STORMSHIELD

STORMSHIELD ENDPOINT SECURITY EVOLUTION

RELEASE NOTES

Version 2

Document last update: September 29, 2020

Reference: ses-en-release_notes-v2.0

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.

Introduction to Stormshield Endpoint Security Evolution 2.0

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

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

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

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

For more information on SES Evolution 2.0, see the ***Installation guide*** and the ***Administration guide***.

Summary of the features

The version 2.0 of SES Evolution provides 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.).

Compatible Microsoft Windows versions

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

Administration console
Windows 7 in 32 and 64 bits
Windows 8.1 update - August 2014 - 32/64 bits
Windows 10 Enterprise 2015 LTSB - 32/64 bits
Windows 10 Enterprise 2016 LTSB - 32/64 bits
Windows 10 1809 - 32/64 bits
Windows 10 1903 - 32/64 bits
Windows 10 1909 - 32/64 bits
Windows 10 2004 - 32/64 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 7 - 64 bits
Windows 8.1 update 3 (August 2014) - 64 bits
Windows 10 Enterprise 2015 LTSB – 64 bits
Windows 10 Enterprise 2016 LTSB – 64 bits
Windows 10 1809 – 64 bits
Windows 10 1903 – 64 bits
Windows 10 1909 – 64 bits
Windows 10 2004 – 64 bits
Windows Server 2008 R2
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

* On a newly installed Windows Server 2012 R2 operating system, Framework .NET 4.6.2 must be installed beforehand to enable the SES Evolution installation center to run.

Agent
Windows 7 in 32 and 64 bits
Windows 8.1 update 3 (August 2014) - 32 or 64 bits
Windows 10 Enterprise 2015 LTSB - 32/64 bits
Windows 10 Enterprise 2016 LTSB - 32/64 bits
Windows 10 1809 - 32/64 bits
Windows 10 1903 - 32/64 bits
Windows 10 1909 - 32/64 bits
Windows 10 2004 - 32/64 bits

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

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

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

Compatibility with other firewalls
In some cases, when another firewall with a priority higher than the SES Evolution agent's priority is installed on the same workstation and pauses the processing of a packet, regardless of its decision on how to process the packet, SES Evolution will never analyze it.

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

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 2.0 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**.

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.

STORMSHIELD