is no longer offered in keylogging protection rules. It was made redundant with the *Passive rule* mode.

Support references: SESNG-5370

All file access originating from the network can now be blocked using file access control rules.

Support references: SESNG-6878

A message now appears if you create an identifier with a path that ends in one or several space characters.

Logs

Support references: 182073CW

In the administration console, the attack chart now displays correctly when it contains WiFi logs.

Support references: SESNG-6372

Filters that exclude agent logs did not always function in the administration console. This issue has been fixed.

Support references: 183960CW

After users are deleted, they no longer appear in the list of users when logs are edited.

Device control

Support references: SESNG-5580

Occasionally, the agent would not display an authorization message when a USB device was plugged in, even though the USB device access control rule required it. This issue has been fixed.

Dashboard

Support references: SESNG-5780

When the SES Evolution environment contains several agent handlers, their status is now correctly displayed in the administration console's dashboard.

Agent management

Support references: SESNG-5505

Agent groups can no longer be created with invalid parameters.

Support references: SESNG-6910

The status of stopped agents now displays correctly in the **Agents** page of the administration console.

Support references: SESNG-7391

The Windows 10 21H1 operating system now displays correctly in the **Agents** page of the administration console.

Compatibility with other firewalls

Support references: SESNG-5309

Compatibility with other firewalls has been enhanced.

SES Evolution 2.0.2 fixes

SES Evolution upgrade

New version of policies
When SES Evolution is updated, Stormshield security policies are now updated as well.

Open administration console
The **Force update** button can now be used in the Installation Center to continue with an update even when an administration console is still open.

Error while updating the administration console
Updating the administration console no longer causes a recurring error in the logs of the backend component. The log is now generated at one go.

Updating the SES Evolution agent
After the SES Evolution agent was updated, it would occasionally prevent some processes from launching. This issue has been fixed.

Security Policies

Importing and exporting rule sets
Rule sets can now be exported and imported again into another SES Evolution environment in the same version.

Application identifiers
Using recursive identifiers and certificates together within the same security rule to identify an application would sometimes cause a blue screen. This issue has been fixed.

SES Evolution default policy
The default policy now includes compatibility with the Hardening mode in Panda Adaptive Defense 360. SES Evolution hides process hollowing operations when Panda causes them for legitimate reasons.

The audit rule set in the default policy was modified to restrict logs that are not relevant to security administrators. This reduces the number of logs displayed and the amount of system CPU that SES Evolution uses.

SES Evolution Agent

Support references: 178084CW - 180244CW

Under certain conditions, SES Evolution agents would send status information that would be misinterpreted by the agent handler. In such cases, the information displayed on the **Agents** panel of the administration console could be incorrect. Various other issues could also occur, such as the administrator being unable to respond to challenges. This issue has been fixed.

Agents waiting to be restarted after features are changed are now displayed correctly in the dashboard of the administration console.

Removable devices

Support references: 180798CW - 164622PW

Using *FTDI Chip* products no longer causes a blue screen. Overall compatibility with devices has been enhanced.

Resolved vulnerabilities for SES Evolution 2.0.1

Protection against denial of service attacks added

Protection against DDoS attacks was added to the API that registers new agent handlers in the Backend. Now only one agent handler can be registered every 15 seconds.

Value in the registry deleted

A value relating to the security of challenges was unnecessarily present in the registry. This vulnerability was fixed by deleting this value.

SES Evolution 2.0.1 fixes

Installing SES Evolution

Password fields
In the Installation Center, the password and confirm password fields are now always correctly verified.

License validity
In the Installation Center, the format and validity of the license are verified as soon as the license file is selected, instead of at the end of the installation.

Security Policies

Support reference: 177214CW

Network access
Some types of network access were not filtered by application protections because they were initiated by the system. They can now be blocked. This option makes it possible to block remote access to shared folders located on workstations that are protected by the SES Evolution agent.

If you upgrade SES Evolution to version 2.0.1, the default policy is not updated. You can download the corresponding rule set from your dedicated MyStormshield area to add network access permissions for system processes. For more information, refer to the Stormshield Knowledge base.

Network IDs
The **Invert identifier scope** option is now correctly saved in the network ID editing window.

Audit rules on drivers
Specific behavior in the *Driver loading* and *Driver integrity* protection rules is now correctly applied. These rules no longer generate unjustified logs for allowed drivers.

Logs

Searching in agent logs

In the administration console, the maximum duration of an agent log search has been increased from 30 seconds to 15 minutes. A message now appears when the search exceeds this duration.

Displaying incidents

When an incident is opened, only alert logs are now displayed, up to a maximum of 1000 logs. The remaining logs are loaded when the attack chart is consulted, up to a maximum of 100000 logs. This makes it possible to build an attack chart with comprehensive logs.

SES Evolution Agent

Lengthy logs

Lengthy logs no longer cause the graphical interface of the SES Evolution agent to unexpectedly shut down.

Self-protection rules

Self-protection rules on some registry keys of SES Evolution agents were not correctly applied. This issue has been fixed.

Display

Windows 10 agents

The **Agents** panel in the administration console now displays the correct version of the operating system for Windows 10 agents.

Summary of features

Version 2.0 of SES Evolution offers the following features.

SES Evolution 2.0 features

Protection	
Memory overflow	Protects your pool from intrusion attempts and vulnerability exploitation.
Process hollowing	
Security token theft	
File system bypass	
Keylogging	
File access control	Controls all system resources and access to them. Allows applications to make changes, access these resources or blocks them. You can also simply monitor them.
Registry base access control	
Memory access control	
Execution control	
Driver loading detection	Detects rootkits that attempt to load or change drivers in the kernel.
Driver alteration detection	
Application firewall	Controls incoming and outgoing network communications for each application.
Wi-Fi access point control	Manages allowed Wi-Fi networks and prevents the Wi-Fi-LAN bridge from being set up.
Floppy disk or CD/DVD drive control, serial ports	Controls devices allowed in your pool through fully customizable rules.
Bluetooth device control	
USB device control	
USB decontamination air gap	Controls the USB keys and hard disks in your pool, manages trusted devices and blocks devices that have not been validated.

Configuration	
Management via agent groups	Organizes your pool according to your requirements through a simple but powerful system of agent groups.
Configuration deployment	Deploys new configurations in all agents with a single click in the administration console.
Stormshield security policy	Protects your pool with a default policy that covers common threats and adds custom security rules to fully adapt the policy to your environment.
Context-based security policies	Adapts security to agents' environment so that they apply different policies based on their location.
Policy management through rule sets	Pool security rules in your policies and manage exceptions easily.

Scheduled tasks	Runs commands on agents by configuring scripts from the administration console.
Agent modularity	Manages features installed on each agent from the administration console: uninstall unused features, delete incompatible versions and reduce the attack surface.
Challenges	Allows some operations to be performed securely through a question/response system.
Simultaneously connected administrators	Organizes your administrators by role to manage simultaneous access to various resources on the administration console.

Activity monitoring	
Dashboard	See the status of your pool in a glimpse with a simple dashboard.
Log tracking	Views events that agents raise, filtering them by priority, type, group, etc.
Attack analysis	Follows incidents and analyzes attacks in a dedicated panel that illustrates steps in charts and provides additional information to better understand each attack.
Agent monitoring	Tracks the pool's agents in real time, checks their status and assigns them to groups
Syslog server export	Exports all events in your SIEM system to include them in your other sources of security information (firewall, antivirus, etc.).

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, 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.