

## Evoting – Basic installation and hardening

Version 1.9  
Windows image documentation

Date 2025-06-23

### Prerequisites

To create the image, the technician PC needs the following applications

AnyBurn	<a href="https://www.anyburn.com/download.php">https://www.anyburn.com/download.php</a>
Rufus	<a href="https://rufus.ie/de/">https://rufus.ie/de/</a>
Windows ADK	<a href="https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install">https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install</a>
HP Image Assistant	<a href="https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPIA.html">https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPIA.html</a>
Lenovo Update Retriever	<a href="https://support.lenovo.com/ch/en/solutions/ht037099-download-thinkvantage-technologies-administrator-tools">https://support.lenovo.com/ch/en/solutions/ht037099-download-thinkvantage-technologies-administrator-tools</a>

### Create packages

#### Software

##### 7zip

64-Bit MSI from <https://www.7-zip.org/download.html>

##### GMP

This installer is provided by the customer

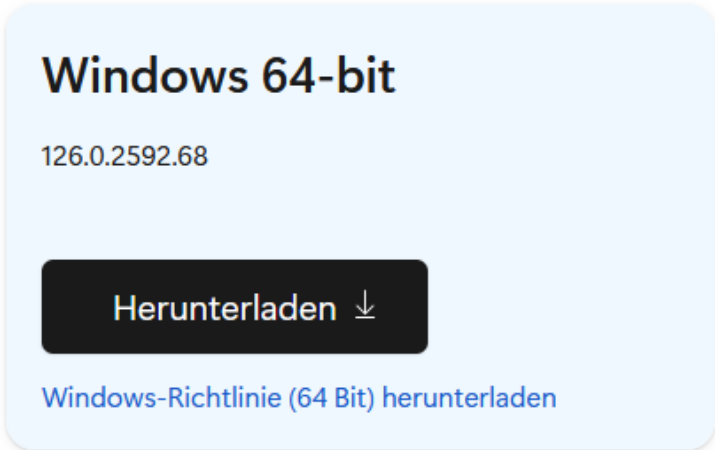
##### KeePass

Version 2.xx Setup from <https://keepass.info/download.html>

##### KeyStore Explorer

On <https://keystore-explorer.org/downloads.html> download the newest Windows setup (including JRE)

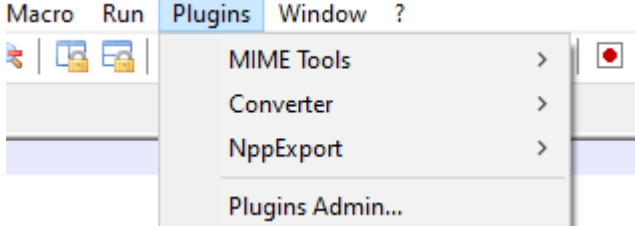
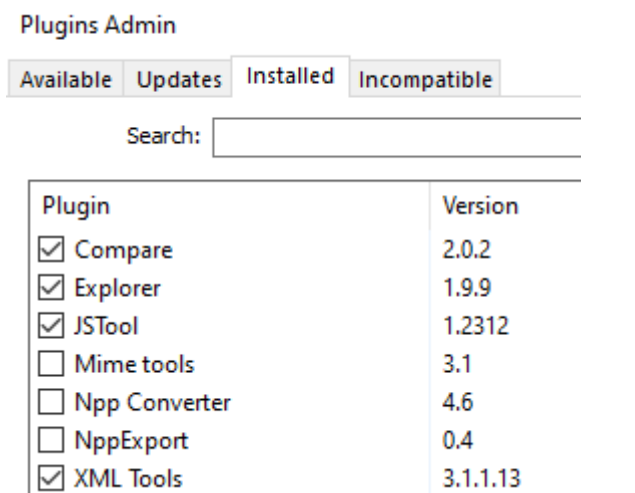
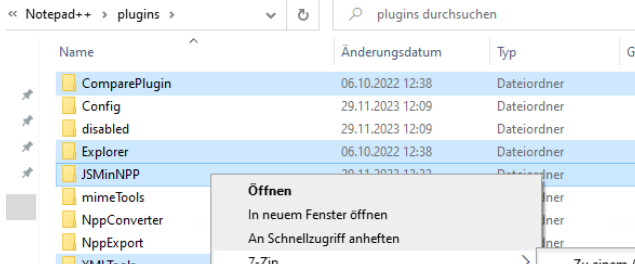
##### Edge

	<p><a href="https://www.microsoft.com/de-de/edge/business/download">https://www.microsoft.com/de-de/edge/business/download</a></p> <p>Download 64-bit package</p>
---	---

##### Notepad++

Newest 64-Bit installer from <https://notepad-plus-plus.org/downloads/>

## Notepad++ Plugins

 <p>The screenshot shows the 'Plugins' menu in Notepad++. The menu items are: MIME Tools, Converter, NppExport, and Plugins Admin... The 'Plugins Admin...' option is highlighted.</p>	<p>On a test computer, install Notepad++ and start Plugins Admin</p>																
 <p>The screenshot shows the 'Plugins Admin' window. The 'Installed' tab is selected. A search bar is at the top. Below it is a table with columns 'Plugin' and 'Version'.</p> <table border="1"> <thead> <tr> <th>Plugin</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Compare</td> <td>2.0.2</td> </tr> <tr> <td><input checked="" type="checkbox"/> Explorer</td> <td>1.9.9</td> </tr> <tr> <td><input checked="" type="checkbox"/> JSTool</td> <td>1.2312</td> </tr> <tr> <td><input type="checkbox"/> Mime tools</td> <td>3.1</td> </tr> <tr> <td><input type="checkbox"/> Npp Converter</td> <td>4.6</td> </tr> <tr> <td><input type="checkbox"/> NppExport</td> <td>0.4</td> </tr> <tr> <td><input checked="" type="checkbox"/> XML Tools</td> <td>3.1.1.13</td> </tr> </tbody> </table>	Plugin	Version	<input checked="" type="checkbox"/> Compare	2.0.2	<input checked="" type="checkbox"/> Explorer	1.9.9	<input checked="" type="checkbox"/> JSTool	1.2312	<input type="checkbox"/> Mime tools	3.1	<input type="checkbox"/> Npp Converter	4.6	<input type="checkbox"/> NppExport	0.4	<input checked="" type="checkbox"/> XML Tools	3.1.1.13	<p>Install «Compare», «Explorer», «XML Tools» and «JSTool»</p>
Plugin	Version																
<input checked="" type="checkbox"/> Compare	2.0.2																
<input checked="" type="checkbox"/> Explorer	1.9.9																
<input checked="" type="checkbox"/> JSTool	1.2312																
<input type="checkbox"/> Mime tools	3.1																
<input type="checkbox"/> Npp Converter	4.6																
<input type="checkbox"/> NppExport	0.4																
<input checked="" type="checkbox"/> XML Tools	3.1.1.13																
 <p>The screenshot shows the 'plugins' folder in Notepad++. The folder contains several files: ComparePlugin, Config, disabled, Explorer, JSMinNPP, mimeTools, NppConverter, NppExport, and XMLTools. A context menu is open over the 'ComparePlugin' file, showing options: Öffnen, In neuem Fenster öffnen, An Schnellzugriff anheften, 7-Zip, and Zu einem Archiv hinzufügen...</p>	<p>Then package the four plugins as a self-extracting 7z archive</p>																

## PowerShell 7

On <https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.4> download the current LTSC channel x64 PowerShell 7.4.x MSI

## OpenSSL

On [https://wiki.overbyte.eu/wiki/index.php/ICS\\_Download#Download\\_OpenSSL\\_Binaries](https://wiki.overbyte.eu/wiki/index.php/ICS_Download#Download_OpenSSL_Binaries) download the latest Win-64 3.x version

## OpenSSL Config

On <https://github.com/openssl/openssl/tree/master/apps>, download the following three files:

- openssl.cnf
- openssl-vms.cnf
- ct\_log\_list.cnf

Then add them to a self-extracting 7-Zip file

## SDelete

Download from <https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete> and extract the 32-Bit and 64-Bit executable

## TotalCommander

Download 64-Bit Installer from <https://www.ghisler.com/download.htm>

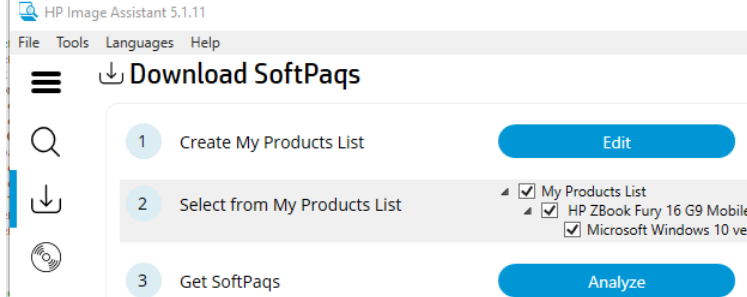
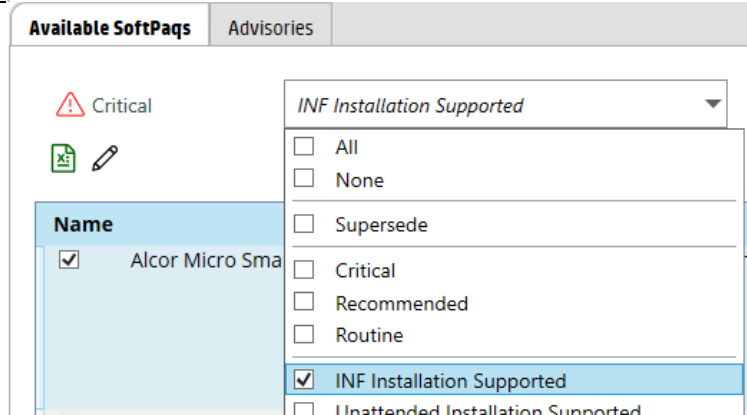
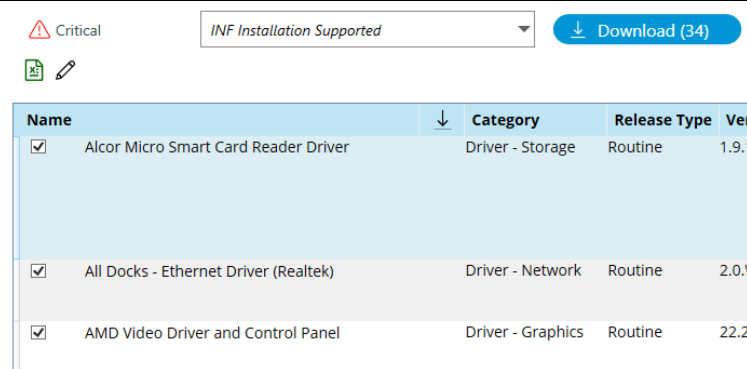
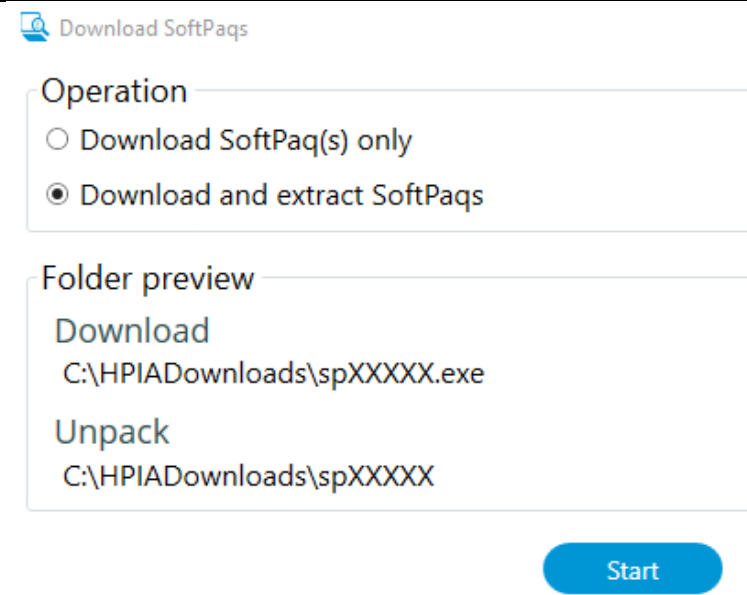
## Drivers

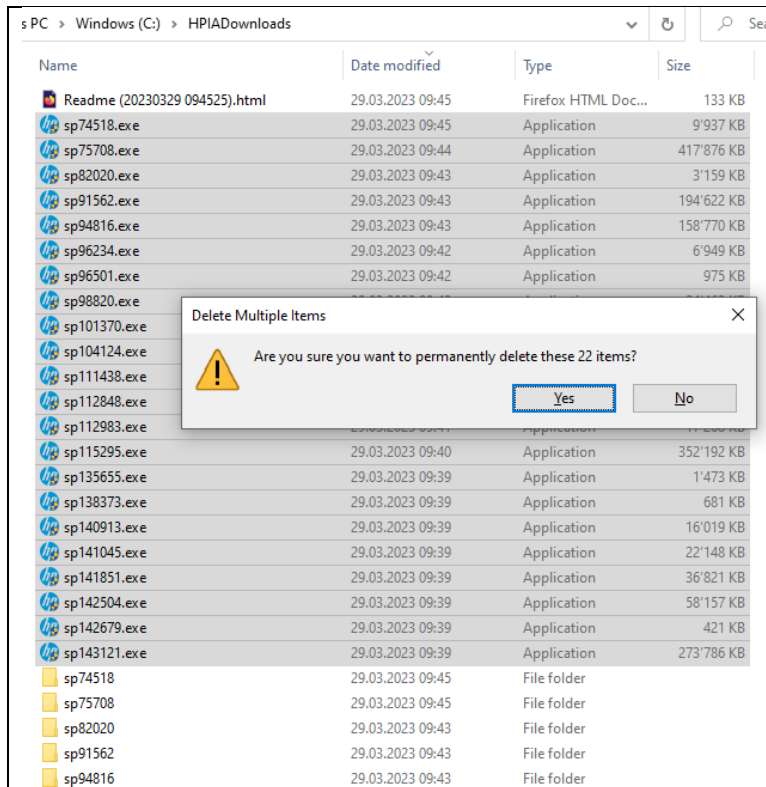
## Supported models

The following laptop models are supported, and have their drivers integrated in the image:

EliteBook 850 G5 (83B2), ZBook Fury 16 G9 (89C6), ZBook Fury 16 G10 (?), ZBook Fury 16 G11 (8CA7), ZBook Studio 16 G11 (8CF5), ThinkPad P52s (20LC), ThinkStation P8 (30HJ)

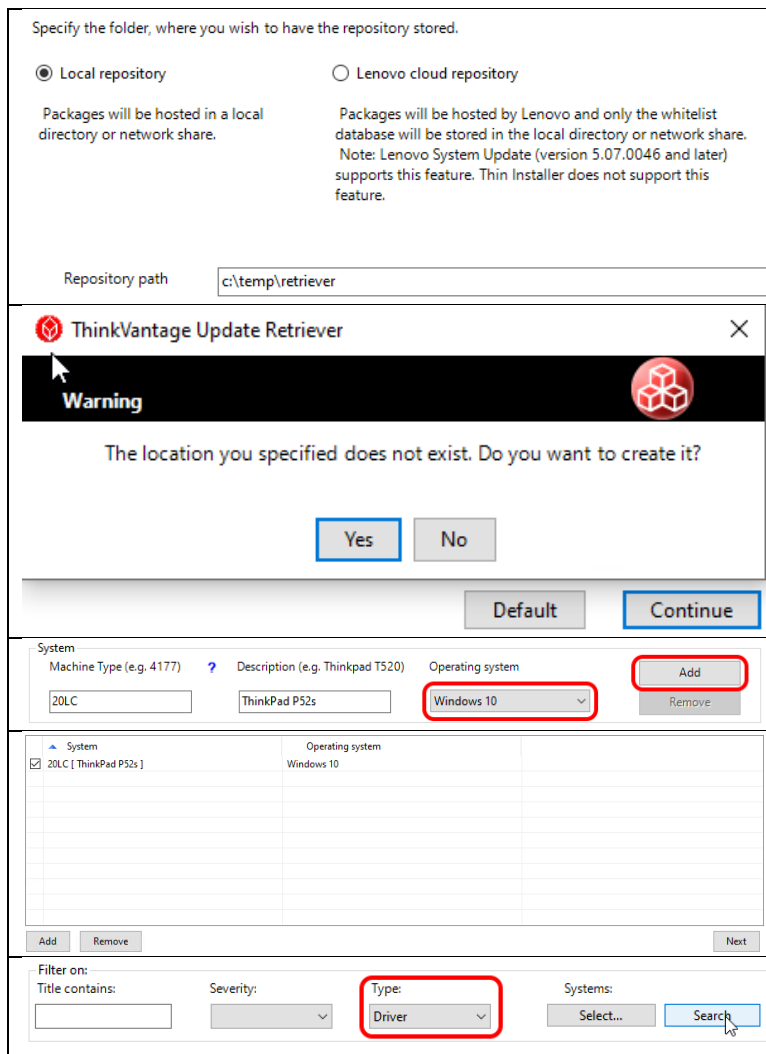
HP

	<p>Start HP Image Assistant, click on the download icon on the left, then choose "Edit Product List", and add the computer model(s) we need drivers for, then click analyse</p>
	<p>Check "Inf Install supported" to filter for only drivers (not application or BIOS)</p>
	<p>Then click "Download"</p>
	<p>Choose "Download and Extract"</p>



In the download directory, delete the driver packages, but keep the extracted directories and the readme file

## Lenovo



Start Lenovo Update Retriever, and configure the repository location to a local directory

Press "Continue", then "Yes"

Add the laptop model you want to get drivers for

Then select it and press "Next"

After the search has finished, choose "Type=Driver" and press "Search"

☒ Select All
 [View quer](#)

Title	Update ID	Severity	Type	Existing version	Version	Size
<input checked="" type="checkbox"/> Intel Dynamic Plat...	n27he01w	Recommended	Driver	-	8.3.10208.5644	3.31 MB
<input checked="" type="checkbox"/> Integrated Camera...	n27cp01w_rea	Recommended	Driver	-	10.0.16299.11319	6.70 MB
<input checked="" type="checkbox"/> Integrated Camera...	n27cp01w_sun	Recommended	Driver	-	3.5.18.32	6.70 MB
<input checked="" type="checkbox"/> Intel Bluetooth Dri...	n27wv02w	Recommended	Driver	-	20.60.0.4	1.95 MB
<input checked="" type="checkbox"/> NXP NFC Driver(W...	n27wc01w	Recommended	Driver	-	12.0.3.0	1.42 MB
<input checked="" type="checkbox"/> NXP NFC Driver (...)	n27wb01w	Recommended	Driver	-	12.0.1.0	1.66 MB
<input checked="" type="checkbox"/> NXP NFC Driver (...)	n27wa03w	Recommended	Driver	-	12.0.2.0	1.71 MB
<input checked="" type="checkbox"/> Fibocom L830-EB ...	n23wf01w	Recommended	Driver	-	3.2.0.1	1.37 MB
<input checked="" type="checkbox"/> Fibocom L830-EB ...	n23wh04w	Recommended	Driver	-	3.19041.2034.1	1.31 MB
<input checked="" type="checkbox"/> Intel Dynamic Plat...	n27hd06w	Recommended	Driver	-	8.4.11000.6436	3.51 MB
<input checked="" type="checkbox"/> Integrated Camera...	n27cd14w_rea	Recommended	Driver	-	10.0.19041.20176	20.50 MB
<input checked="" type="checkbox"/> Integrated Camera...	n27cd14w_sun	Recommended	Driver	-	5.0.18.88	20.50 MB
<input checked="" type="checkbox"/> Synaptics UltraNav...	n20gx20w	Critical	Driver	-	19.3.4.228	27.41 MB
<input checked="" type="checkbox"/> Intel Chipset Drive...	n27ic04w	Recommended	Driver	-	10.1.18228.8176	3.54 MB
<input checked="" type="checkbox"/> Intel PRO/1000 LA...	n27rw06w	Critical	Driver	-	12.18.9.11	1.57 MB
<input checked="" type="checkbox"/> Realtek Media Car...	n27x805w	Recommended	Driver	-	10.0.17134.31242	1.85 MB

Changes since last search: (+)Added (Δ)Changed (-)Removed  
 Total selected: 42 updates, 2.21 GB

☐ Hide Option  
☐ This version  
☐ This version and all future versions
 

Hide

Back

Next

Select all drivers and press "Next"

☒ Select All
 

20LC [ ThinkPad P52s ]-Windows 10

Title	Update ID	Severity	Version
<input checked="" type="checkbox"/> Alcor Smart Card Reader Driver - 10 (1703 or later)/11(...)	n27v104w	Recommended	1.7.46.1307
<input checked="" type="checkbox"/> Fibocom L830-EB Wireless WAN Driver - 10 (1709 or la...	n23wh04w	Recommended	3.19041.2034.1
<input checked="" type="checkbox"/> Fibocom L830-EB Wireless WAN Driver (Windows 10 B...	n23wf01w	Recommended	3.2.0.1
<input checked="" type="checkbox"/> Fibocom L850-GL Wireless WAN Driver - 10 (1709 or la...	n23wj37w_v1	Critical	2.0.1.112
<input checked="" type="checkbox"/> Generic DisplayLink Driver for ThinkPad USB 3.0 Ultra/...	dislink1012875	Recommended	10.1.2875.0
<input checked="" type="checkbox"/> Generic DisplayLink Driver for USB Docks and Adapter...	dislink1027042	Recommended	10.2.7042.0
<input checked="" type="checkbox"/> Integrated Camera Driver for Realtek - 10 (1709 or later...	n27cd14w_rea	Recommended	10.0.19041.20176
<input checked="" type="checkbox"/> Integrated Camera Driver for Realtek(Windows 10 Buil...	n27cp01w_rea	Recommended	10.0.16299.11319
<input checked="" type="checkbox"/> Integrated Camera Driver for Sunplus - 10 (1709 or late...	n27cd14w_sun	Recommended	5.0.18.88
<input checked="" type="checkbox"/> Integrated Camera Driver for Sunplus(Windows 10 Buil...	n27cp01w_sun	Recommended	3.5.18.32
<input checked="" type="checkbox"/> Intel 8265 Wireless LAN Driver - 10 (1809 or Later)/11(2...	n24w810w	Critical	20.70.30.1
<input checked="" type="checkbox"/> Intel 8265 Wireless LAN Driver (Windows 10 Version 18...	n24w807w	Critical	20.70.18.2
<input checked="" type="checkbox"/> Intel Bluetooth Driver - 10 (1709 or Later)/11 (21H2 or ...)	n27ww11w	Critical	22.150.0.6
<input checked="" type="checkbox"/> Intel Bluetooth Driver(Windows 10 Build 1703) - 10 [64]	n27wv02w	Recommended	20.60.0.4
<input checked="" type="checkbox"/> Intel Chipset Driver - 10 /11 (21H2 or later)	n27ic04w	Recommended	10.1.18228.8176
<input checked="" type="checkbox"/> Intel Dynamic Platform and Thermal Framework - 10 (...)	n27hd06w	Recommended	8.4.11000.6436
<input checked="" type="checkbox"/> Intel Dynamic Platform And Thermal Framework (Win...	n27he01w	Recommended	8.3.10208.5644
<input checked="" type="checkbox"/> Intel Gigabit Ethernet Driver - 10 (1809 or later)/11 (21...	n27rv06w	Recommended	12.19.1.37
<input checked="" type="checkbox"/> Intel Graphics Driver - 10 (1703 or Later)/11(21H2 or La...	n27dt22w	Critical	30.0.100.9865
<input checked="" type="checkbox"/> Intel Management Engine Software - 10 (1703 or Later)...	n27ra21w	Critical	2205.15.0.2623
<input checked="" type="checkbox"/> Intel PRO/1000 LAN Adapter Software(Windows 10 Ver...	n27rw06w	Critical	12.18.9.11
<input checked="" type="checkbox"/> Intel Serial IO Driver - 10 (1809 or Later)/11(21H2 or Lat...	n27j01w	Recommended	30.100.1841.2

42 updates, 2.21 GB

Back

Finish

"Finish"

ThinkVantage Update Retriever has finished downloading new updates

Current Results (Click link to view details):

[42 updates downloaded successfully.](#)

Wait for the downloads to finish

PC > Windows (C:) > temp > retriever > n1fupa0w

Name	Date modified	Type	Size
n1fupa0w	3/29/2023 10:07 AM	Application	4,326 KB
n1fupa0w	3/29/2023 10:07 AM	Text Document	44 KB
n1fupa0w_2	3/29/2023 10:05 AM	XML Document	11 KB

This will create a lot of directories with drivers inside executable archives

Administrator: Windows PowerShell

```

PS C:\WINDOWS\system32> ls C:\temp\retriever\*.exe -Recurse | % { $_.BaseName; & $_ /VERYSILENT "/DIR=c:\temp\retriever2\$( $_.BaseName)" /extract=yes | Out-Null }
dislink1012875
dislink1027042
n1fup99w
n20gx20w
n28pe10w
n27e118w
n27cd14w
n27cd14w
getw10ver4
n27cp01w
getw10ver4
n27cp01w
          
```

Use the following command in a window with admin rights to extract the packages:

```

ls C:\temp\retriever\*.exe -
Recurse | % { $_.BaseName; &
$_ /VERYSILENT
"/DIR=c:\temp\retriever2\$( $_.
BaseName)" /extract=yes | Out-
Null }
          
```

PC > Windows (C:) > temp > retriever2 > n1fupa0w > Comp >

Name	Date modified	Type	Size
LEPLang	3/29/2023 10:13 AM	File folder	
Resource	3/29/2023 10:13 AM	File folder	
dock_port	12/4/2022 9:57 PM	PNG File	9 KB
EasyResume	12/4/2022 10:04 PM	Application	2,298 KB
EventLogger.dll	12/4/2022 10:04 PM	Application exten...	103 KB
InstHelper.dll	12/4/2022 10:04 PM	Application exten...	169 KB
iTin.Core.dll	12/4/2022 10:05 PM	Application exten...	45 KB
Lenovo.Vantage.RpcClient.dll	12/4/2022 10:05 PM	Application exten...	31 KB

This extracts the archive to usable file collections

## Driver package adjustments

Occasionally, HP Image Assistant downloads multiple drivers for the same device. Especially if this is for a large driver such as for the video card, the older duplicate should be deleted.

For some of the laptop models, not all drivers are needed, and some must be deleted before creating the packages.

HP 850 G5:

- Delete the driver for "Conexant HD Audio Driver" (currently SP140283)
- Delete the driver for "AMD Video Driver" (currently SP142415)

HP ZBook Fury 16 G9:

- Delete the driver for "AMD Video Driver" (currently SP156134)
- Delete the driver for "Realtek HD Audio" (currently SP156237)
- Delete the driver for "Intel XMM LTE" (currently SP145803)

HP ZBook Fury 16 G10:

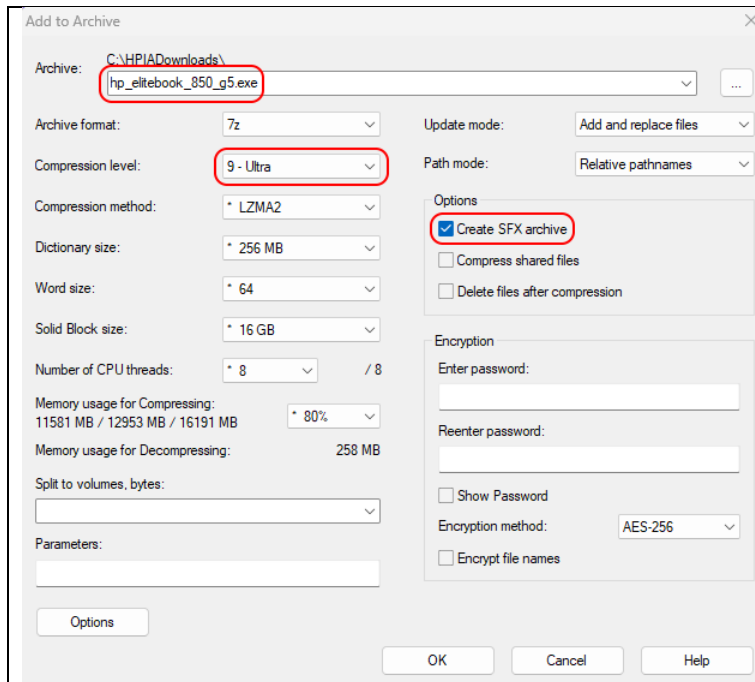
- Delete the driver for "Realtek HD Audio" (currently SP157063)
- Delete the driver for "Intel XMM" (currently SP155280)

## Create the package

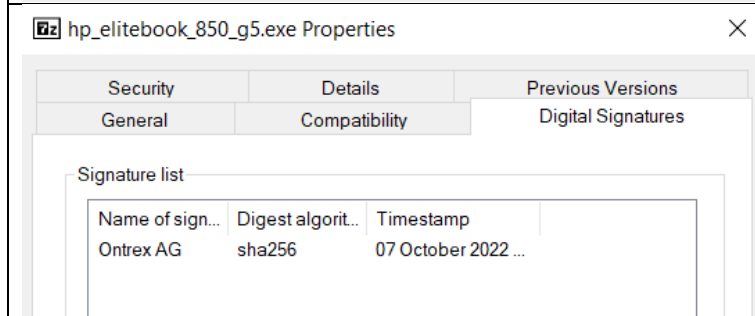
PC > Windows (C:) > HPIADownloads >

Name	Date modified	Type	Size
sp74518	29.03.2023 09:45	File folder	
sp75708	29.03.2023 09:45	File folder	
sp82020	29.03.2023 09:43	File folder	
sp91562	29.03.2023 09:43	File folder	
sp94816	29.03.2023 09:43	File folder	
sp96234	29.03.2023 09:43	File folder	
sp96501	29.03.2023 09:43	File folder	
sp98820	29.03.2023 09:43	File folder	
sp101370	29.03.2023 09:43	File folder	
sp104124	29.03.2023 09:43	File folder	
sp111438	29.03.2023 09:43	File folder	
sp112848	29.03.2023 09:43	File folder	
sp115295	29.03.2023 09:43	File folder	
sp135655	29.03.2023 09:43	File folder	
sp138373	29.03.2023 09:43	File folder	
sp140913	29.03.2023 09:43	File folder	
sp141045	29.03.2023 09:43	File folder	
sp141851	29.03.2023 09:39	File folder	
sp142504	29.03.2023 09:39	File folder	
sp142679	29.03.2023 09:39	File folder	
sp143121	29.03.2023 09:39	File folder	
Readme (20230329 094525).html	29.03.2023 09:45	Firefox HTML Doc...	133 KB

Add the extracted folders to a 7zip archive



As self-extracting archive with ultra compression level, with the name of the laptop model



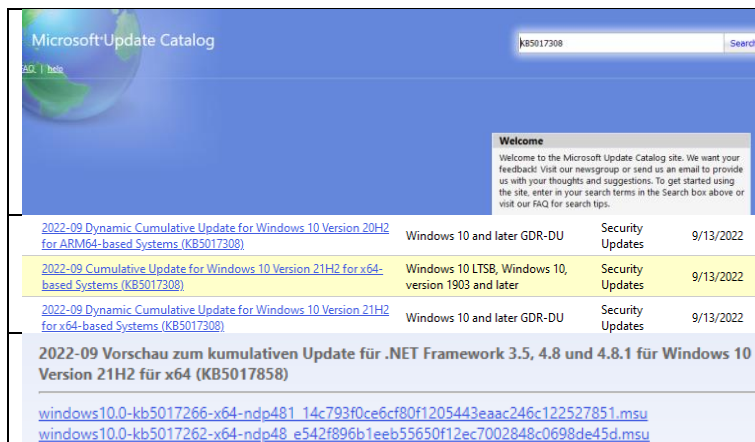
Sign the finished archive (with timestamp)

## Updates

To identify which updates are needed, set up a computer with the last image version, enable networking on it, and let it automatically run Windows Update using Microsoft Update. Write down the KB numbers of any update it's installing, then download those updates separately and integrate them into the new image version.

Then, apply the image again, and repeat the above step until Windows Update reports that no updates need to be installed on a freshly applied image.

## Windows



Go to <https://catalog.update.microsoft.com/Home.aspx> and search for the KB article numbers in the top right

For the monthly updates, download the regular cumulative update, not the dynamic one

For .NET only download the 4.8.1 package, not the 4.8

<a href="#">Windows Malicious Software Removal Tool - v5.106 (KB890830)</a>	Windows 7, Windows Server 2008	Update Rollups	10/11/2022
<a href="#">Windows Malicious Software Removal Tool x64 - v5.106 (KB890830)</a>	Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, Windows 10 LTSB, Windows Server 2016, Windows Server 2019, Windows 10, version 1903 and later, Windows Server, version 1903 and later, Windows 11	Update Rollups	10/11/2022
<a href="#">Windows Malicious Software Removal Tool - v5.106 (KB890830)</a>	Windows 8.1, Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later, Windows 11	Update Rollups	10/11/2022

## .NET Desktop Runtime 8.0.13

The .NET Desktop Runtime enables you to run existing Windows desktop applications. **This release includes the .NET Runtime; you don't need to install it separately.**

OS	Installers	Binaries
Windows	<a href="#">x64</a>   <a href="#">x86</a>   <a href="#">Arm64</a>   <a href="#">winget instructions</a>	

For the malicious software removal tool, sort by date, then pick the newest package for Windows 10 64 bit

For .NET 8, go to <https://dotnet.microsoft.com/en-us/download/dotnet/8.0> and download the newest “Desktop Runtime” for x64

## Microsoft Defender

Antimalware solution Microsoft Defender Antivirus for Windows 11, Windows 10, Windows 8.1, and Windows Server 32-bit   64-bit   ARM	On <a href="https://www.microsoft.com/en-us/wdsi/defenderupdates">https://www.microsoft.com/en-us/wdsi/defenderupdates</a> Download the 64-bit Version for the antivirus definitions
<a href="#">Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2211.5)</a> Microsoft Defender Antivirus Definition Updates 12/8/2022	For the antimalware update, download the newest "Definition Updates" package
<a href="#">updateplatform.x86fre_85dfdcc7cc8df1062fc64ae81dbe0fc3b4e20e45.exe</a> <a href="#">updateplatform.amd64fre_7f1e1eb218c67263a51f402fb080f1bbe311041b.exe</a> <a href="#">updateplatform.arm64fre_9383ac7ca8917dc66023c6ff68d3679c8285f6bc.exe</a>	Pick the one for "amd64fre"

## BIOS

2 Select from My Products List <ul style="list-style-type: none"> <li>My Products List <ul style="list-style-type: none"> <li>HP ZBook Fury 16 G10 Mobile Workstation PC</li> <li>Microsoft Windows 10 version 21H2 (64-bit)</li> <li>HP ZBook Fury 16 G9 Mobile Workstation PC</li> <li>Microsoft Windows 10 version 21H2 (64-bit)</li> <li>HP EliteBook 850 G5 Notebook PC</li> <li>Microsoft Windows 10 version 21H2 (64-bit)</li> </ul> </li> </ul> 3 Get SoftPaqs <span>Analyze</span>	For HP, select all models, then press Analyze										
<input type="text" value="bios"/>	Filter for the word "bios"										
<div> <span>Critical</span> <span>Select Components to Download/Apply</span> <span>Download (3)</span> </div> <table border="1"> <thead> <tr> <th>Name</th><th>Category</th></tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> <span>HP BIOS and System Firmware (U96)</span></td><td>BIOS - System Firm</td></tr> <tr> <td><input checked="" type="checkbox"/> <span>HP BIOS and System Firmware (V96)</span></td><td>BIOS - System Firm</td></tr> <tr> <td><input type="checkbox"/> <span>HP BIOS Config Utility (BCU)</span></td><td>Software - System</td></tr> <tr> <td><input checked="" type="checkbox"/> <span>HP Firmware Pack (Q78)</span></td><td>BIOS</td></tr> </tbody> </table>	Name	Category	<input checked="" type="checkbox"/> <span>HP BIOS and System Firmware (U96)</span>	BIOS - System Firm	<input checked="" type="checkbox"/> <span>HP BIOS and System Firmware (V96)</span>	BIOS - System Firm	<input type="checkbox"/> <span>HP BIOS Config Utility (BCU)</span>	Software - System	<input checked="" type="checkbox"/> <span>HP Firmware Pack (Q78)</span>	BIOS	Then check all the BIOS updates and click "Download"
Name	Category										
<input checked="" type="checkbox"/> <span>HP BIOS and System Firmware (U96)</span>	BIOS - System Firm										
<input checked="" type="checkbox"/> <span>HP BIOS and System Firmware (V96)</span>	BIOS - System Firm										
<input type="checkbox"/> <span>HP BIOS Config Utility (BCU)</span>	Software - System										
<input checked="" type="checkbox"/> <span>HP Firmware Pack (Q78)</span>	BIOS										





er PC
> Windows (C:)
> temp2
> GPOs

Name	Änderungsdatum	Typ
{4B6589C2-0290-4764-8058-9825B56B4169}	04.10.2022 09:04	Dateiordner
{7AD4F62E-9296-4FEA-9765-C4E3EEAAE...	04.10.2022 09:04	Dateiordner
{23DEF82E-039F-40D5-BBCC-35444958D0...	04.10.2022 09:04	Dateiordner
{B669E0C6-C1E3-4582-B797-FE384B21CD...	04.10.2022 09:04	Dateiordner
{B697C660-A87B-4AF1-B37D-9440912605...	04.10.2022 09:04	Dateiordner
{C94113F4-C027-4F5F-8210-85F4AC2C60...	04.10.2022 09:04	Dateiordner
{DD304A7D-15A7-42B7-AB52-2338F4ECE...	04.10.2022 09:04	Dateiordner
{E675A3BA-6C5C-4E57-A3D3-96C19CEC7...	04.10.2022 09:04	Dateiordner

PS C:\temp2\GPOs> ligo /parse /m ".\{(23DEF82E-039F-40D5-BBCC-35444958D065)\DomainSysvol\GPO\Machine\registry.pol" /q > i e\_computer.txt
PS C:\temp2\GPOs> ligo /parse /m ".\{(4B6589C2-0290-4764-8058-9825B56B4169)\DomainSysvol\GPO\User\registry.pol" /q > use r.txt
PS C:\temp2\GPOs> ligo /parse /m ".\{(7AD4F62E-9296-4FEA-9765-C4E3EEAAECC1)\DomainSysvol\GPO\Machine\registry.pol" /q > credentialguard.txt
PS C:\temp2\GPOs> ligo /parse /m ".\{(B669E0C6-C1E3-4582-B797-FE384B21CD01)\DomainSysvol\GPO\Machine\registry.pol" /q > d efender.txt
PS C:\temp2\GPOs> ligo /parse /m ".\{(B697C660-A87B-4AF1-B37D-9440912605E7)\DomainSysvol\GPO\Machine\registry.pol" /q > b itlocker.txt
PS C:\temp2\GPOs> ligo /parse /m ".\{(C94113F4-C027-4F5F-8210-85F4AC2C6082)\DomainSysvol\GPO\User\registry.pol" /q > ie ser.txt
PS C:\temp2\GPOs> ligo /parse /m ".\{(DD304A7D-15A7-42B7-AB52-2338F4ECE2C7)\DomainSysvol\GPO\Machine\registry.pol" /q > c omputer.txt

Extract the baseline zip file

Export the GPOs as text file using the [script](#).

## Swiss Post recommendations

<pre> 52 log " Set hardening rules from Swiss Post" 53 log " Registry Keys" 54 55 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer", "NoAddPrinter", 1)] 56 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers", "AddPrinterB 57 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Wscntfrg\Parameters", "Start", 0)] 58 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole", "SecurityLevel", 0)] 59 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer", "NtLm", 1)] 60 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile", "DefaultInboundAction", 1)] 61 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile", "DefaultOutboundAction", 1)] 62 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile", "DefaultInboundAction", 1)] 63 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile", "DefaultOutboundAction", 1)] 64 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters", "DisableComponents", "0xffffffff") 65 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters", "Nc_ShowShareAccessUI", 0)] 66 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters", "Nc_ShowShareAccessUI", 0)] 67 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "NoConnectedDrive", 1)] 68 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "NoConnectedDrive", 1)] 69 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "EnableLUA", 1)] 70 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "EnableLUA", 1)] 71 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "ConsentPromptBehaviorAdmin", 2)] 72 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "ConsentPromptBehaviorAdmin", 2)] 73 74 log " Disable Tereb" 75 netsh interface teredo set state disabled 76 log " Result SLA5TEXTCODE" 77 78 log " Disable guest user" 79 net user guest /active:no 80 log " Result SLA5TEXTCODE" 81 82 log " Changing Audit Policy" 83 auditpol /set /subcategory:"Authentifizierungsrichtlinienänderung" /success:enable /failure:disable 84 auditpol /set /subcategory:"Autorisierungsrichtlinienänderung" /success:enable /failure:disable 85 auditpol /set /subcategory:"Richtlinienänderungen überwachen" /success:enable /failure:disable 86 87 log " Block SOMP" 88 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules", "Custom-Block-SOMPv4", "v2.30\Acti 89 [Microsoft.Windows.Registry::SetValue("HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules", "Custom-Block-SOMPv6", "v2.30\Acti </pre>	<p>The security settings from the Swiss Post have been implemented as PowerShell commands inside the customization.ps1</p>
--	--

## CIS Benchmark

<p>cis.txt</p> <pre> 1 ; ----- 2 ; CIS Benchmark Policies 3 4 Computer 5 SYSTEM\CurrentControlSet\Control\Lsa 6 RunAsPPL 7 DWORD:1 8 9 Computer 10 SOFTWARE\Policies\Microsoft\Windows\System 11 AllowCustomSSPsAPs 12 DWORD:0 13 14 Computer 15 Software\Policies\Microsoft\Windows\CloudContent 16 DisableConsumerAccountStateContent 17 DWORD:1 </pre>	<p>The settings from the CIS benchmark have been implemented as LGPO exports in the file cis.txt</p>
---	--

## Custom settings

In addition to the predefined hardening rules taken from other sources, we have implemented a few security settings of our own. These mostly deal with cloud integration, privacy, and data leakage prevention.

Setting	Set to
Turn off the advertising ID	Enabled
Allow telemetry	Disabled
Do not show feedback notifications	Enabled
Do not allow web search	Enabled
Turn off Windows error reporting	Enabled
Disable changing Automatic Configuration settings	Enabled

There are also almost 100 privacy enhancing settings for the Edge browser that would be out of scope to document here in detail, but are listed in the text file "edge.txt" in the image.

### Non-implemented security settings

The following security baseline settings recommended by either Microsoft or the Swiss Post haven't been implemented in the image. They are present in the configuration files but commented out and documented here with the respective reason why they weren't enabled.

Setting	Reason
Disable Windows + R	It's a usability decrease without a clear security benefit
Static DNS server	We didn't want to set a public DNS server like 8.8.8.8 due to privacy issues, and the security risk from a DNS based MitM attack seemed low considering we're using transport encryption
Configure Windows Defender SmartScreen: Block	Because the offline laptops don't have network connectivity, this would cause queries to SmartScreen to not work, and authorized E-Voting applications to be blocked
Deny write access to removable drives not protected by BitLocker	We need to save data to unencrypted USB drives during the e-voting process
Block untrusted and unsigned processes that run from USB	We need to be able to run executables from USB drives during the e-voting process
Script execution policy: All Signed	We need to be able to run unsigned scripts during the e-voting process

## Autounattend-File

To allow the setup to proceed without user choices, we use an unattend file to automatically configure various settings and actions during Windows Setup. The unattend file is copied to the root file of the boot media under the name autounattend.xml.

Following are the settings that are implemented in the file, separated by the steps they are happening in.

### WindowsPE

- OS Language is set to German
- User locale and system locale are set to Swiss German
- Keyboard layout is set to Swiss German
- Windows EULA is automatically accepted
- Registration organization of Windows is set to "Evoting"
- Disk is partitioned into 3 partitions:
  - 500 MB EFI partition for BitLocker
  - 16 MB MSR partition for disk metadata
  - Rest of the disk as a primary partition for the OS
- Partitions are formatted:
  - EFI partition as FAT32 and labelled "System"
  - OS partition as NTFS and labelled "Windows"
- The Windows installation is applied from the "Windows 10 Enterprise N LTSC" image

### OOBESystem

- WLAN setup is skipped
- EULA is skipped
- Privacy settings are skipped
- Time zone is set to Western Europe Standard Time
- An administrator account is configured with a default password
- OS Language is set to German
- User locale and system locale are set to Swiss German
- Keyboard layout is set to Swiss German

### Specialize

- Auto logon is configured for the administrator account
- Six PowerShell commands are started in sequence
  - PowerShell script execution policy is set to "RemoteSigned"
  - The drive letter of the boot media is retrieved from WMI
  - Drivers are installed
  - Applications are installed
  - Policies and other settings are applied
  - The updates are staged to the computer hard disk to later be installed

## Checklist for image update

When a new version of the image is created, the following steps need to be executed:

- Check for [every application](#) whether a new version is available and replace those. For some of them, the customer might have to be contacted since the downloads aren't public. For some applications, an update might not be allowed due to compatibility issues.
- Create a new driver package for each [supported model](#). Make sure to [exclude the drivers](#) that have caused issues in the past.
- Download current BIOS update packages for every model, and update the script "check-biosupdatestatus.ps1" to the current versions
- Check with the customer if any security settings need to be adjusted.

- Set up a VM with the last image, then update it from the Microsoft servers, note the KB numbers of the updates that are being installed, and integrate them into the image.
- Check if any Notepad++ plugins have been updated by launching the application and looking at the update tab in Plugins Admin
- Create a Release Candidate ISO file, then modify the image verification script until it returns the correct results.
- Image a computer using the ISO file and doublecheck whether all Windows Updates are counted as installed.
- Sign the image verification script.
- Create a zip file with the [documentation](#).
- Upload the iso file, the documentation, and the image verification script to the sharing platform
- Archive the image components onto the project network server

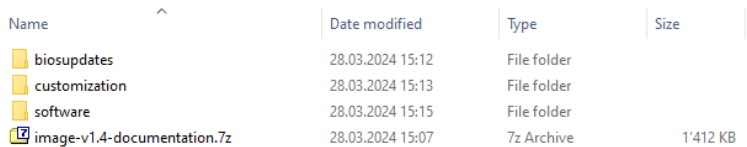
## Create documentation to publish

We need to make available a collection of files to the public to document what we've done and allow some transparency to the voters. We create an archive of script and documentation files and provide that to the customer who takes care of the publishing itself.

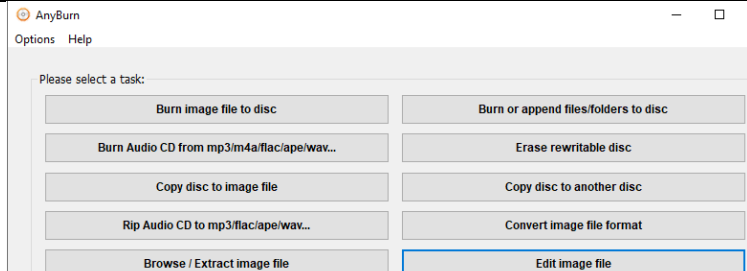
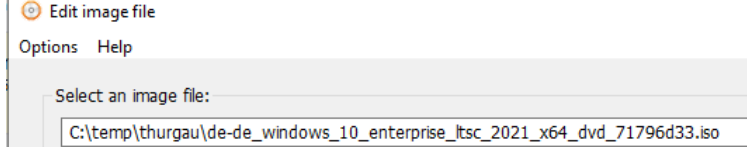
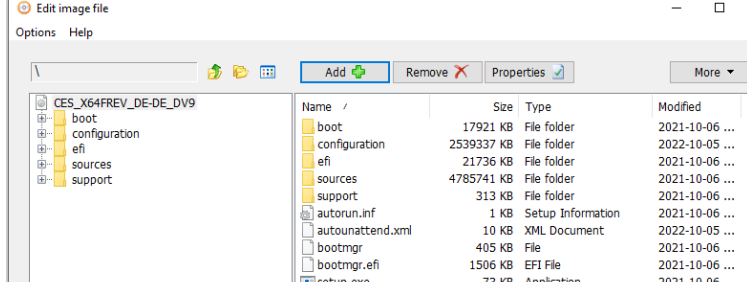
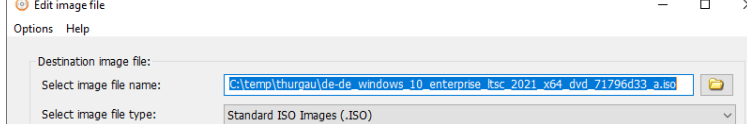
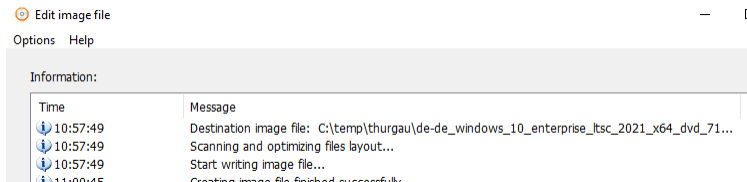
	<p>Export a list of all the customized files to a CSV file using the command:</p> <pre>ls E:\configuration\ -Recurse   select FullName, Length, LastWriteTime   Export-Csv C:\data\thurgau\documentation\filelist.csv -NoTypeInformation -Encoding UTF8</pre>
	<p>Archive the four PowerShell files and the entire "customization" directory into a 7z file...</p>
	<p>...and add:</p> <ul style="list-style-type: none"> <li>• autounattend.xml</li> <li>• filelist.csv</li> <li>• the image verification script</li> <li>• image documentation Word file as a PDF</li> </ul>
	<p>Upload the resulting file</p>

## Archival

While we don't archive the full ISO files due to space issues, we want to archive the most important files for future reference.

	<p>Create a subdirectory for the current image version, and copy the documentation 7z, as well as the directories: <i>customization</i>, <i>software</i> and <i>biosupdates</i></p>
---	---

## Create the bootable ISO

	<p>Start Anyburn, then choose "Edit Image"</p>
	<p>Open a bootable ISO file</p>
	<p>Add the "autounattend.xml" and the "configuration" directory</p>
	<p>Save under a different name</p>
	<p>Wait until it's finished</p>

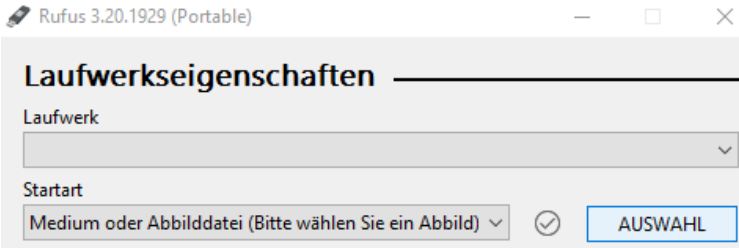
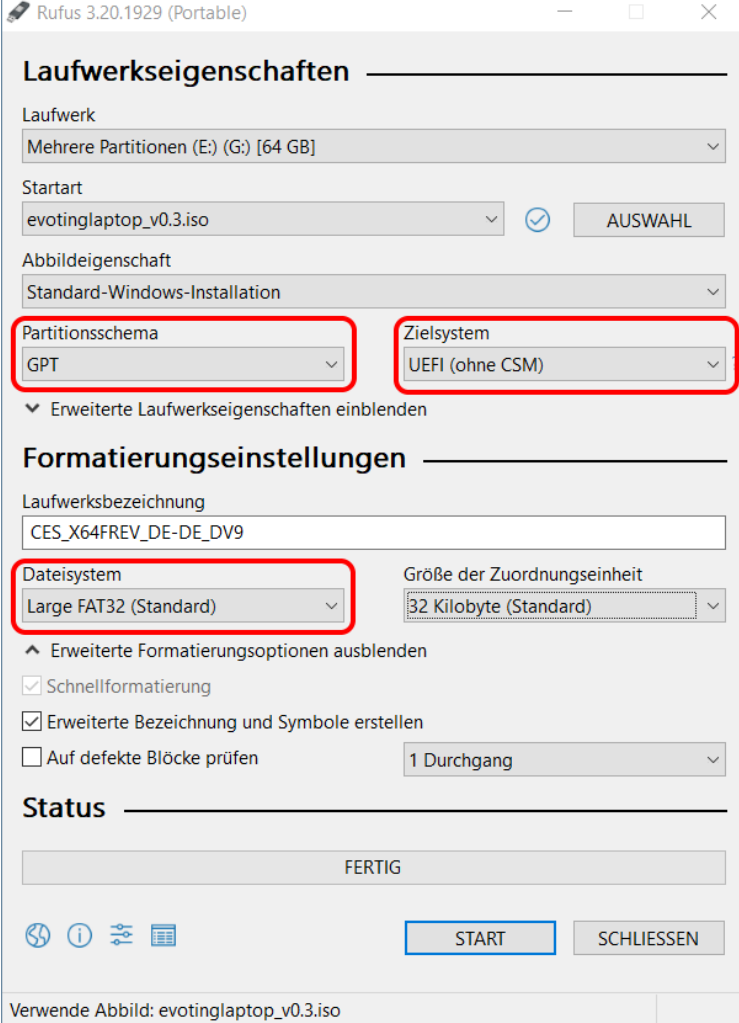
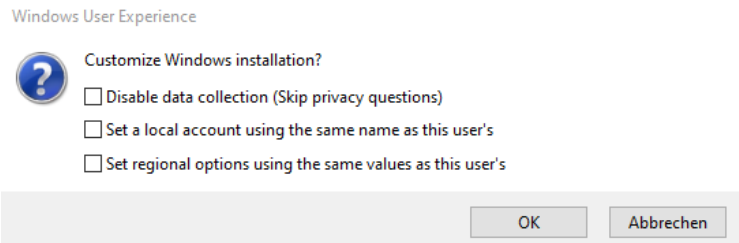
## Upload the image

	<p>Rename the resulting image to evotinglaptop_vx.y.iso</p>
---	---

<p>All Files &gt; Kiteworks &gt; Kanton Thurgau</p> <hr/> <div> <input type="checkbox"/> Name ^         </div> <hr/> <div> <input type="checkbox"/>  Upload         </div> <hr/> <div> <input type="checkbox"/>  evotinglaptop_v0.5.iso         </div>	<p>And upload it to the Kiteworks share</p> <p><a href="https://kiteworks.ontrex.ch/#/folder/8666a49b-a3d7-4831-9d02-45666f755d19">https://kiteworks.ontrex.ch/#/folder/8666a49b-a3d7-4831-9d02-45666f755d19</a></p>
--	--

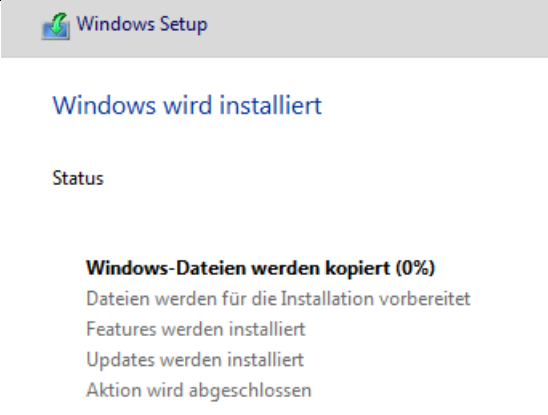
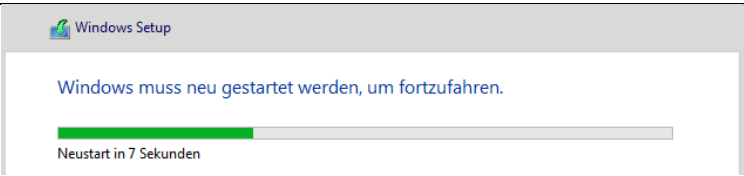
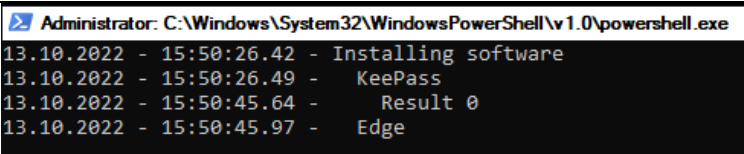
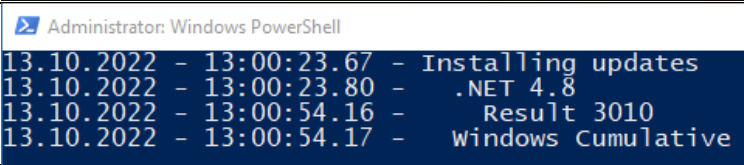
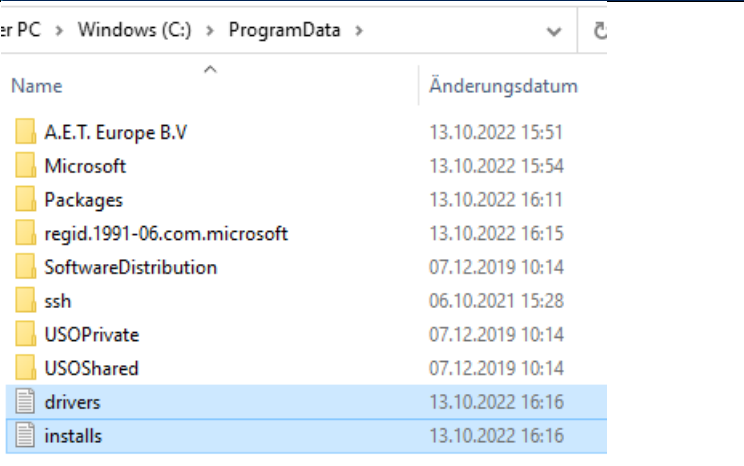
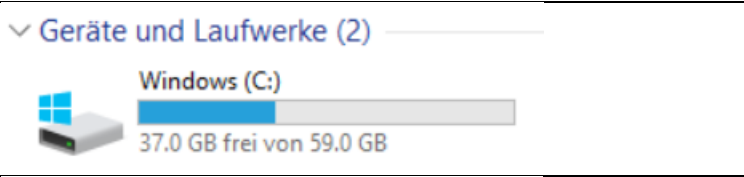
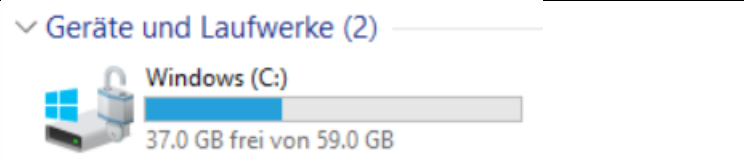
## User Guide

### Extract the ISO to a USB Stick

	<p>Start Rufus and select the ISO file</p>
	<p>Use GPT, UEFI (without CSM) and Large FAT32 as options</p> <p>Do not modify the drive name, it has to stay on the default value</p>
	<p>Do not let Rufus do any adjustments to the Windows installation</p>

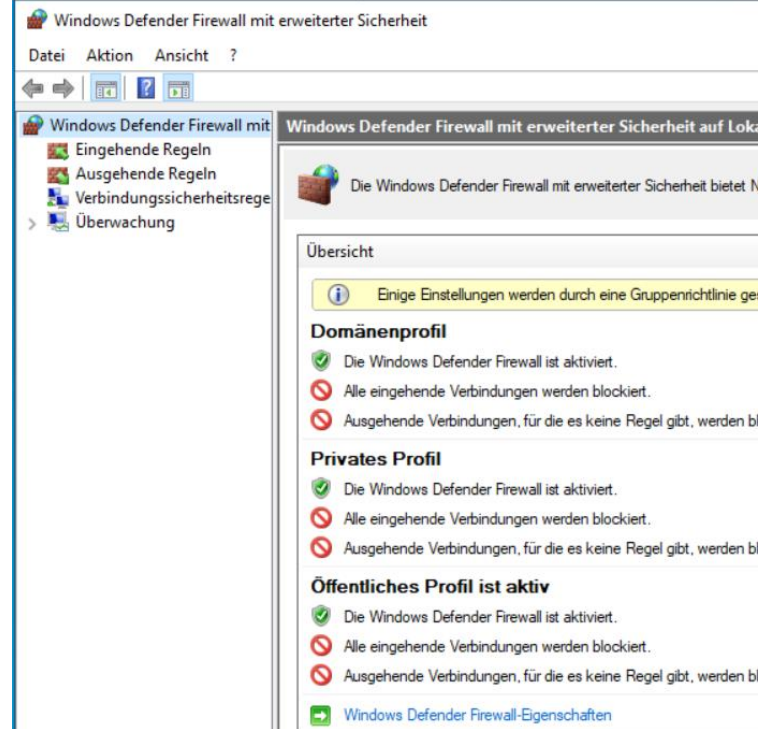
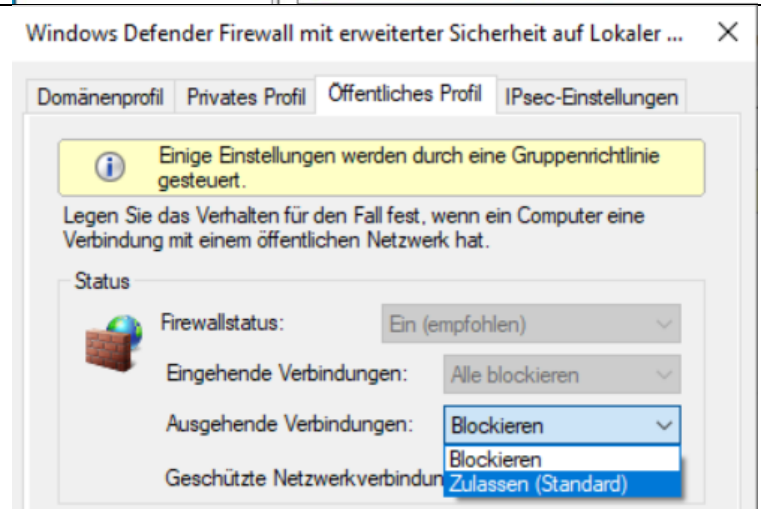



## Apply the image to a computer

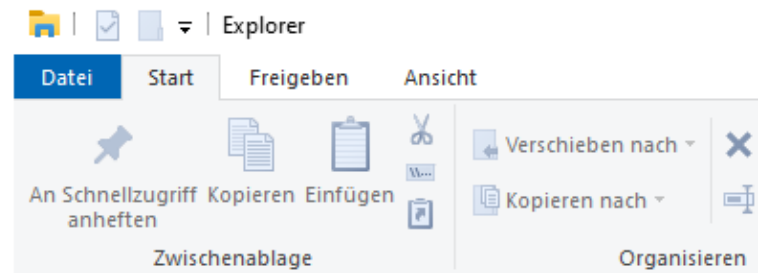
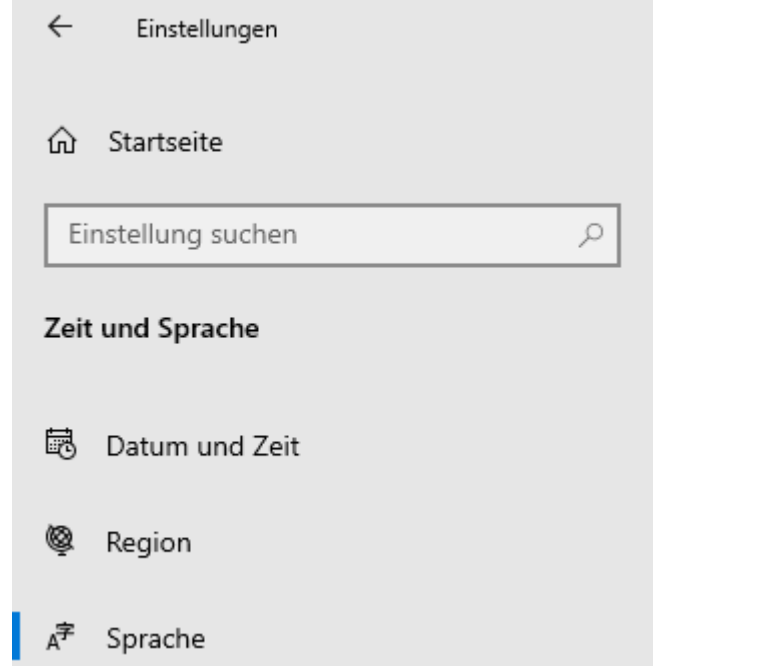

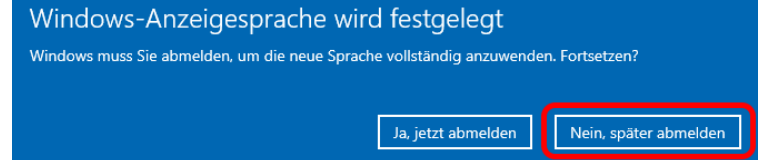
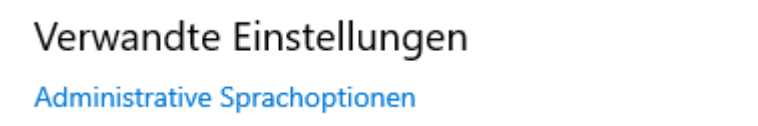
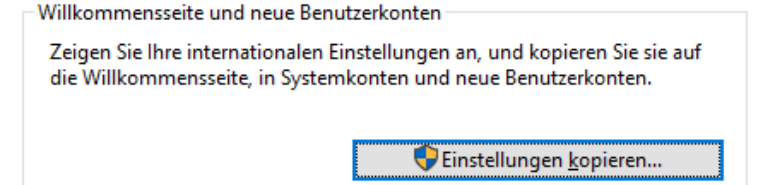
	<p>Boot the laptop from the USB stick by pressing either F9 for HP, F12 for Lenovo, or Esc for Panasonic early in the boot process.</p> <p>The Windows Setup will then automatically start</p>
	<p>After a while it'll reboot...</p>
	<p>...and continue by installing drivers, applications etc</p>
	<p>When the computer is installing updates, the USB stick can be removed</p>
	<p>Log files about the setup are created in the directory c:\programdata</p>
	<p>The hard drive will not be immediately encrypted</p>
	<p>After a few reboots however it'll be encrypted (if the laptop is connected to a power supply)</p>

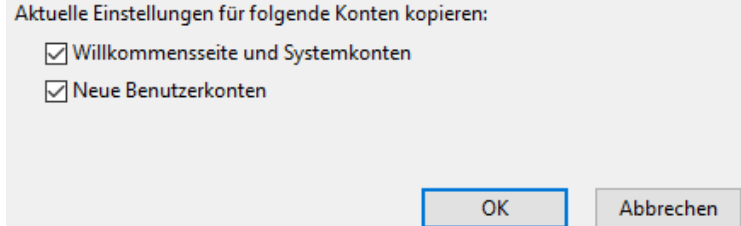
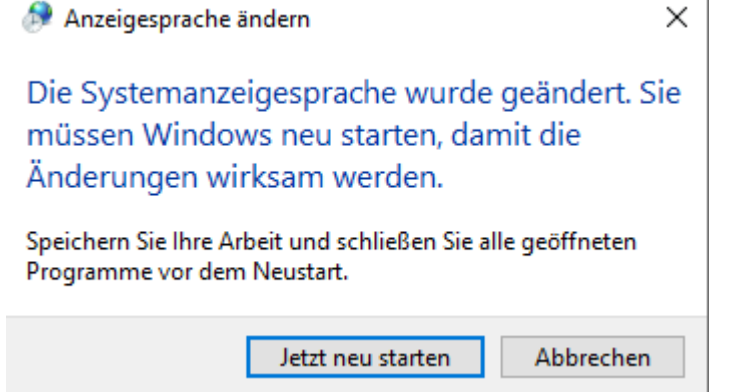
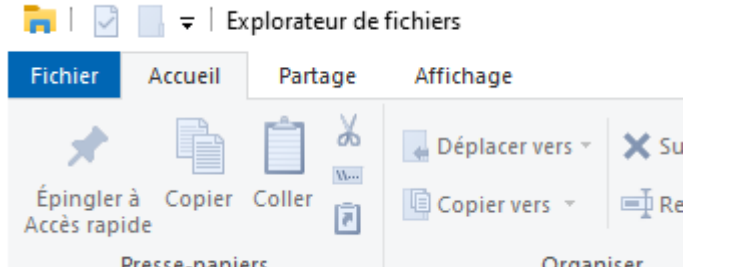
## Enable network connectivity

By default, both incoming and outgoing network connections are blocked. If the specific laptop that is being set up needs to have Internet connectivity, outgoing connections have to be manually enabled.

	<p>With the administrator account, open the Windows Firewall settings</p>
	<p>Set outbound connections to "Allowed" under the public profile</p>
	<p>Then restart the computer</p>

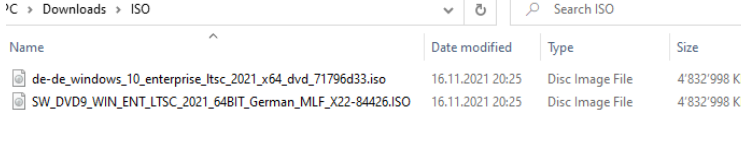
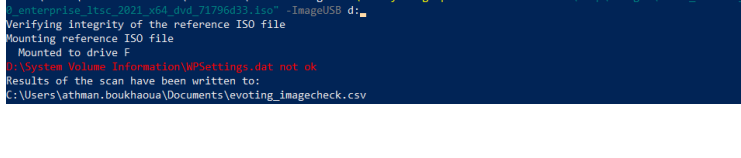
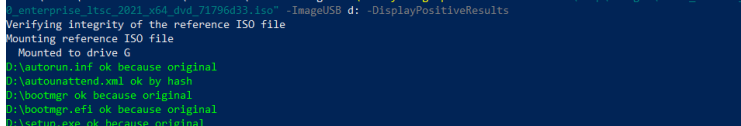
## Change language

	<p>By default, the UI language is in German.</p> <p>If the PC is required to be in French...</p>
	<p>...then open Settings and go to “Time and Language”, then “Language”</p>
	<p>Change the display language to French</p>
	<p>Do <i>not</i> log off when prompted</p>
	<p>Scroll down and click “Administrative language options”</p>
	<p>Click “Copy Settings”</p>

	<p>Set the checkboxes on the login page and the new user accounts, then press OK</p>
	<p>Confirm the restart</p>
	<p>After that, Windows is in French</p>

## Verify image authenticity

To verify that a USB stick hasn't been tampered with and contains only either official Microsoft files or files that have been put there as part of the image customization, the script "verify-image.ps1" can be used.

	<p>Download the German Windows LTSC 2021 ISO from an official Microsoft source, like the VLSC, the partner download portal or Visual Studio Downloads.</p>
	<p>Run the script with the parameter -ReferenceISO pointing to the above ISO file, and -ImageUSB set to the USB drive that should be checked</p>
	<p>Optionally, the parameter "-DisplayPositiveResults" can be used to show correctly checked files in green</p>

	A	B	C	D	E	F	G	H	
1	Info	Reason	Result	FileName					The script will output a detailed report in the "Documents" directory that shows check results for all files
2	3378723C	original	ok	D:\autorun.inf					
3	E803F131	hash	ok	D:\autounattend.xml					
4	4EEAC11B	original	ok	D:\bootmgr					
5	96B7EE39	original	ok	D:\bootmgr.efi					
6	30043368	original	ok	D:\setup.exe					
7	A6FB0A49	hash	failed	D:\System Volume Information\WPSettings.dat					
8	16327144	original	ok	D:\boot\bcd					
9	CD2C00CE	original	ok	D:\boot\boot.sdi					
10	2F9C2428	original	ok	D:\boot\bootfix.bin					
11	55A47316	original	ok	D:\boot\bootsect.exe					
12	F425E135	original	ok	D:\boot\etfsboot.com					
13	BF8A9CC6	original	ok	D:\boot\memtest.exe					
14	C89CDA7E	original	ok	D:\boot\de-de\bootsect.exe.mui					

## Version History

### v0.1

- Initial Version
- Includes 8 applications, drivers for 4 models and initial hardening rules from both Swiss Post and Microsoft
- Includes updates for October 2022

### v0.2

- Add 7-Zip application
- Add Total Commander configuration, license, and shortcut in Start Menu
- Enable display of hidden files and file extensions in Explorer
- Remove camera driver from 850 G3 driver package
- Fix driver install logic for both 850 G3 and 850 G5
- Downgrade Smart Screen policy in Explorer from Block to Warn

### v0.3

- UAC is now set to highest level
- PowerShell execution policy set to allow unsigned scripts
- Changed username for admin login to "EvotingAdmin"

### v0.4

- Blocking all outgoing ICMP packets
- Blocking all outgoing network connections by default
- Blocking cameras and audio devices in with device installation restrictions
- Update Total Commander to version 10.52
- Installing Total Commander to c:\totalcmd
- Installing OpenSSL to c:\openssl

### v0.5

- Updated OpenSSL to 1.1.1s
- Enabled the hardening rule "Disable new DMA devices when the PC is locked"

### v1.0

- Disabled all Bluetooth devices
- Disabled automatic Windows Updates
- Disabled 31 Windows services for additional hardening
- Added support for laptop model HP ZBook Fury 16 G9
- Added almost 100 privacy hardening rules for Edge Browser
- Updates to Windows for December 2022
- Updates to applications: Notepad++ 8.4.8, STunnel 5.67

### v1.1

- Added .NET 6 Runtime
- Disabled Sleep Mode
- Added a barcode and OCR font
- Increased local account password expiration to 120 days
- Split setup logs into two files to make them more readable
- Updates to Windows for March 2023
- Updates to applications: KeePass 2.53.1, Notepad++ 8.5.1, OpenSSL 1.1.1t, STunnel 5.69

### v1.1.1

- Removed SafeSign
- Installed GMP to c:\vmgj
- Updates to applications: KeePass 2.54, Notepad++ 8.5.3, OpenSSL 3.1.1

## v1.2

- Added 63 new hardening rules from CIS benchmarks
- Disabled Hibernate Mode
- Assigned text files to open with Notepad++
- Customized task bar
- Removed support for HP EliteBook 850 G3
- Updates to Windows and drivers for July 2023
- Updates to applications: 7-Zip 23.01, Notepad++ 8.5.4, STunnel 5.70

## v1.3

- Uninstalled Windows Experience Pack
- Allowed standard users to change the system time
- Added the font "Roboto Mono"
- Added the Notepad++ Plugin "JSTool"
- Updates to Windows and drivers for November 2023
- Updates to applications: KeePass 2.55, Notepad++ 8.6, OpenSSL 3.2.0, SDelete 2.05, STunnel 5.71, TotalCommander 11.02

### v1.3.1

- Added support for laptop model HP ZBook Fury 16 G10

## v1.4

- Disabled Windows Recovery Partition
- Added two applications: PowerShell 7 and KeyStore Explorer 5.5.3
- Added BIOS updates to the image for every supported model
- Added a script that notifies if the installed BIOS version is too old
- Updates to Windows and drivers for March 2024
- Updates to applications: KeePass 2.56, Notepad++ 8.6.4, OpenSSL 3.2.1, STunnel 5.72, TotalCommander 11.03

## v1.5

- Removed an application: STunnel
- Updates to BIOS, Windows and drivers for June 2024
- Updates to applications: KeePass 2.57, Notepad++ 8.6.8, OpenSSL 3.3.1, 7-Zip 24.07, PowerShell 7.4.3

## v1.6

- Added French language pack
- Updates to BIOS, Windows and drivers for September 2024
- Updates to applications: Notepad++ 8.6.9, OpenSSL 3.3.2, 7-Zip 24.08, PowerShell 7.4.5

## v1.7

- Updates to BIOS, Windows and drivers for November 2024
- Updates to applications: KeePass 2.57.1, Notepad++ 8.7.1, OpenSSL 3.4.0, PowerShell 7.4.6

## v1.8

- Replaced .NET 6 Runtime with .NET 8 Runtime
- Updates to BIOS, Windows and drivers for February 2025
- Updates to applications: 7-Zip 24.09, Notepad++ 8.7.7, PowerShell 7.4.7, TotalCommander 11.5

## v1.9

- Added support for ZBook Fury G11, ZBook Studio G11 and ThinkStation P8
- Removed support for ThinkPad P52s
- Added default configuration files for OpenSSL
- Updates to BIOS, Windows and drivers for June 2025

- Updates to applications: KeePass 2.58, KeyStore Explorer 5.60, Notepad++ 8.8.1, OpenSSL 3.5.0, PowerShell 7.4.10, TotalCommander 11.51

## Image Authenticity

The authenticity of files in the image is guaranteed through a few different ways:

- Microsoft files are either signed by Microsoft or contained in an ISO file that has a well-known hash published on the official Microsoft website as well as third party websites.
- Driver files from hardware manufacturers are signed by the manufacturers. Windows would display a warning popup when a driver installation with an invalid signature is attempted, so any unsigned driver would be visible during imaging.
- Application executables are signed by their respective developers.
- Application add-ins that we deploy for Notepad++ or Total Commander are not signed. However, they are downloaded from inside their signed parent executable over an HTTPS connection.
- Ontrex custom developed files are either signed by Ontrex, or a hash of the file is stored in a signed script.

This reduces the risk that any malicious files are present in the image, at least to the degree that we can trust the respective developers.

## Lessons learned

1. Windows updates cannot be installed during the "specialize" step. Probably due to provisioning mode. They instead need to be installed in a RunOnce key.
2. Scheduled tasks also cannot be added during Windows Setup because the task service isn't running yet.
3. BitLocker encryption cannot start if there is a DVD inserted in the optical drive, or the laptop is not connected to a power supply.
4. There is no way to block USB network adapters only. If using the DenyDeviceClasses GPO, it blocks every network adapter including internal ones.
5. You cannot define power settings by registry keys. You need to use the powercfg.exe commands.

## Scripts

### export-gpos.cmd

```
lgpo /parse /m ".\{23DEF82E-039F-40D5-BBCC-35444958D065}\DomainSysvol\GPO\Machine\registry.pol" /q > ie_computer.txt
lgpo /parse /m ".\{4B6589C2-0290-4764-8058-9825B56B4169}\DomainSysvol\GPO\User\registry.pol" /q > user.txt
lgpo /parse /m ".\{7AD4F62E-9296-4FEA-9765-C4E3EEAAECC1}\DomainSysvol\GPO\Machine\registry.pol" /q > credentialguard.txt
lgpo /parse /m ".\{B669E0C6-C1E3-4582-B797-FE384B21CDD1}\DomainSysvol\GPO\Machine\registry.pol" /q > defender.txt
lgpo /parse /m ".\{B697C660-A87B-4AF1-B37D-9440912605E7}\DomainSysvol\GPO\Machine\registry.pol" /q > bitlocker.txt
lgpo /parse /m ".\{C94113F4-C027-4F5F-8210-85F4AC2C6082}\DomainSysvol\GPO\User\registry.pol" /q > ie_user.txt
lgpo /parse /m ".\{DD304A7D-15A7-42B7-AB52-2338F4ECE2C7}\DomainSysvol\GPO\Machine\registry.pol" /q > computer.txt
```

## Sources

<https://winaero.com/create-bootable-usb-for-windows-10-install-wim-larger-than-4gb/>  
<https://learn.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy>



<https://learn.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-available-to-vendors>

<https://github.com/wormeyman/FindFonts/blob/master/Add-Font.ps1>

<https://www.alkanesolutions.co.uk/2021/12/06/installing-fonts-with-powershell/>