



STORMSHIELD



GUIDE

STORMSHIELD ENDPOINT SECURITY

FIRST TIME CONFIGURATION GUIDE

Version 7.2

Document last update: August 10, 2020

Reference: [ses-en-first_time_configuration_guide-v7.2](#)



Table of contents

1. Getting started	5
2. Protecting and configuring the SES server	6
3. Protecting access to the SES console	7
4. Configuring SES agents	8
4.1 Dynamic configuration	8
4.2 Static configuration	8
5. Creating a basic security policy template	9
5.1 Configuring SES in a day	9
5.2 Configuring SES in at least two days	9
5.3 Configuring system behavior control	10
5.3.1 Executable file creation	10
5.3.2 Protection against privilege escalation	10
5.3.3 Protection against spontaneous reboots	10
5.3.4 Protection against keyloggers	10
5.3.5 Protection against memory overflow	10
5.3.6 Kernel component protection	11
5.4 Configuring application behavior control	11
5.4.1 Applications access and Execution control	11
5.4.2 Execution control on removable devices	11
5.4.3 Network access and File access	11
6. Configuring protection against privilege escalation	12
7. Configuring protection against memory overflow	13
8. Configuring protection against keyloggers	14
8.1 Deleting logs with false positives	14
8.2 Allowing keyboard shortcuts	14
8.3 Allowing virtual environments	15
8.4 Allowing TeamViewer, DameWare, VNC, etc.	15
8.5 Allowing videoconference tools	15
8.6 Allowing Common Desktop Agent and all other programs	15
8.7 Expected result	15
9. Allowing and blocking file extensions	16
9.1 Expected result	17
10. Blocking viruses that spread easily	18
10.1 Blocking exe and js files with a misleading extension	18
10.1.1 Preventing execution of files with double extensions ending .exe	18
10.1.2 Preventing files with double extensions ending .js from being read	18
10.1.3 Preventing files with double extensions ending .rtf from being read	19
10.2 Restricting the capabilities of Windows scripts	20
10.2.1 Application identifiers	21
10.2.2 Application rules	21
10.3 Restricting the capabilities of Microsoft Office applications	21
10.3.1 Application identifiers	21
10.3.2 Application rules	22



10.4 Restricting screensavers to those installed by Microsoft Windows	22
10.4.1 Application identifiers	22
10.4.2 Extension rules	22
11. Blocking persistent malware	23
12. Protecting your mailbox	24
13. Protecting passwords	25
14. Creating an extension whitelist	26
14.1 Identifying extensions used	26
14.2 Creating extension rules in application rules	26
14.3 Filtering and exporting System logs	26
14.4 ExtractTool	26
14.4.1 Importing logs	27
14.4.2 Configuring ExtractTool in order to obtain a single identifier	27
14.5 Importing the results to the SES console	28
14.6 Allowing applications to access extensions	28
15. Blocking Internet access	29
15.1 Allowing Windows antivirus updates	29
15.2 Allowing web/FTP browsers	29
15.3 Allowing videoconferences or remote control	29
15.4 Allowing synchronization tools (if necessary)	29
15.5 Blocking attempts by the Microsoft Office suite to access the Internet, if possible	29
15.6 Allowing Stormshield Data Security	30
15.7 Allowing software updates	30
15.8 Prohibiting Microsoft memory dumps	30
16. Protecting the network	31
16.1 Ports 137/138 - NetBIOS	31
16.2 Port 1900 - SSDP discovery	31
16.3 Port 5355 - LLMNR	31
16.4 Port 17500 - Dropbox LAN synchronization	32
16.5 Port 5353 - Bonjour protocol	32
16.6 Port 21 - FTP	33
17. Using scripts to configure a policy	34
17.1 Detecting the local group	34
17.2 Detecting the time	35
17.3 Detecting the presence of a laptop battery	35
17.4 Detecting multihoming	35
17.5 Changing configurations in a click	38
17.5.1 Switching to normal mode	38
17.5.2 Switching to warning mode	38
17.5.3 Creating the test to check that a file exists	39
17.5.4 Configuring the SES environment	39
17.6 Disconnecting Stormshield Data Security Enterprise during an SES memory overflow event	39
17.6.1 Creating the User Defined Test that disconnects SDS	39
17.6.2 Creating the script that disconnects SDS	40
17.6.3 Implementing the script when an event occurs	40



18. Analyzing logs	41
18.1 Disabling automatic refresh	41
18.2 Selecting the log period to be analyzed	41
18.3 Selecting the columns to be displayed	41
18.4 Increasing the amount of logs per page in options	41
18.5 Analyzing Action=OVERFLOW logs	42
18.6 Analyzing Action=KEYLOG logs	42
18.7 Analyzing Action=REBOOT logs	42
18.8 Analyzing Action=SU logs	42
18.9 Analyzing Action=SOCK-CONNECT logs	43
18.10 Analyzing Action=SOCK-ACCEPT logs	43
18.11 Analyzing Statut=EXT-BLK logs	43
18.12 Analyzing remaining logs	43
19. Clearing logs	44
19.1 Selecting the duration of log retention	44
19.2 Creating an SQL script on the server	44
19.3 Creating a bat script on the server that calls up the SQL script	44
19.4 Creating a scheduled task	44

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



1. Getting started

The aim of this document is to help you in your initial implementation of SES. It acts as a complement to the solution's *Administration guide*, which provides a comprehensive description of its features.

Since every organization has different needs and particularities in its information system, this document only indicates recommendations; certain security rules do not apply to all contexts.

Our configuration recommendations for the SES solution apply to version 7.2 of SES.



2. Protecting and configuring the SES server

The first step in deploying the solution consists in securing the SES server. We recommend that you perform the following operations:

- Run a Windows update
- Install an antivirus on the server
- Enable the Windows firewall on the server
- Create a backup of the server
- Monitor the server (with a tool such as Nagios)

The ports that need to be opened on the server's Windows firewall are:

- Incoming communications:
 - TCP 80 (customizable): SES agent to SES server (download MSI file + update antivirus)
 - TCP 443 (customizable): SES agent to SES server (download certificate)
 - TCP 16004: SES agent to SES server (logs)
 - TCP 16005: SES agent to SES server
 - TCP 16006: SES agent to SES server
 - TCP 16007: SES console to SES server (synchronization)
- Outgoing communication:
 - TCP 1433 (customizable): SES server SQL server (database access)
 - UDP 1434 (customizable): SES server SQL server (database access)

WARNING

If the SQL server uses dynamic ports (this is the case for default installations with SQL express), you have two options:

- Modify the SQL configuration in order to have static ports, or
- Open other ports on the Windows server firewall.



3. Protecting access to the SES console

If you are managing SES on behalf of a client, you will need to create different administration accounts for each administrator. The solution allows logging each action.

The **Monitoring** section makes it possible to locate changes that have been made and the identity of the user who made them. This may be useful, for example, when an issue arises with a configuration or a security policy.



4. Configuring SES agents

4.1 Dynamic configuration

We recommend that you use the following dynamic agent configurations:

- Warning mode + no notification + allow agent shutdown: during the first installation phase,
- Normal mode + notification + prohibit agent shutdown: for advanced IT users,
- Normal mode + no notification + prohibit agent shutdown: for end users.

4.2 Static configuration

As soon as the solution is installed, we suggest that you specify the version of the agent. For example, if you are installing SES version 7.223, you need to configure the agent update in version 7.223:

POLICIES / STATIC AGENT CONFIGURATION / DefaultStaticAgentPolicy (Version: 5)	
Check Out Export	
Policy	Links
Challenges	
Script 1	(none)
Script 2	(none)
Script 3	(none)
Script 4	(none)
Script 5	(none)
Manage Update	
Update to deploy (ex: 7.2.23)	7.2.23

Therefore, when you migrate to version 7.2.24, you will create another static configuration that you will apply only to computers that will be used for testing the migration.

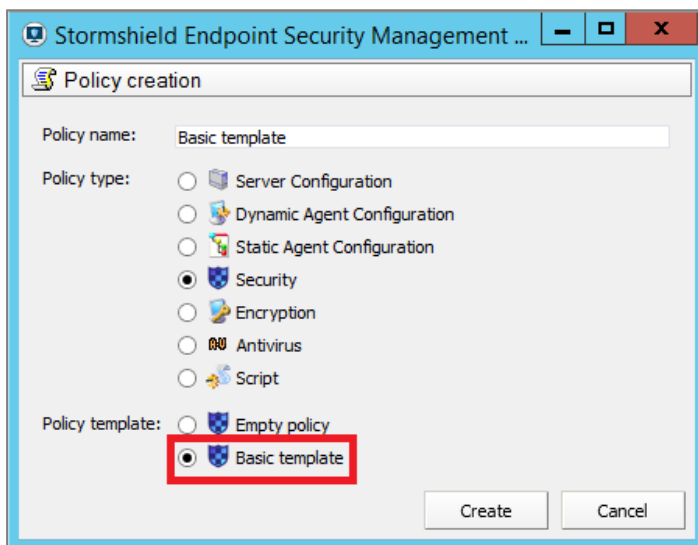


5. Creating a basic security policy template

An organization's level of IT security essentially depends on the amount of time allocated to security. We will be giving two configuration examples below. The first security policy blocks 95% of vulnerabilities, while the second, which provides better security, blocks 99.9% of them (these figures are just estimates and may vary according to the types of threats encountered).

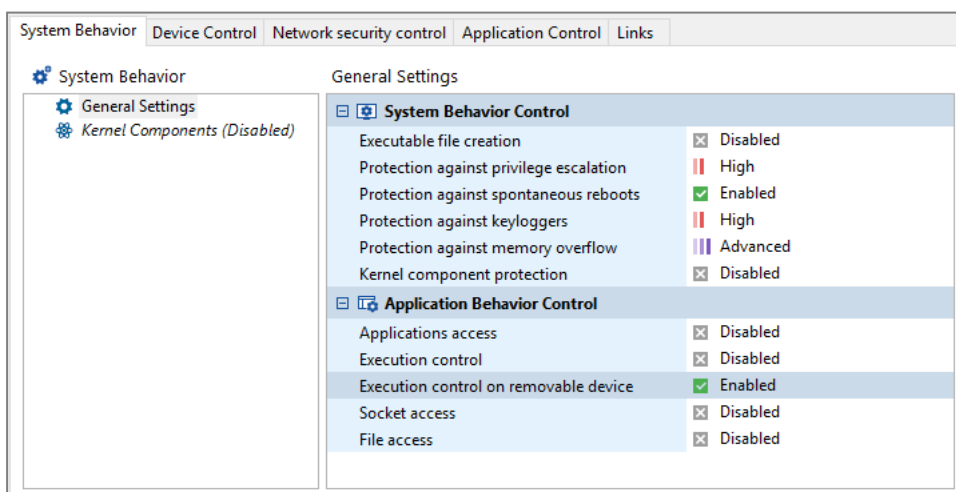
5.1 Configuring SES in a day

If you wish to complete your first configuration within a single day, create a security policy based on the basic template:



5.2 Configuring SES in at least two days

Select a basic policy template and add several general settings:



Application control can be used in blacklist or whitelist mode. We suggest that you use blacklist mode for the majority of endpoints to be protected. Whitelist mode can be used in environments that are very seldom modified (built-in systems, quarantined workstations with a specific application, point of sale terminals, etc.).



Using detailed logs or whitelist mode may impact performance on workstations, as processes that may be run on the workstation are closely monitored, and may therefore slow down the computer's startup phase.

5.3 Configuring system behavior control

For further detail, please refer to the *SES Administration guide*.

5.3.1 Executable file creation

- **Disabled:** low security,
- **High/Critical:** high security with the following conditions:
 - SES must be disabled every time a program is installed/updated,
 - A pre-production infrastructure must be used for the creation of rules affecting essential trusted applications.

This form of protection can be easily enabled on servers, for example RDS 2016 Servers.

5.3.2 Protection against privilege escalation

- **Disabled:** low security,
- **High:** this level is not recommended as critical mode protects better,
- **Critical:** high security with the following conditions:
 - SES should probably be disabled whenever a program is installed/updated.
 - A pre-production infrastructure must be used for the creation of rules affecting essential trusted applications.

In order to block pass-the-hash attacks (for example using the mimikatz program), the critical level is required.

5.3.3 Protection against spontaneous reboots

This protection method is recommended for servers only. Whenever this protection is used, deployment applications such as SCCM, Ninite, LANDesk, etc. must be trusted.

5.3.4 Protection against keyloggers

- **Disabled:** low security,
- **High:** high security with the following condition:
 - Rules regarding trusted applications must be created in order to allow several programs. For more information, see the section [Configuring protection against keyloggers](#).
- **Critical:** not recommended, as it generates false positives.

5.3.5 Protection against memory overflow

This is the method that provides the workstation with the best protection, and we recommend enabling it where possible. However, you may need to create several rules regarding trusted applications. For more information, see the section [Configuring protection against memory overflow](#).



5.3.6 Kernel component protection

This method is only possible if all computers use the same drivers (same hardware), and it only runs on 32-bit Microsoft Windows systems.

5.4 Configuring application behavior control

5.4.1 Applications access and Execution control

These methods require a certain number of rules to be created on trusted applications (~300), so you are advised against using them unless you are using very high security.

5.4.2 Execution control on removable devices

This method is strongly recommended if you do not block USB drives on your system.

The user has to confirm that an executable can be run from a removable device, and the response is written to the logs. A report can therefore be generated that shows what software was run from USB sticks for each user.

Further examples, the following actions may set off notifications:

- If a ReadyBoost USB drive is plugged in, Windows Updates may start running .exe files on the drive,
- Barco projectors with USB connectors will ask to run the executable file: *d:\clickshare_for_windows.exe*.

5.4.3 Network access and File access

These methods require a certain number of rules to be created on trusted applications, so you are advised against using them unless you are using very high security.



6. Configuring protection against privilege escalation

Many applications require privilege escalation, which is the case for most installation programs.

WARNING

Ordinarily, the PowerShell application does not require privilege escalation in order to run (depending on the script used). Allowing PowerShell to escalate its privileges would allow a large number of malicious programs to run.

- Prohibit PowerShell,
- Or restrict PowerShell to GPO-signed scripts,
- Or restrict PowerShell to scripts in a special folder or on a file server.



7. Configuring protection against memory overflow

The following applications have been known to cause memory overflow, so trusted rules need to be applied to them. To find out how to create trusted rules in the **Application control** panel, refer to the *SES Administration guide*.

- Intel applications for Bluetooth:
 - c:\program files (x86)\intel\bluetooth\devmonsrv.exe
 - c:\program files (x86)\intel\bluetooth\mediasrv.exe
 - c:\program files (x86)\intel\bluetooth\obexsrv.exe
- TeraCopy:
 - *\teracopy.exe
- Cygwin software suite:
 - c:\cygwin64*.exe
- Several antiviruses are also capable of causing memory overflow: Symantec and Kaspersky for example.

You are strongly advised to trust the antivirus.

We suggest that you trust other applications only if they do not function with SES in Normal mode.

Web browsers Internet Explorer/Firefox/Chrome, and Adobe applications must never be trusted. If you encounter memory overflow on one of these applications, this means that a virus has just been blocked. If this is not the case, do get in touch with the SES Technical Assistance Center.



8. Configuring protection against keyloggers

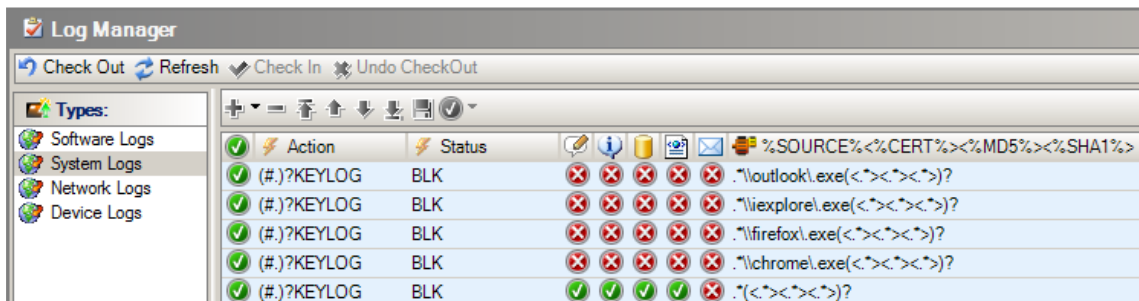
8.1 Deleting logs with false positives

Microsoft Office applications and web browsers generate keylogging events, which are considered false positives. For example:

- c:\program files\microsoft office 15\root\office15\winword.exe
- c:\program files\microsoft office 15\root\office15\excel.exe
- c:\program files\microsoft office 15\root\office15\powerpnt.exe
- c:\program files\microsoft office 15\root\office15\onenote.exe
- *clview.exe
- *skype.exe
- *Lync.exe
- c:\program files\internet explorer\iexplore.exe
- c:\program files [x86]\google\chrome\application\chrome.exe
- c:\program files [x86]\mozilla firefox\firefox.exe
- Windows Live

We advise against trusting such applications. In the **Log Manager** panel you can hide these false positive entries from the logs. This will avoid queries from users who will no longer see these alerts.

For example:



We suggest that you include clear comments to explain such a configuration if several administrators have access to the console.

8.2 Allowing keyboard shortcuts

Keyboard shortcuts are combinations of keys that allow, for example, increasing or decreasing volume.

On Dell computers the following program logs keystrokes:

- c:\program files\delltpad\apmsgfwd.exe

On Hewlett-Packard computers:

- c:\program files [x86]\hewlett-packard\hp mainstream keyboard\cnhkey.exe
- c:\program files [x86]\hewlett-packard\hp mainstream keyboard\modledkey.exe



We recommend trusting these applications if you trust the hardware vendor. Trusted rules must therefore be created in **Application control**.

8.3 Allowing virtual environments

Virtual environments (VMWare, Citrix, etc.) take control of virtual machines. Such applications must be trusted, for example:

- c:\program files [x86]\vmware\vmware workstation\x64\vmware-vmx.exe

8.4 Allowing TeamViewer, DameWare, VNC, etc.

Remote control tools log keystrokes, for example:

- c:\program files [x86]\teamviewer\teamviewer_desktop.exe
- c:\program files [x86]\teamviewer\tv_x64.exe
- c:\program files [x86]\teamviewer\tv_w32.exe

These applications must be trusted if users wish to remotely take control of a computer. Depending on the situation, or for security reasons, it may be better to block such applications.

8.5 Allowing videoconference tools

Some videoconference tools (e.g.: Skype, WebEx, GoToMeeting) make it possible to remotely control computers, for example:

- c:\program files\skype\phone\skype.exe

We recommend trusting such applications.

8.6 Allowing Common Desktop Agent and all other programs

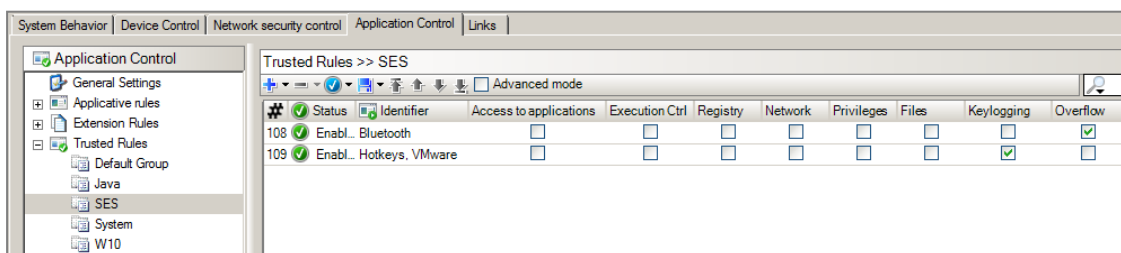
If you have a Samsung printer, for example, you would have the following program:

- c:\program files\common files\common desktop agent\cdasrv.exe

Test the program with SES in Normal mode. If it does not work, create a trusted rule in SES.

8.7 Expected result

The configuration of your security policy should therefore resemble the following configuration:





9. Allowing and blocking file extensions

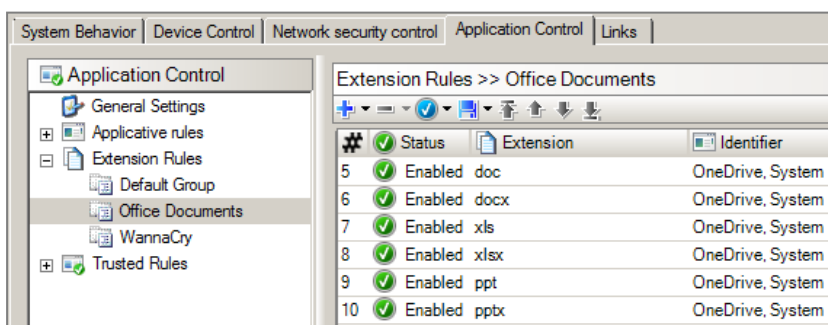
If you have used the basic security policy template:

- Add the antivirus permission for the extension *.pst* so that the antivirus can detect viruses in your mail,
- Block multimedia extensions in order to reduce the amount of CPU resources used by TSE servers.

Block the following application extensions if possible:

Extension	Use
docm	Macro-enabled document
dotm	Macro-enabled template. Warning, these are used by Outlook, Word, Excel, etc. Allow <i>normal.dotm</i> in the application rules, and block <i>*.dotm</i> .
hta	HTML Program Format
pif	Windows Program Information File for dos programs
pptm	Macro-enabled presentation
potm	Macro-enabled template
ppam	Macro-enabled add-in file
ppsm	Macro-enabled slide show
sldm	Macro-enabled slide
torrent	Torrent files
vbe	Visual Basic Editor
vbs	Visual Basic Scripting. Warning: scripts may use this when a Windows session is opened, for example. In such cases, <i>vbs</i> scripts must be allowed in <i>cscript.exe</i> application rules, and <i>*.vbs</i> must be blocked.
xlsm	Macro-enabled workbook
xltm	Macro-enabled template
xlam	Macro-enabled add-in file
wsf	Windows Script File
wsh	Windows Scripting Host

To prevent abnormal processes from accessing Microsoft Office documents, allow only specific applications to access Office documents, for example:



The "System" ID corresponds to the following files:

Type	Value	Description
Path / Certificate	c:\program files*	Program Files x64
Path / Certificate	c:\program files (x86)*	Program Files x32
Path / Certificate	c:\windows*	Windows
Path / Certificate	"\setup".exe - Microsoft Corporation.cer (Microsoft Code Signing PCA) (Microsoft Code Signing PCA) (Microsoft Code Signing PCA) (Microsoft Code Signing PCA) Setup	



9.1 Expected result

The configuration of extension-based protection in your security policy should therefore resemble the following configuration:

Extension Rules >> Dangerous				
	Status	Extension	Identifier	Description
11	Enabled	hta	systemroot explorer.exe	HTML Program Format
12	Enabled	vb	systemroot explorer.exe	Visual Basic Scripting
13	Enabled	vbe	systemroot explorer.exe	Visual Basic Editor
14	Enabled	vbs	systemroot explorer.exe	Visual Basic Scripting
15	Enabled	wsf	systemroot explorer.exe	Windows Script File
16	Enabled	wsh	systemroot explorer.exe	Windows Scripting Host
17	Enabled	torrent	systemroot explorer.exe	Torrent
18	Enabled	scr	systemroot explorer.exe systemroot system32\rundll32.exe Screensavers	Screensavers
19	Enabled	pif	systemroot explorer.exe	Program Information File (for DOS programs)
20	Enabled	jse	systemroot explorer.exe	JScript Encoded Script File
21	Enabled	msc	systemroot explorer.exe systemroot system32\consent.exe systemroot system32\mmc.exe	Microsoft Management Console Snap-in Control File



10. Blocking viruses that spread easily

10.1 Blocking exe and js files with a misleading extension

In Windows group policies (GPO), we recommend that you do not hide known extensions.

Viruses can hide behind double extensions to fool the user and thus spread easily. For example:

- .pdf.exe
- .pdf.js
- .pdf.rtf

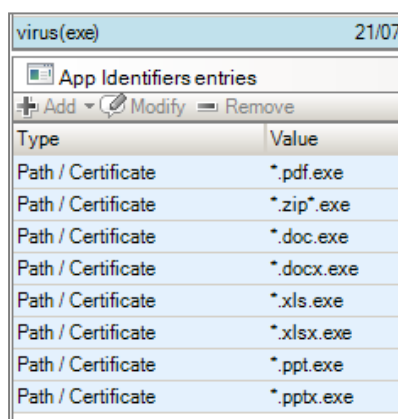
To block this possibility, apply the following recommendations.

10.1.1 Preventing execution of files with double extensions ending .exe

To prevent execution of files with double extensions .xxx.exe and which may contain viruses, follow the procedure below:

Application identifiers

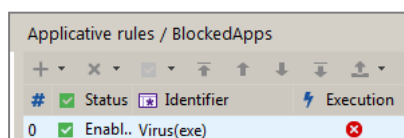
Create a "Virus" application identifier that groups the following misleading extensions:



Type	Value
Path / Certificate	*.pdf.exe
Path / Certificate	*.zip*.exe
Path / Certificate	*.doc.exe
Path / Certificate	*.docx.exe
Path / Certificate	*.xls.exe
Path / Certificate	*.xlsx.exe
Path / Certificate	*.ppt.exe
Path / Certificate	*.pptx.exe

Applicative rules

Prohibit the execution of the identifiers created earlier:

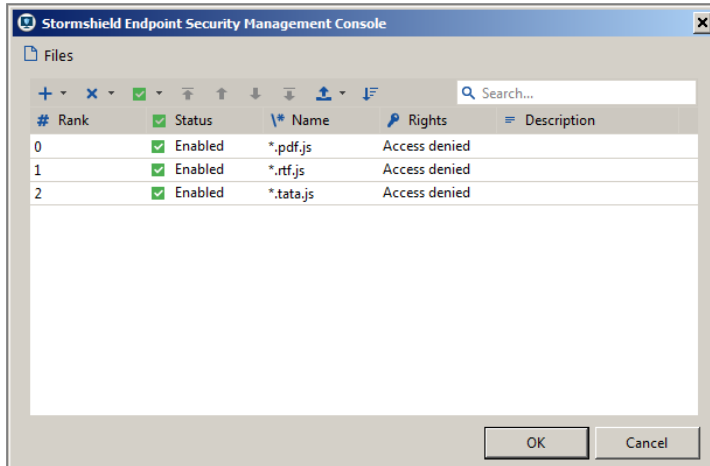
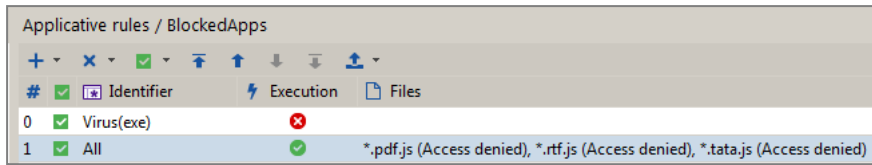


#	Status	Identifier	Execution
0	Enabl.	Virus(exe)	

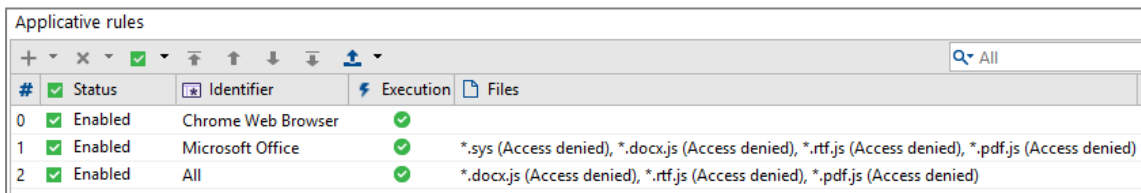
10.1.2 Preventing files with double extensions ending .js from being read

To prevent files with double extensions .xxx.js and which may contain viruses from being read or activated, follow the procedure below:

1. Select the identifier **All** and add each double extension ending .js to the **File** column with "Access Denied" rights in the sub-rules:



2. If a rule preceding the **All** rule already contains specific **Files** sub-rules, you need to add the double extensions which must be blocked in this rule as well. It is not enough to specify these extensions in the **All** rule because the agent stops browsing rules as soon as it finds one which matches the running process and which has **Files** sub-rules (whether they match the targeted resource or not).



10.1.3 Preventing files with double extensions ending .rtf from being read

To prevent files with double extensions ending `.rtf` from being read, you must create an applicative rule similar to the rule described in the previous section about `.js` extensions. You can also complete the sub-rules in the rule previously created for `.js` files.

However, when WordPad or any other application allowing `.rtf` files to be read is not able to open a file with its normal name, it uses the Windows “short names” [or 8.3 file names].

For example the name *file.pdf.rtf* becomes *filepd~1.rtf*.

The double extension is then hidden by the short name and the applicative rule is not sufficient. It will not be applied because the double extension will not be recognized.

To prevent these types of double extensions to be read, you need to:

1. Create an applicative rule similar to the rule described in the previous section about `.js` extensions.
2. Disable the Windows 8.3 format using the command `fsutil.exe behavior set disable8dot3 1` from the command prompt opened as administrator.

Only files created after issuing the command will be affected. Those created prior will continue to support the short (8.3) filename and thus will not be blocked.



If you are unable to disable the 8.3 file format or you need to block files already created with this option active, then you can add the files to block to the previously created rule for *.js* files using the format **~*.rtf*.

Applicative rules			
#	Identifier	Execution	Files
0	Virus(exe)	✗	
1	All	✓	*.pdf.js (Access denied), *.rtf.js (Access denied), *.tata.js (Access denied), *.pdf.rtf (Access denied), *~*.rtf (Access denied)

Stormshield Endpoint Security Management Console					
Files					
#	Rank	Status	Name	Rights	Description
0		✓ Enabled	*.pdf.js	Access denied	
1		✓ Enabled	*.rtf.js	Access denied	
2		✓ Enabled	*.tata.js	Access denied	
3		✓ Enabled	*.pdf.rtf	Access denied	
4		✓ Enabled	*~*.rtf	Access denied	

- If a rule preceding the **All** rule already contains specific **Files** sub-rules, you need to add the double extensions which must be blocked in this rule as well. It is not enough to specify these extensions in the **All** rule because the agent stops browsing rules as soon as it finds one which matches the running process and which has **Files** sub-rules (whether they match the targeted resource or not).

Applicative rules				
#	Status	Identifier	Execution	Files
0	✓ Enabled	Chrome Web Browser	✓	
1	✓ Enabled	Microsoft Office	✓	*.sys (Access denied), *.docx.js (Access denied), *.rtf.js (Access denied), *.pdf.js (Access denied)
2	✓ Enabled	All	✓	*.docx.js (Access denied), *.rtf.js (Access denied), *.pdf.js (Access denied)

10.2 Restricting the capabilities of Windows scripts

- wscript.exe* runs *js* javascripts, but must not create **.exe* files.
- cscript.exe* runs *vbs* vbscripts, but must not create **.exe* files.

It would be impractical to block *js* files in file extensions, as this extension is widely used by websites and therefore by web browsers.

By double-clicking on a *js* file in a file explorer, it will be opened in Wscript.

It would be possible to block vbscripts with the file extension protection, but blocking *cscript* makes it possible to block *vbs* scripts that have extensions other than *vbs*.



10.2.1 Application identifiers

scripts	01/09/2016 11:23:54	0
App Identifiers entries		
+ Add ▾ ✎ Modify ➡ Remove		
Type	Value	
Path / Certificate	c:\windows\system32\cscript.exe	
Path / Certificate	c:\windows\syswow64\cscript.exe	
Path / Certificate	c:\windows\system32\wscript.exe	
Path / Certificate	c:\windows\syswow64\wscript.exe	

10.2.2 Application rules

63	✓	Enabl... scripts	✓	**.bat (Creation denied) **.vbs (Creation denied) **.com (Creation denied) **.dll (Creation denied) **.exe (Creation denied) **.scr (Access denied) **.sys (Creation denied)
----	---	------------------	---	---

10.3 Restricting the capabilities of Microsoft Office applications

Files with a *.dotm* extension are macro-enabled document templates. Such files cannot be blocked with extension rules as Microsoft Outlook and Word use *.dotm* files for default templates.

You therefore need to allow *.dotm* files relevant to Microsoft Outlook and Word, and prohibit other *.dotm* files.

10.3.1 Application identifiers

Word Excel Powerpoint OneNote	12/07/20
App Identifiers entries	
+ Add ▾ ✎ Modify ➡ Remove	
Type	Value
Path / Certificate	*\winword.exe
Path / Certificate	*\excel.exe
Path / Certificate	*\powerpnt.exe
Path / Certificate	*\onenote.exe
Path / Certificate	*\onenotem.exe

Outlook	01/0
App Identifiers entries	
+ Add ▾ ✎ Modify ➡ Remove	
Type	Value
Path / Certificate	*\outlook.exe



10.3.2 Application rules

Word Excel Powerpoint OneNote		c:\users*\appdata\roaming\microsoft\templates* (Access authorized (execute)) c:\users*\appdata\roaming\microsoft\office\recent* (Access authorized (execute)) *.dotm (Access denied) *.sys (Creation denied) *.vbs (Creation denied) *.js (Creation denied) *.dll (Creation denied) *.exe (Creation denied) *.com (Creation denied) *.scr (Creation denied)
-------------------------------	--	--

An application rule for Microsoft Outlook already exists, but it can be modified as follows to block malicious *.dotm* files:

c:\users*\appdata\roaming\microsoft\templates*.dotm (Access authorized (execute)) *.dotm (Access denied) c:\program files (x86)\mozillafirefox\firefox.exe (Access authorized (execute)) *imapisvc.inf (Access authorized (execute)) c:\program files\microsoft office 15\root\office15\groove.exe (Access authorized (execute)) *acrobat.exe (Access authorized (execute)) *acrord32.exe (Access authorized (execute)) programfiles\microsoft office* (Access authorized (execute)) *.ade (Access denied) *.adp (Access denied) *.asx (Access denied) *.bas (Access denied) *.bat (Access denied) *.chm (Access denied) *.cmd (Access denied) *.com (Access denied) *.cpl (Access denied) *.exe (Creation denied)

If **Creation denied** is selected for the extension **.exe* instead of **Access denied**, this will save you from having to create many rules.

10.4 Restricting screensavers to those installed by Microsoft Windows

As many viruses are concealed in screensavers, we recommend that you restrict screensavers to only those installed natively by Microsoft.

10.4.1 Application identifiers

Screensavers		12/09/2016 15:22:
App Identifiers entries		
+ Add - Modify - Remove		
Type	Value	
Path / Certificate	c:\windows\system32*.scr	

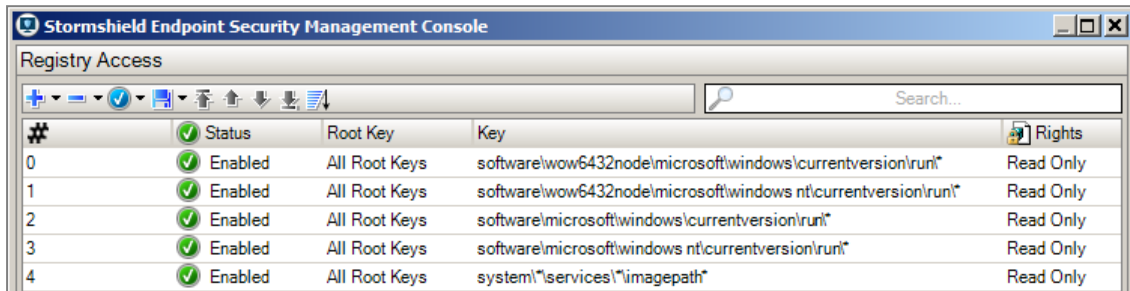
10.4.2 Extension rules

	Enabled scr	systemroot \system32\rundll32.exe Screensavers
--	-------------	---



11. Blocking persistent malware

Malware programs are saved in registry keys so that they can be launched the next time Microsoft Windows is run. To prevent this from happening, you need to prevent all programs (= "*"") from being able to write in the following registry keys:



The screenshot shows the 'Stormshield Endpoint Security Management Console' window. The 'Registry Access' tab is active, displaying a table of registry keys and their access permissions. The table has columns for '#', 'Status', 'Root Key', 'Key', and 'Rights'. All listed keys are 'Enabled' and have 'Read Only' rights.

#	Status	Root Key	Key	Rights
0	Enabled	All Root Keys	software\wow6432node\microsoft\windows\currentversion\run*	Read Only
1	Enabled	All Root Keys	software\wow6432node\microsoft\windows\nt\currentversion\run*	Read Only
2	Enabled	All Root Keys	software\microsoft\windows\currentversion\run*	Read Only
3	Enabled	All Root Keys	software\microsoft\windows\nt\currentversion\run*	Read Only
4	Enabled	All Root Keys	system*\services*\imagepath*	Read Only

You then need to trust legitimate applications that need to be launched at startup. To do so, you need to create trusted rules for these applications and select the corresponding checkbox in the **Registry** column.

The following programs, for example, can be trusted:

- c:\windows\servicing\trustedinstaller.exe
- c:\windows\system32\wermgr.exe
- c:\windows\system32\stikynot.exe
- c:\windows\system32\services.exe
- c:\program files\windows sidebar\sidebar.exe
- c:\program files [x86]\stormshield\stormshield endpoint security agent\srservice.exe
- c:\users*\appdata\local\microsoft\onedrive\onedrive.exe
- c:\program files [x86]\dropbox\client_*\dropbox.exe
- c:\users*\appdata\roaming\zoom\bin\zoom.exe
- c:\program files [x86]\malwarebytes anti-malware\mbam.exe



12. Protecting your mailbox

The following is a list of extensions used in Microsoft Outlook:

Extension Rules				
	Status	Extension	Identifier	Description
34	Enabled	pst	"outlook.exe systemroot explorer.exe	Microsoft Outlook Mail Database
35	Enabled	ost	"outlook.exe systemroot explorer.exe	Microsoft Outlook Mail Database

Tools such as "nk2edit" make it possible to collect the email addresses of your Outlook contacts. This means that malware would also be able to do the same in order to spread to other workstations. You therefore need to prohibit access to the following folder from all applications except Outlook:

Enabled	c:\users*\appdata\local\microsoft\outlook\roamcache*	Access denied
---------	--	---------------

Applicative rules >> Desktop tools				
	Status	Identifier	Execution	Files
2	Enabled	Microsoft Office		<ul style="list-style-type: none">*.sys (Access denied)*.vbs (Read only - RX (execution allowed))*.js (Read only - RX (execution allowed))*.dll (Read only - RX (execution allowed))*.exe (Read only - RX (execution allowed))*.com (Read only - RX (execution allowed))*.scr (Read only - RX (execution allowed))*.png (Read/write - RW (execution denied))*.jpg (Read/write - RW (execution denied))*.bmp (Read/write - RW (execution denied))*.gif (Read/write - RW (execution denied))



13. Protecting passwords

If you store your passwords in a password manager, you can define an application rule to protect access to files with the extension of the manager, for example the extension *kdbx* for the KeePass password safe.



14. Creating an extension whitelist

Malicious programs such as CryptoLocker target files based on their extensions. The following is a method for protecting your data.

14.1 Identifying extensions used

For example *.doc*, *.docx*, *.xls*, *.xlsx*, *.ppt*, *.pptx*, *.dwg*, etc.

14.2 Creating extension rules in application rules

Test rules in **Warning** mode in the **Dynamic Agent Configuration** or in **Test** mode on the extension rules themselves. Next, analyze the logs and improve on the rules where necessary before switching to **Normal** mode.

Extension Rules >> Macro Office			
	Status	Extension	Identifier
7	Enabled	docm	systemroot \explorer.exe
8	Enabled	xls	systemroot \explorer.exe
9	Enabled	xltm	systemroot \explorer.exe
10	Enabled	xlam	systemroot \explorer.exe
11	Enabled	pptm	systemroot \explorer.exe
12	Enabled	potm	systemroot \explorer.exe
13	Enabled	ppam	systemroot \explorer.exe
14	Enabled	ppsm	systemroot \explorer.exe
15	Enabled	sldm	systemroot \explorer.exe

14.3 Filtering and exporting System logs

Filter logs with the status "EXT-BLK".

System Logs						
Page 1 Export As Automatic refresh Advanced filters Options						
Logs displayed: Current year Logs : 0-1000/10579 from 01/01/2017 00:00:00 to 01/01/2018 00:00:00 - (UTC+01:00) Europe de l'Ouest (heure d'été)						
Filters: Status is Add All conditions Status is EXT-BLK X						
Date	Agent Mode	Action	Status	Source path	Detail	
24/05/2017 17:30:55	Warning	OPEN	EXT-BLK	c:\program files\microsoft security client\msmpeng.exe	c:\users\sl\appdata\roaming\mozilla\firefox	
24/05/2017 17:30:54	Warning	CREATE	EXT-BLK	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\sl\appdata\roaming\mozilla\firefox	
24/05/2017 17:30:54	Warning	CREATE	EXT-BLK	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\sl\appdata\roaming\mozilla\firefox	
24/05/2017 17:30:54	Warning	OPEN	EXT-BLK	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\sl\appdata\roaming\mozilla\firefox	
24/05/2017 17:30:54	Warning	RENAME	EXT-BLK	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\sl\appdata\roaming\mozilla\firefox	
24/05/2017 17:28:25	Warning	CREATE	EXT-BLK	c:\program files (x86)\microsoft office\rootoffice16\outlook.exe	c:\users\sl\appdata\local\microsoft\window	
24/05/2017 17:28:22	Warning	CREATE	EXT-BLK	c:\program files (x86)\microsoft office\rootoffice16\outlook.exe	e:\csmda_v2_040_objects.pptx	
24/05/2017 17:28:21	Warning	CREATE	EXT-BLK	c:\program files (x86)\microsoft office\rootoffice16\outlook.exe	c:\users\sl\desktop\report generator.xslm	

Export logs in *.csv*. To obtain a more accurate policy, you can also perform the operation extension by extension.

14.4 ExtractTool

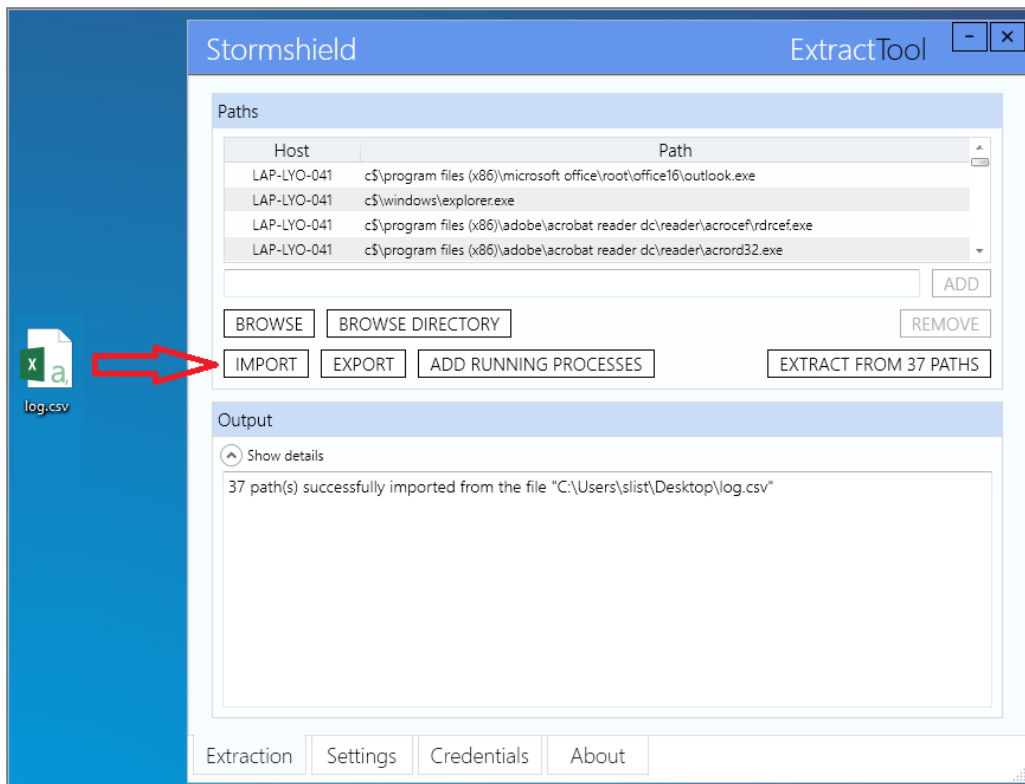
The ExtractTool allows hashing files, and/or the extraction of the path and/or extracting certificates from signed files (the digital signature can be embedded or from the Microsoft security catalogue). The resulting elements can then be imported into the SES console to create a list of application identifiers. These identifiers can then be used to create either a Black List or White List application protection security policy.

To obtain Stormshield's ExtractTool program, contact your Stormshield pre-sales engineer.



14.4.1 Importing logs

Using ExtractTool, import log files in .csv format:



14.4.2 Configuring ExtractTool in order to obtain a single identifier



Stormshield ExtractTool

Extraction parameters

Extension filters : *.cab *.cat *.ctl *.dll *.exe *.ocx *.sys *.msi *.xpi *.xap

Parallelization : 2 threads per logical processor ▾

☐ Hash files Hash algorithm : SHA1 ▾

☒ Extract signing certificates

Startup

☐ Start with Windows ☐ Extract on startup ☐ Exit after extraction

Output

Directory : C:\Users\slis\Desktop

☒ Explore to output directory after extraction

☒ Generate SES application identifier Output mode : Single ▾

Extraction Settings Credentials About

After you have completed the configuration, start the extraction by clicking on **Extract from x PATHS**.

14.5 Importing the results to the SES console

Perform the following operations in the order below:

1. Import certificates to the SES console,
2. Import application identifiers to the SES console.

14.6 Allowing applications to access extensions

This new identifier will now be able to access all the extensions defined in the security policy.



15. Blocking Internet access

It is possible to prevent almost all applications (application = "*") from accessing the Internet with the exception of a few. The following are examples of exceptions for 64-bit Windows 7/8/10 operating systems.

15.1 Allowing Windows antivirus updates

- c:\program files\windows defender\mpcmdrun.exe

15.2 Allowing web/FTP browsers

- c:\program files (x86)\internet explorer\iexplore.exe (32 bits)
- c:\program files\internet explorer\iexplore.exe (64 bits)
- c:\program files (x86)\mozilla firefox\firefox.exe (32 bits)
- c:\program files\mozilla firefox\firefox.exe (64 bits)
- c:\program files (x86)\google\chrome\application\chrome.exe
- c:\program files\filezilla ftp client\filezilla.exe

15.3 Allowing videoconferences or remote control

- c:\users*\appdata\local\citrix\gotomeeting*\g2mcomm.exe
- c:\program files (x86)\teamviewer\teamviewer.exe
- c:\programdata\webex\webex*\atmgr.exe

15.4 Allowing synchronization tools (if necessary)

- c:\program files (x86)\dropbox\client\dropbox.exe
- c:\program files (x86)\dropbox\update\dropboxupdate.exe
- c:\users*\appdata\local\microsoft\onedrive\onedrive.exe
- c:\users*\appdata\local\microsoft\onedrive*\onedrivestandaloneupdater.exe
- c:\program files (x86)\google\drive\googledrivesync.exe
- c:\program files\siber systems\goodsync\goodsync.exe

15.5 Blocking attempts by the Microsoft Office suite to access the Internet, if possible

The Microsoft Office suite accesses the Internet:

- To look for Office document templates,
- To check the validity of licenses,
- To look for viruses with Word/Excel macros, etc.



As a security measure, large corporations are strongly advised to install a Microsoft KMS (Key Management Service) license server on their LANs, and block Microsoft Office applications from accessing the Internet.

- c:\program files\microsoft office 15\root\office15\winword.exe
- c:\program files\microsoft office 15\root\office15\excel.exe
- c:\program files\microsoft office 15\root\office15\powerpnt.exe
- c:\program files\microsoft office 15\root\office15\outlook.exe

15.6 Allowing Stormshield Data Security

In order to be able to download the certificate revocation lists, SDS must be able to go on the Internet:

- c:\program files\arkoon\security box\kernel\sbkml.exe

SDS for Cloud and Mobility shares the same need to access the Internet:

- c:\users*\appdata\local\stormshield\stormshield data security\datasecurity.exe

15.7 Allowing software updates

Some examples:

- c:\program files\keepass password safe 2\keepass.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe

15.8 Prohibiting Microsoft memory dumps

The following application sends memory dumps to Microsoft whenever applications unexpectedly shut down. It must not be allowed to access the Internet:

- c:\windows\system32\wermgr.exe



16. Protecting the network

You must configure security on Microsoft Windows and on applications to protect your network.

16.1 Ports 137/138 - NetBIOS

A Microsoft Windows domain with an Active Directory in version 2008 or higher can run without NetBIOS. Ports 137 and 138 can therefore be blocked for all "recent" applications.

16.2 Port 1900 - SSDP discovery

On Microsoft Windows 7/8/10, the SSDP discovery service is enabled by default.

This may generate a large amount of SES network logs to port 1900.

You are advised to disable this service in Microsoft Windows:

- Run *services.msc* and shut down the **SSDP discovery** service: **SSDPSRV**.

Note that in Windows 8.1 and 10, the UPnP Device Host service will not start if SSDP Discovery is disabled.

16.3 Port 5355 - LLMNR

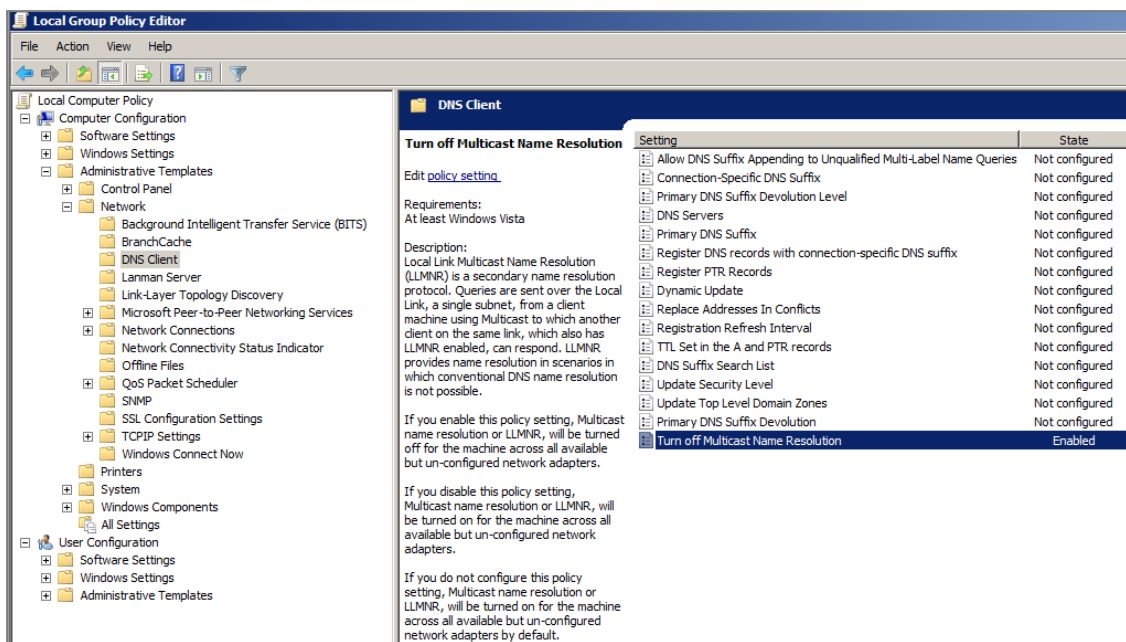
The LLMNR (Link-local Multicast Name Resolution) protocol is based on the DNS (Domain Name System) protocol. It allows computers to resolve names on the same local network without the need for a central DNS server.

On Windows 7/8/10, the LLMNR service is enabled by default.

This may generate a large amount of SES network logs to port 5355.

We suggest that you disable this service in Microsoft Windows:

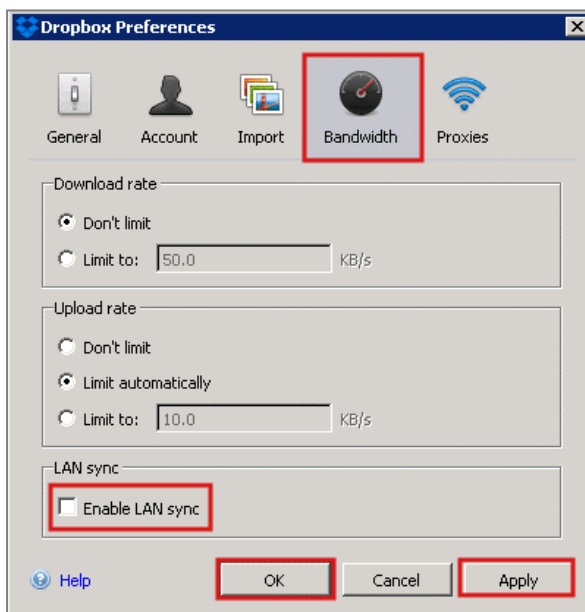
1. Enter *gpedit.msc* in the search field of the Microsoft Windows **Start** menu to open the **Local group policy editor**.
2. Browse the tree until you reach the folder **Computer configuration** > **Administrative templates** > **Network** > **DNS Client**.
3. In the parameters of the **DNS Client** folder, double-click on **Turn off multicast name resolution** and select **Disabled**.



16.4 Port 17500 - Dropbox LAN synchronization

Dropbox sends LAN synchronization frames over port 17500 to the broadcast IP address.

Synchronization can be disabled in the Dropbox client.



16.5 Port 5353 - Bonjour protocol

Apple systems and programs (such as iTunes) use the Bonjour protocol over port 5353.

With SES, network access can be denied to the application *mDNSResponder.exe*.

- For 32-bit systems:



1. Open the Microsoft Windows command prompt.
2. Enter the command `"%PROGRAMFILES%\Bonjour\mDNSResponder.exe" -remove` and confirm.
3. Enter the command `regsvr32 /u "%PROGRAMFILES%\Bonjour\mdnsNSP.dll"` and confirm.

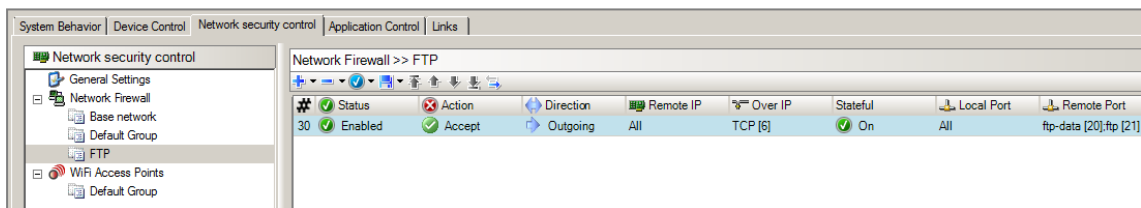
- For 64-bit systems:

1. Open the Microsoft Windows command prompt.
2. Enter the command `"C:\Program Files (x86)\Bonjour\mDNSResponder.exe" -remove` and confirm.
3. Enter the command `regsvr32 /u "C:\Program Files (x86)\Bonjour\mdnsNSP.dll"` and confirm.

After restarting, check that all of your programs run correctly and are able to access the Internet. If everything is running normally, you can rename or remove the *Bonjour* folder.

16.6 Port 21 - FTP

Firewall rules block port 21 by default, but it can be unblocked. Ensure that you place this rule at the top of the list of rules (#0) so that it will be applied.





17. Using scripts to configure a policy

The scripts below can be used in SES. They allow, for example, applying various security policies depending on the local user, time, whether a laptop or desktop is being used, etc.

17.1 Detecting the local group

This script allows finding out whether the user authenticated on the Windows session belongs to a specific local group (sent as an argument).

The following is an example of the command to be run if you wish to query the local "Administrators" group:

```
cscript.exe c:\check_admin.vbs Administrators
```

```

If Wscript.Arguments.Count < 1 Then
    Wscript.Echo "Enter the command and the local group, Ex : cscript.exe c:\check_
admin.vbs Administrators "
    Wscript.Quit(0) 'Quits and returns the value "FALSE" to SES

End If

'=====

GroupToMatch = Wscript.Arguments(0)
const separate = "\"
strComputer = "."
'=====

Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\"
& strComputer & "\root\cimv2")
Set colComputer = objWMIService.ExecQuery("Select * from Win32_ComputerSystem")

Set colGroups = GetObject("WinNT://" & strComputer & "")
colGroups.Filter = Array("group")
'=====

' Retrieving the CurrentUser
For Each objComputer in colComputer
    CurrentUserName = objComputer.UserName
Next

'=====

For Each objGroup In colGroups
    For Each objUser in objGroup.Members
        If UCase (objGroup.name) = UCase (GroupToMatch) Then
            If UCase (objUser.Name) = UCase ((Right (CurrentUserName, Len
(CurrentUserName) - Instr (CurrentUserName, separate))) then
                wscript.echo "The user: " & (Right (CurrentUserName, Len (CurrentUserName) -
Instr (CurrentUserName, separate)) & " is member of the group: " & GroupToMatch

                wscript.quit (1) 'Quits and returns the value "TRUE" to SES
            else

                If UCase (objUser.Name) = UCase (CurrentUserName) then
                    wscript.echo "The user: " & CurrentUserName & "

is part of the group: " & GroupToMatch
                    wscript.quit (1) 'Quits and returns the value "TRUE" to SES
                End if
            end if
        End if
    Next
Next

```



```
wscript.echo "The user: " & CurrentUserName & " is not member of the group " &  
GroupToMatch & " or this group does not exist"  
Next  
wscript.quit (0) 'Quits and returns the value "FALSE" to SES
```

17.2 Detecting the time

This script enables the application of a policy according to when a user is at work or off work.

```
If Hour (Now ()) >= 18 OR hour (Now ()) < 9 Then  
    Wscript.echo hour (Now()), "Rest hour"  
    Wscript.quit (1)  
Else  
    Wscript.echo hour (Now ()), "Working hour"  
    wscript.quit (0)  
End If
```

17.3 Detecting the presence of a laptop battery

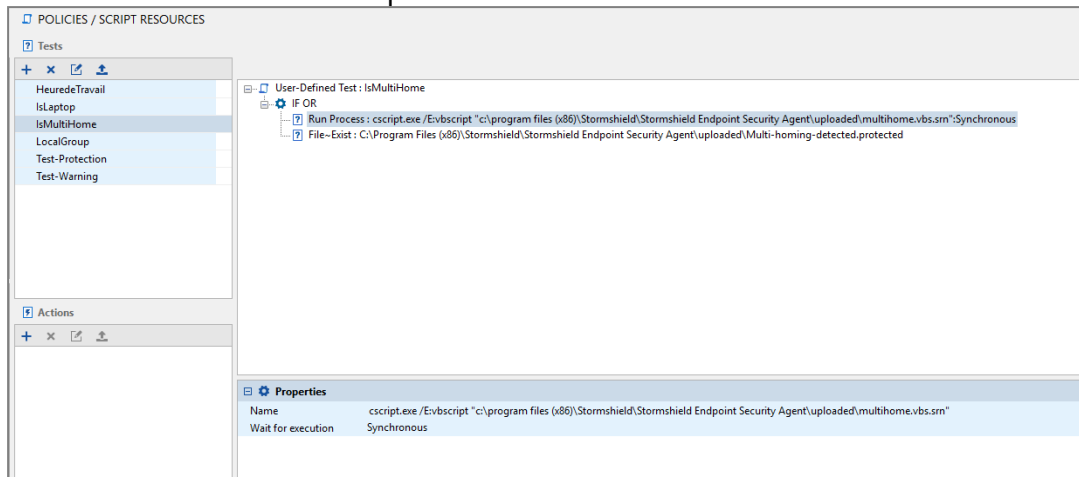
This script makes it possible to find out whether SES is being run on a laptop or desktop.

```
' Launch script with:  
' wscript.exe //d //x has_a_battery.vbs  
  
If IsLaptop (".") Then  
    WScript.Echo "Laptop"  
    wscript.quit (1) 'return true to SES  
Else  
    WScript.Echo "Desktop or Server"  
    wscript.quit (0) 'return false to SES  
End If  
  
Function IsLaptop (myComputer)  
' This Function checks if a computer has a battery pack.  
' One can assume that a computer with a battery pack is a laptop.  
'  
' Argument:  
' myComputer [string] name of the computer to check,  
' or "." for the local computer  
' Return value:  
' True if a battery is detected, otherwise False  
On Error Resume Next  
Set objWMIService = GetObject ("winmgmts://" & myComputer & "/root/cimv2")  
Set colItems = objWMIService.ExecQuery ("Select * from Win32_Battery" , , 48)  
IsLaptop = False  
For Each objItem in colItems  
    IsLaptop = True  
Next  
If Err Then Err.Clear  
On Error Goto 0  
End Function
```

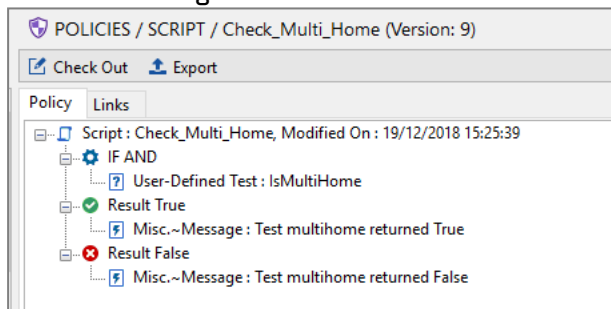
17.4 Detecting multihoming

This script makes it possible to find out whether the computer is connected simultaneously to two Internet links. If this is so, the script will create a file: *C:\Program Files [x86]\Stormshield\Stormshield Endpoint Security Agent\uploaded\Multi-homing-detected.protected*.

To run the script deployed by SES:

**1. Create a User-Defined Test in Script Resources:****2. Note the command line to run the script:**

Cscript.exe /E:Vbscript "C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Agent\uploaded\Multi-Homing-script.vbs.srn"

3. If the script runs without error it will return 0 = false. If the file exists it will return 1 = true. The IF OR test will therefore return true.**4. Create a script to implement your preferred action depending on the result. This example returns a message:**

```
'Variables
'
vGatewayProtected = "C:\Program Files (x86)\Stormshield\Stormshield Endpoint
Security Agent\uploaded\Gateway.protected" 'Can be modified / adapted
vMultiHomingProtected = "C:\Program Files (x86)\Stormshield\Stormshield Endpoint
Security Agent\uploaded\Multi-Homing-Detected.protected" 'Can be modified /
adapted
'
'List default gateways
'
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\." & strComputer & "\root\CIMV2")
Set colItems = objWMIService.ExecQuery("SELECT * FROM Win32_
NetworkAdapterConfiguration Where IPEnabled = True")
Set oFso = WScript.CreateObject("Scripting.FileSystemObject")
Set GatewayProtectedFile = oFso.CreateTextFile(vGatewayProtected, True)
'
For Each objItem In colItems
    strDefaultIPGateway = Join(objItem.DefaultIPGateway, ",")
    GatewayProtectedFile.WriteLine(strDefaultIPGateway)
Next
'
'Count the number of default gateway address in the Gateway.protected file
'
Const ForReading = 1
Set oReg = New RegExp
Set oFso = CreateObject("Scripting.FileSystemObject")
```



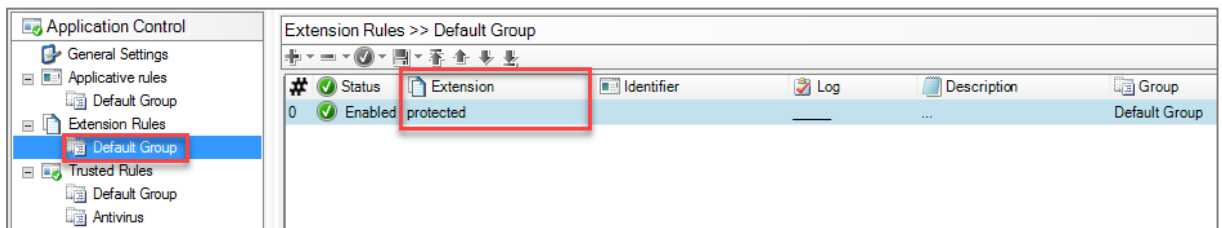
```

sData = oFso.OpenTextFile(vGatewayProtected, ForReading).ReadAll
With oReg
    .Global = True
    .Pattern = "\r\n"
    lGatewayAddressNumber = .Execute(sData).Count
End With
GatewayprotectedFile.close

Set oFex = CreateObject("Scripting.FileSystemObject")
If lGatewayAddressNumber > 1 and oFex.FileExists(vMultiHomingProtected) then
    'If the file Gateway.protected already exists do nothing
Elseif lGatewayAddressNumber > 1 then
    'If the file Gateway.protected contains 2 or more default gateway addresses then
    the file Multi-homing-detected.protected
    'is created. This value can be modified if a workstation needs more than 1
    default gateway address
    Set MultiHomingProtectedFile = oFso.CreateTextFile(vMultiHomingProtected,True)
    Dim objShell1
    Set objShell1 = CreateObject ("WScript.Shell")
    objShell1.Run ""c:\Program Files (x86)\Stormshield\Stormshield Endpoint
    Security Agent\ssusrlog.exe"" -w MULTI_HOMING_ON ""multi homing
    test""
    'This command generates a log to inform the enduser and the administrator
Else
    Set oFdo = CreateObject("Scripting.FileSystemObject")
    If oFdo.FileExists(vMultiHomingProtected) Then
        oFdo.DeleteFile(vMultiHomingProtected)
        Dim objShell2
        Set objShell2 = CreateObject ("WScript.Shell")
        objShell2.Run ""c:\Program Files (x86)\Stormshield\Stormshield Endpoint
        Security Agent\ssusrlog.exe"" -i MULTI_HOMING_OFF
        ""multi homing test""
        'This command generates a log to inform the enduser and the administrator
    End If
End If
'Removing the Gateway.protected file
Dim oFdo
Set oFdo = CreateObject ("Scripting.FileSystemObject")
oFdo.DeleteFile vGatewayProtected
Set oFso = Nothing
Set oFdo = Nothing
Set oReg = Nothing
WScript.Quit()

```

The above script uses files with a "*protected*" extension. This type of file can be protected using a file extension rule such as:





17.5 Changing configurations in a click



2 Autolt scripts (<https://www.autoitscript.com/site/autoit/>) are shown below, which allow creating/erasing a `c:\tmp\warning.txt` file that allows changing the SES configuration.

These scripts must be compiled with Autolt, and shortcuts must be created on the desktop to these .exe files.

17.5.1 Switching to normal mode

```
#include <WinAPIFiles.au3>
#include <MsgBoxConstants.au3>

;
; AutoIt Version: 3.0
; Language: English
; Platform: Win32/64
; Author: John Doe
;

Local Const $sFilePath = "C:\tmp\normal.txt"
Local $hFileOpen = FileOpen ($sFilePath, $FO_OVERWRITE)
If $hFileOpen = -1 Then
    MsgBox ($MB_SYSTEMMODAL, "", "An error occurred when writing to disk.")
    Exit
EndIf
FileClose ($hFileOpen)
FileDelete ("c:\tmp\warning.txt")
Run ("C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Agent\ssmon.exe /reconnect")
```

17.5.2 Switching to warning mode

```
#include <WinAPIFiles.au3>
#include <MsgBoxConstants.au3>

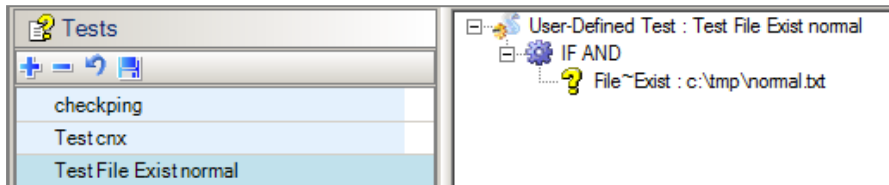
;
; AutoIt Version: 3.0
; Language: English
; Platform: Win32/64
; Author: John Doe
;

Local Const $sFilePath = "C:\tmp\warning.txt"
Local $hFileOpen = FileOpen ($sFilePath, $FO_OVERWRITE)
If $hFileOpen = -1 Then
    MsgBox ($MB_SYSTEMMODAL, "", "An error occurred when writing to disk.")
    Exit
EndIf
FileClose ($hFileOpen)
```

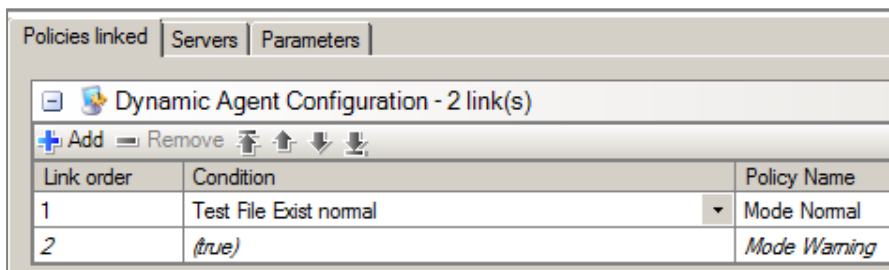


```
FileDelete ("c:\tmp\normal.txt")
Run ("C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security
Agent\ssmon.exe /reconnect")
```

17.5.3 Creating the test to check that a file exists



17.5.4 Configuring the SES environment

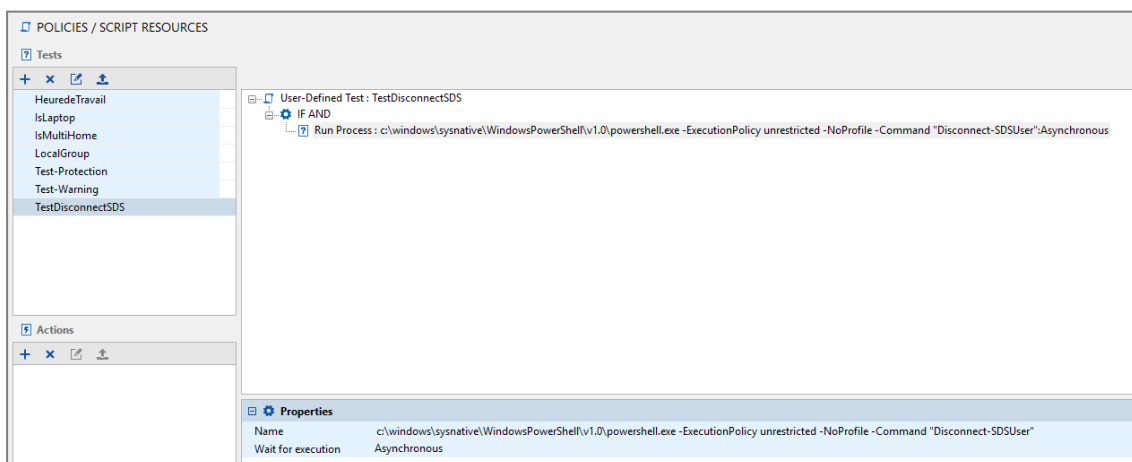


17.6 Disconnecting Stormshield Data Security Enterprise during an SES memory overflow event

If SES detects a memory overflow, the SDS Enterprise solution can be disconnected from the computer in order to prevent malicious programs from accessing for example, folders encrypted with the Stormshield Data Team module of SDS. The script will trigger and disconnect SDS when SES detects an overflow event and generates a log entry.

17.6.1 Creating the User Defined Test that disconnects SDS

This test is used to launch the script.



```
c:\windows\sysnative\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy
unrestricted -NoProfile -Command "Disconnect-SDSUser"
```

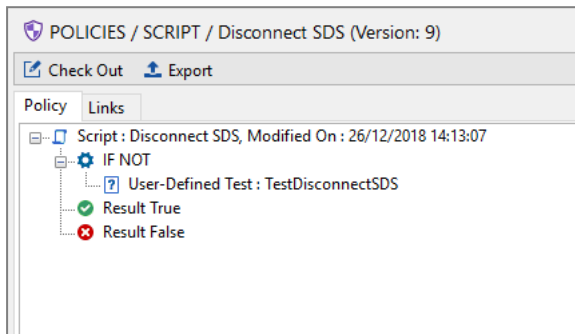
The "sysnative" directory in the path allows the script to run on 32 and 64-bit systems.



Select **Asynchronous** in the **Wait for execution** parameter.

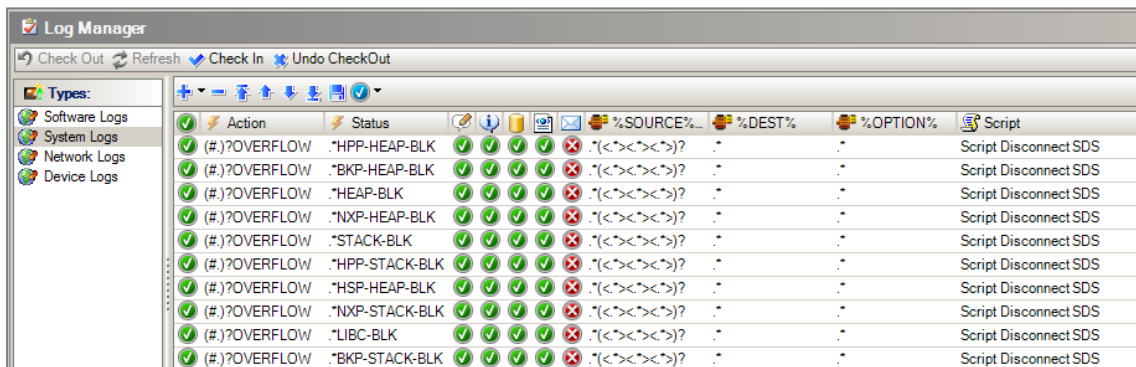
17.6.2 Creating the script that disconnects SDS

Include the User Defined Test in the script below that can then be triggered when the memory overflow event is recorded



17.6.3 Implementing the script when an event occurs

In the log configuration, the script created earlier needs to be called up:





18. Analyzing logs

The purpose of analyzing logs is to keep the amount of logs in the console as low as possible in order to retain and receive only the most relevant logs.

18.1 Disabling automatic refresh

Disable the automatic refresh option so that new lines will not be added during the actual log analysis.

18.2 Selecting the log period to be analyzed

We recommend analyzing logs from the day after you have applied the latest changes to the security policy. Refer to the **Monitoring** panel to find out the exact date.

18.3 Selecting the columns to be displayed

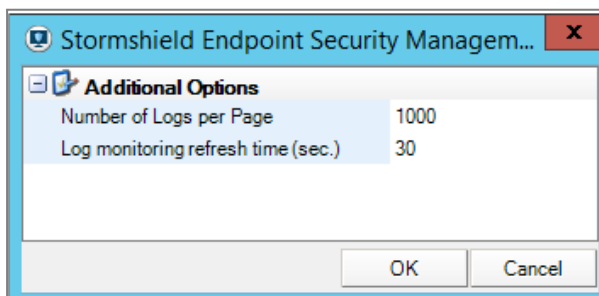
As logs tend to contain a lot of information, we recommend hiding columns that may not be useful in some cases:

- IP address
- Host name
- AD Name
- Agent ID
- Agent mode (not necessary if all computers are in the same Warning or Normal mode)
- Description
- Source MD5
- Source SHA-1
- Source sender
- RID

The **Details** and **Option** columns are very important, as they show which files and network ports are blocked, among other information.

18.4 Increasing the amount of logs per page in options

By default, 100 logs are shown per page. To avoid having too many pages, change this parameter to 1000 logs per page in the **Options** menu in the log monitoring panels.





18.5 Analyzing Action=OVERFLOW logs

The screenshot shows the 'System Logs' window. At the top, there are navigation icons, a search bar, and buttons for 'Export As', 'Automatic refresh', 'Advanced filters', and 'Options'. Below this, it says 'Logs displayed: 1 hour' and 'Logs : 0 from 11/7/2017 11:13:00 AM to 11/7/2017 12:13:00 PM - (UTC+01:00) W. Europe Daylight Time'. In the 'Filters' section, 'Action' is selected in the dropdown, and 'contains' is selected in the operator dropdown. The text 'OVERFLOW' is entered in the filter input field.

Intel Bluetooth drivers, for example, are known to cause memory overflows. No other applications must be trusted in SES. Any memory overflows that may appear in your logs would have been blocked by SES.

Using the filters in logs, you can prevent such logs from being displayed.

This screenshot shows the 'System Logs' window with the filter updated. The operator dropdown now shows 'doesn't contain'. The filter input field still contains 'OVERFLOW'. To the right of the input field is an 'Add' button. Further right, there are buttons for 'All conditions', 'Action doesn't contain OVERFLOW' (with an 'X' to remove it), and 'Action contains OVERFLOW' (with an 'X' to remove it).

18.6 Analyzing Action=KEYLOG logs

The screenshot shows the 'System Logs' window. The filter dropdown is set to 'Action' and the operator dropdown is set to 'contains'. The filter input field is empty. To the right of the input field is an 'Add' button. Further right, there are buttons for 'All conditions', 'Action is not OVERFLOW' (with an 'X'), and 'Action contains KEYLOG' (with an 'X').

Trusted rules may need to be added for keyboard shortcuts, videoconference programs, Citrix/Remoteng remote control, etc.

Using the filters in logs, you can prevent such logs from being displayed.

This screenshot shows the 'System Logs' window with two filters. The first filter is 'Action' contains 'KEYLOG'. The second filter is 'Action is not OVERFLOW' (with an 'X' to remove it). The 'All conditions' button is highlighted.

18.7 Analyzing Action=REBOOT logs

Application installers, and SCCM deployment applications for example, are applications that require reboot privileges.

Using the filters in logs, you can prevent such logs from being displayed.

The screenshot shows the 'System Logs' window with three filters. The first filter is 'Action' contains 'KEYLOG'. The second filter is 'Action is not OVERFLOW' (with an 'X'). The third filter is 'Action is not REBOOT' (with an 'X'). The 'All conditions' button is highlighted.

18.8 Analyzing Action=SU logs

In the **Details** column, you can see the type of privilege escalation, for example SE_LOAD_DRIVER_PRIVILEGE. Add a trusted rule if necessary for the application being logged.

Using the filters in logs, you can prevent such logs from being displayed.



18.9 Analyzing Action=SOCK-CONNECT logs

Such logs correspond to applications that log on to an IP address (outgoing connection).

In the **Details** column, you will be able to see the destination IP address.

In the **Option** column, you will be able to see the destination port.

Delete all logs with options with values 137/138, which correspond to the NetBIOS port.

Using the filters in logs, you can prevent such logs from being displayed.

18.10 Analyzing Action=SOCK-ACCEPT logs

Such logs correspond to applications that accept incoming connections.

In the **Details** column, you will be able to see the source IP address.

In the **Option** column, you will be able to see the port.

Delete all logs with options with values 137/138, which correspond to the NetBIOS port.

Using the filters in logs, you can prevent such logs from being displayed.

18.11 Analyzing Statut=EXT-BLK logs

Such logs correspond to attempts to access files with a particular extension.

Delete logs that correspond to non-essential Windows programs such as:

- c:\windows\system32\searchprotocolhost.exe
- c:\windows\syswow64\searchprotocolhost.exe
- c:\windows\system32\compattelrunner.exe

18.12 Analyzing remaining logs

If there are fewer than 1000 logs left, they will be displayed on the screen. The last lines of log must not be neglected, as they often highlight issues.



TIP

In application rules, software version numbers can be replaced with an asterisk ("*"), so rules will still be valid for the following versions.



19. Clearing logs

19.1 Selecting the duration of log retention

The duration of log retention may be restricted by the size of the hard disk, the size of the database (10 GB for SQL Express), or by date. In the example below, logs older than 12 months are cleared every night.

19.2 Creating an SQL script on the server

```
USE Stormshield

DELETE FROM dbo.db_SoftwareLog

WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())

DELETE FROM dbo.db_SystemLog

WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())

DELETE FROM dbo.db_NetworkLog

WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())

DELETE FROM dbo.db_MediaLog

WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())
```

19.3 Creating a bat script on the server that calls up the SQL script

Ensure that you use the right path, as the folder may be 90, 100, 110, etc depending on the version of SQL.

```
@echo off

REM Uses the SA account to log on (the password must be in plaintext in the
batches)

REM Method not recommended.

@echo on

"C:\Program Files\Microsoft SQL Server\100\Tools\Binn\sqlcmd.exe" -S
127.0.0.1\Stormshield,1433 -U SA -P P@ssw0rd -i
c:\data\stormshield\purge_logssql.sql

@echo off

REM Uses the privileges of the account that runs the batch (requires an admin
account)

REM Recommended method.

@echo on

"C:\Program Files\Microsoft SQL Server\90\Tools\Binn\sqlcmd.exe" /E -S
127.0.0.1\Stormshield,1433 -i c:\data\stormshield\purge_logssql.sql
```

19.4 Creating a scheduled task

Create a scheduled task that runs the *bat* script every night. Ensure that the user has access privileges to SES SQL databases.



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2020. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.