HOW TO
STORMSHIELD ENDPOINT SECURITY

UPDATING WORKSTATIONS UNDER WINDOWS 10

Product concerned: SES

Document last update: February 1, 2021

Reference: ses-en-how_to_update_workstations_under_W10

Table of contents

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

Getting started

Context

Microsoft regularly releases new versions of the Windows 10 operating system. Updating to the next version may fail if your SES security policies use protection features that block some of the functions on the operating system needed for this update. Your security policies must therefore allow these applications during the update. So before you update to Windows 10, you must configure the SES security policy.

Additional steps are required if you use full disk encryption.

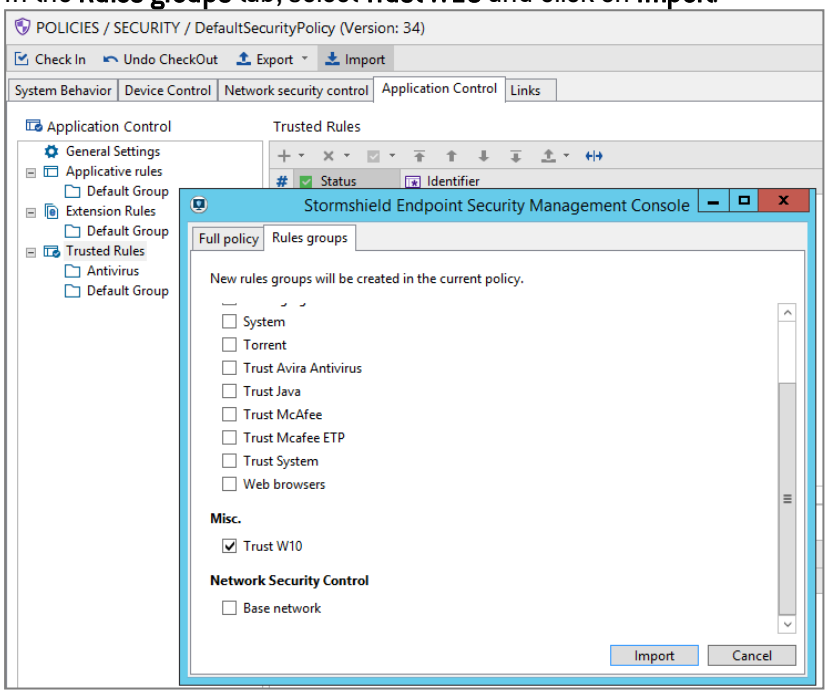
Stormshield Endpoint Security version

This procedure concerns only SES in version 7.2.32 and above, and Windows 10 in version 1607 and above.

Configuring your security policy

Stormshield provides a group of specific Windows 10 rules required for the update in the first version of SES that officially supports the Windows version in question. This rule group is called *Trust W10*. If you do not see it in your security policy, you must import it into each policy that you apply to your Windows 10 workstations.

1. Click on **Import** in the **Application control** tab of the policy.
2. In the **Rules groups** tab, select **Trust W10** and click on **Import**.



3. Deploy the modified policy on agents.
4. If you do not use full disk encryption, update your Windows 10 version as you usually would. If you use full disk encryption, follow the steps that Stormshield recommends in the next section.

Updating Windows 10

Perform this update only if you use full disk encryption. The procedure differs depending on whether the update is manual or via the Windows Update service.

Requirements

Before proceeding to update Windows 10, you must:

- Allow Stop Agent in the configuration. You can undo this authorization after the end of the update.
- Download the archive *Nep_Windows_Upgrade_Support.zip* that you can find in your MyStormshield client area in **Downloads > Stormshield Endpoint Security > 7.2 > Resources**, and copy the contents of the archive to the folder *C:\EncryptionDrivers* on all workstations concerned.
  This archive contains all the scripts that you need to set up the environment for the update.

Updating Windows 10 manually

You must have the ISO file of the new version of Windows, or the corresponding DVD.

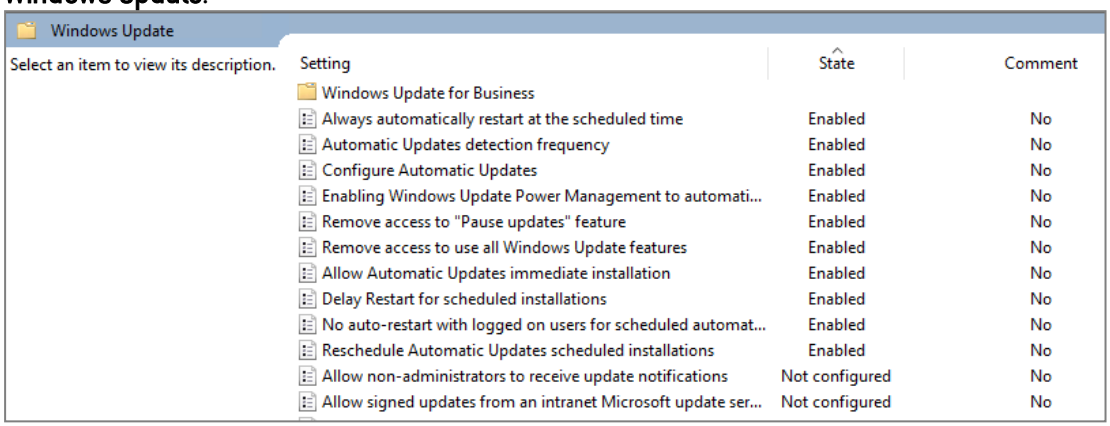
Administrator privileges are required for all operations.

1. Mount the ISO file as a DVD drive on the workstation to update, or insert the DVD into the drive. Do not allow the DVD to run automatically.
2. Allow local PowerShell scripts to be run with the command:
   ```
   Powershell Set-ExecutionPolicy RemoteSigned
   ```
3. Run the script *Install-NepWindowsUpdateConfig.ps1* found in the archive downloaded earlier. This script performs the operations required to disable SES protection features before the Windows 10 update.
4. Launch the manual update using the Windows installation DVD or its ISO image mounted as a disk. Pass the configuration file generated by the previous script as a parameter to the Windows installer:
   ```
   D:\setup.exe /ConfigFile C:\EncryptionDrivers\SetupConfig.ini
   ```
5. Restart as requested.
6. Run the following script to enable SES protection features again:
   ```
   Toggle-SESProtection.ps1 -Enable
   ```
7. Restart the workstation.

Updating Windows 10 via Windows Update

Administrator privileges are required to run all commands.

1. To speed up the installation, Stormshield recommends that you enable the following parameters in **Computer configuration > Administrative Template > Windows Components > Windows Update**:



   - Reduce the parameters **Delay Restart For Scheduled installations** and **Reschedule Automatic Updates scheduled installations** to the minimum duration (1 minute).
   - For the **Configure Automatic Updates** parameter, select **Auto download and schedule the install**.

2. Before you update Windows 10, you must install the script *Start-StormshieldWindowsUpdate* on the workstation. Run the following command:

```
Setup.cmd
```

   This script makes it possible to monitor whether Windows will be updated to a higher version.

3. When the Windows update is available, restart the workstation to search for and install updates.

> **TIP**
> You can manually launch the search for updates and install them without restarting beforehand, by running the command `Start.cmd`.

4. The Stormshield script will automatically uninstall after the second restart, which follows up on the installation of the new Windows version. If you wish to uninstall manually, run the following command before restarting the workstation:

```
Uninstall.cmd
```

documentation@stormshield.eu