

# Evoting – Basic installation and hardening

Version 1.11

Date 2025-12-01

*Windows image documentation*

## 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

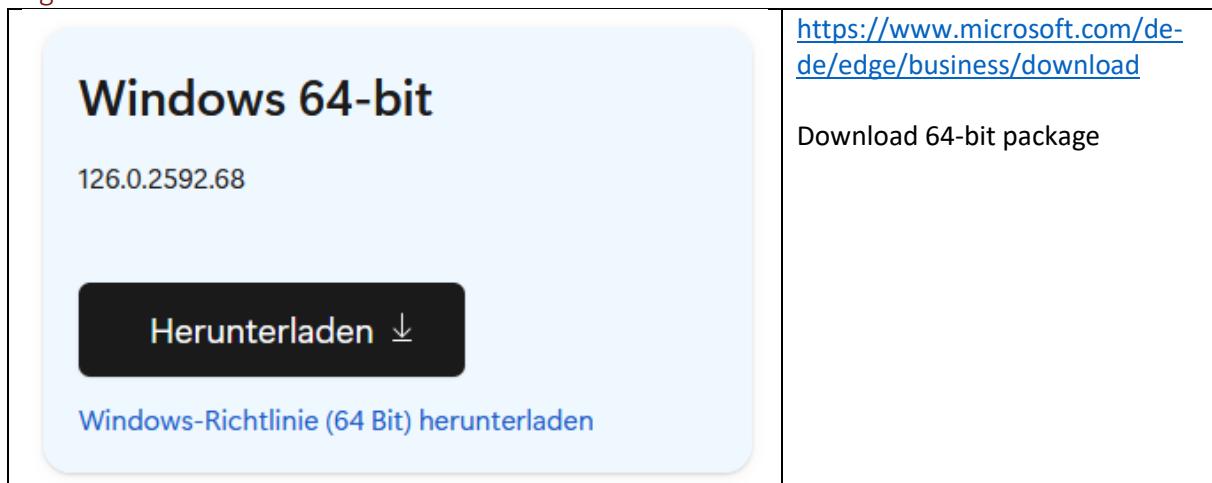
KeePass

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



Windows 64-bit  
126.0.2592.68

Herunterladen ↓

[Windows-Richtlinie \(64 Bit\) herunterladen](#)

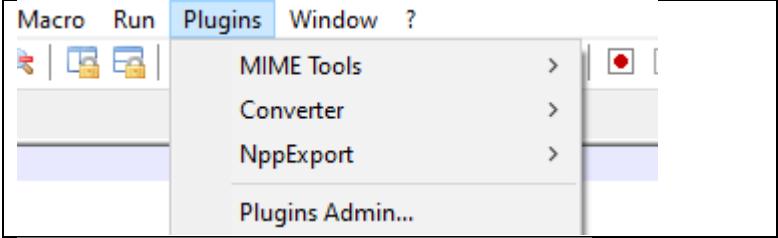
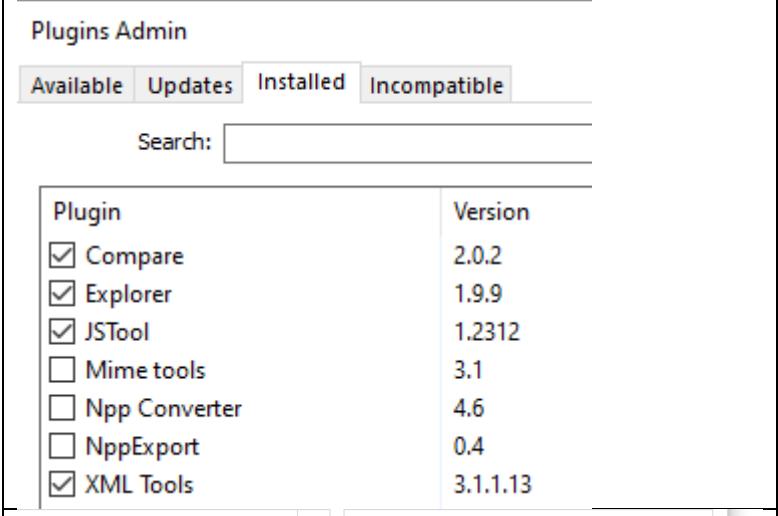
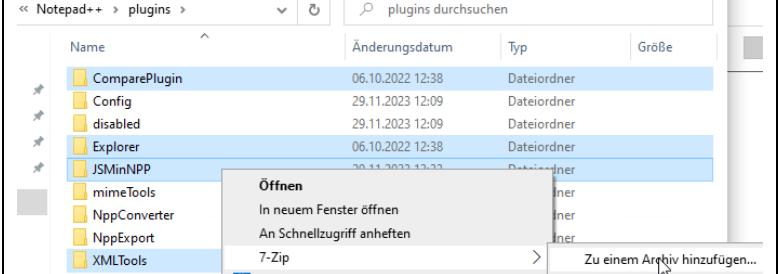
<https://www.microsoft.com/de-de/edge/business/download>

Download 64-bit package

Notepad++

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

## Notepad++ Plugins

	<p>On a test computer, install Notepad++ and start Plugins Admin</p>																
 <table border="1" data-bbox="230 662 722 977"> <thead> <tr> <th>Plugin</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>Compare</td> <td>2.0.2</td> </tr> <tr> <td>Explorer</td> <td>1.9.9</td> </tr> <tr> <td>JSTool</td> <td>1.2312</td> </tr> <tr> <td>Mime tools</td> <td>3.1</td> </tr> <tr> <td>Npp Converter</td> <td>4.6</td> </tr> <tr> <td>NppExport</td> <td>0.4</td> </tr> <tr> <td>XML Tools</td> <td>3.1.1.13</td> </tr> </tbody> </table>	Plugin	Version	Compare	2.0.2	Explorer	1.9.9	JSTool	1.2312	Mime tools	3.1	Npp Converter	4.6	NppExport	0.4	XML Tools	3.1.1.13	<p>Install «Compare», «Explorer», «XML Tools» and «JSTool»</p>
Plugin	Version																
Compare	2.0.2																
Explorer	1.9.9																
JSTool	1.2312																
Mime tools	3.1																
Npp Converter	4.6																
NppExport	0.4																
XML Tools	3.1.1.13																
	<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:

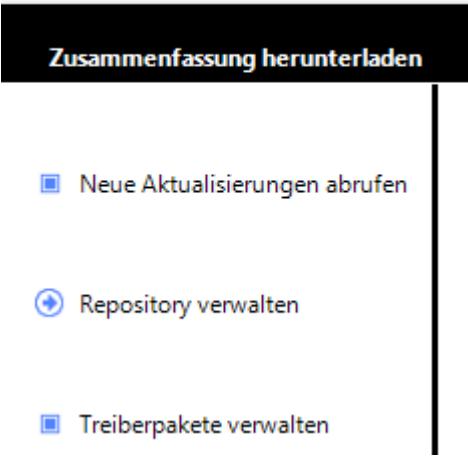
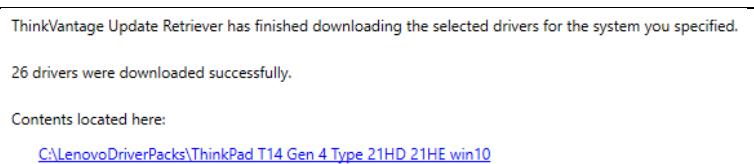
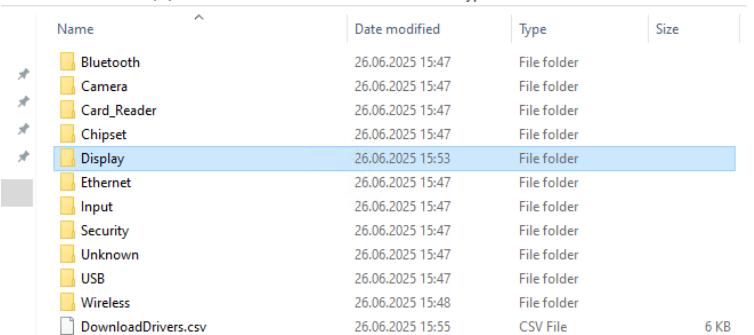
- HP EliteBook 850 G5 (83B2)
- HP ZBook Fury 16 G9 (89C6)
- HP ZBook Fury 16 G10 (?)
- HP ZBook Fury 16 G11 (8CA7)
- HP ZBook Studio 16 G11 (8CF5)
- Lenovo ThinkStation P8 (30HJ)

### 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>Download SoftPaqs</p> <p><b>Operation</b></p> <p><input type="radio"/> Download SoftPaq(s) only</p> <p><input checked="" type="radio"/> Download and extract SoftPaqs</p> <p><b>Folder preview</b></p> <p><b>Download</b> C:\HPIADownloads\spXXXXX.exe</p> <p><b>Unpack</b> C:\HPIADownloads\spXXXXX</p> <p style="text-align: center;"><b>Start</b></p>	<p>Choose "Download and Extract"</p>																																																																																																																				
<p>PC &gt; Windows (C:) &gt; HPIADownloads</p> <table border="1" data-bbox="212 833 949 1123"> <thead> <tr> <th>Name</th> <th>Date modified</th> <th>Type</th> <th>Size</th> </tr> </thead> <tbody> <tr><td>Readme (20230329 094525).html</td><td>29.03.2023 09:45</td><td>Firefox HTML Doc...</td><td>133 KB</td></tr> <tr><td>sp74518.exe</td><td>29.03.2023 09:45</td><td>Application</td><td>9'937 KB</td></tr> <tr><td>sp75708.exe</td><td>29.03.2023 09:44</td><td>Application</td><td>417'876 KB</td></tr> <tr><td>sp82020.exe</td><td>29.03.2023 09:43</td><td>Application</td><td>3'159 KB</td></tr> <tr><td>sp91562.exe</td><td>29.03.2023 09:43</td><td>Application</td><td>194'622 KB</td></tr> <tr><td>sp94816.exe</td><td>29.03.2023 09:43</td><td>Application</td><td>158'770 KB</td></tr> <tr><td>sp96234.exe</td><td>29.03.2023 09:42</td><td>Application</td><td>6'949 KB</td></tr> <tr><td>sp96501.exe</td><td>29.03.2023 09:42</td><td>Application</td><td>975 KB</td></tr> <tr><td>sp98820.exe</td><td></td><td></td><td></td></tr> <tr><td>sp101370.exe</td><td></td><td></td><td></td></tr> <tr><td>sp104124.exe</td><td></td><td></td><td></td></tr> <tr><td>sp111438.exe</td><td></td><td></td><td></td></tr> <tr><td>sp112848.exe</td><td></td><td></td><td></td></tr> <tr><td>sp112983.exe</td><td></td><td></td><td></td></tr> <tr><td>sp115295.exe</td><td>29.03.2023 09:40</td><td>Application</td><td>352'192 KB</td></tr> <tr><td>sp135655.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>1'473 KB</td></tr> <tr><td>sp138373.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>681 KB</td></tr> <tr><td>sp140913.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>16'019 KB</td></tr> <tr><td>sp141045.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>22'148 KB</td></tr> <tr><td>sp141851.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>36'821 KB</td></tr> <tr><td>sp142504.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>58'157 KB</td></tr> <tr><td>sp142679.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>421 KB</td></tr> <tr><td>sp143121.exe</td><td>29.03.2023 09:39</td><td>Application</td><td>273'786 KB</td></tr> <tr><td>sp74518</td><td>29.03.2023 09:45</td><td>File folder</td><td></td></tr> <tr><td>sp75708</td><td>29.03.2023 09:45</td><td>File folder</td><td></td></tr> <tr><td>sp82020</td><td>29.03.2023 09:43</td><td>File folder</td><td></td></tr> <tr><td>sp91562</td><td>29.03.2023 09:43</td><td>File folder</td><td></td></tr> <tr><td>sp94816</td><td>29.03.2023 09:43</td><td>File folder</td><td></td></tr> </tbody> </table> <div data-bbox="355 1096 933 1230" style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p><b>Delete Multiple Items</b></p> <p>Are you sure you want to permanently delete these 22 items?</p> <p style="text-align: center;"><b>Yes</b> <b>No</b></p> </div>	Name	Date modified	Type	Size	Readme (20230329 094525).html	29.03.2023 09:45	Firefox HTML Doc...	133 KB	sp74518.exe	29.03.2023 09:45	Application	9'937 KB	sp75708.exe	29.03.2023 09:44	Application	417'876 KB	sp82020.exe	29.03.2023 09:43	Application	3'159 KB	sp91562.exe	29.03.2023 09:43	Application	194'622 KB	sp94816.exe	29.03.2023 09:43	Application	158'770 KB	sp96234.exe	29.03.2023 09:42	Application	6'949 KB	sp96501.exe	29.03.2023 09:42	Application	975 KB	sp98820.exe				sp101370.exe				sp104124.exe				sp111438.exe				sp112848.exe				sp112983.exe				sp115295.exe	29.03.2023 09:40	Application	352'192 KB	sp135655.exe	29.03.2023 09:39	Application	1'473 KB	sp138373.exe	29.03.2023 09:39	Application	681 KB	sp140913.exe	29.03.2023 09:39	Application	16'019 KB	sp141045.exe	29.03.2023 09:39	Application	22'148 KB	sp141851.exe	29.03.2023 09:39	Application	36'821 KB	sp142504.exe	29.03.2023 09:39	Application	58'157 KB	sp142679.exe	29.03.2023 09:39	Application	421 KB	sp143121.exe	29.03.2023 09:39	Application	273'786 KB	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		<p>In the download directory, delete the driver packages, but keep the extracted directories and the readme file</p>
Name	Date modified	Type	Size																																																																																																																		
Readme (20230329 094525).html	29.03.2023 09:45	Firefox HTML Doc...	133 KB																																																																																																																		
sp74518.exe	29.03.2023 09:45	Application	9'937 KB																																																																																																																		
sp75708.exe	29.03.2023 09:44	Application	417'876 KB																																																																																																																		
sp82020.exe	29.03.2023 09:43	Application	3'159 KB																																																																																																																		
sp91562.exe	29.03.2023 09:43	Application	194'622 KB																																																																																																																		
sp94816.exe	29.03.2023 09:43	Application	158'770 KB																																																																																																																		
sp96234.exe	29.03.2023 09:42	Application	6'949 KB																																																																																																																		
sp96501.exe	29.03.2023 09:42	Application	975 KB																																																																																																																		
sp98820.exe																																																																																																																					
sp101370.exe																																																																																																																					
sp104124.exe																																																																																																																					
sp111438.exe																																																																																																																					
sp112848.exe																																																																																																																					
sp112983.exe																																																																																																																					
sp115295.exe	29.03.2023 09:40	Application	352'192 KB																																																																																																																		
sp135655.exe	29.03.2023 09:39	Application	1'473 KB																																																																																																																		
sp138373.exe	29.03.2023 09:39	Application	681 KB																																																																																																																		
sp140913.exe	29.03.2023 09:39	Application	16'019 KB																																																																																																																		
sp141045.exe	29.03.2023 09:39	Application	22'148 KB																																																																																																																		
sp141851.exe	29.03.2023 09:39	Application	36'821 KB																																																																																																																		
sp142504.exe	29.03.2023 09:39	Application	58'157 KB																																																																																																																		
sp142679.exe	29.03.2023 09:39	Application	421 KB																																																																																																																		
sp143121.exe	29.03.2023 09:39	Application	273'786 KB																																																																																																																		
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																																																																																																																			

Lenovo

	<p>In Update Retriever, chose “Manage driver packages”</p>
	<p>Enter a path, and select a computer model and operating system</p> <p>Press “Next”</p> <p>In the list of drivers, use “Select all”</p> <p>Check for duplicate drivers here, sometimes multiple copies of a graphics driver make the package needlessly large</p> <p>Press “Next, then Finish”</p>
	<p>Wait for the downloads to finish</p>
<p>ThinkVantage Update Retriever has finished downloading the selected drivers for the system you specified.</p> <p>26 drivers were downloaded successfully.</p> <p>Contents located here:</p> <p><a href="C:\LenovoDriverPacks\ThinkPad T14 Gen 4 Type 21HD 21HE win10">C:\LenovoDriverPacks\ThinkPad T14 Gen 4 Type 21HD 21HE win10</a></p>	<p>Then you can open the result directory</p>
	<p>To see the downloaded drivers</p>

## 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 EliteBook 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 SP158316)
- Delete the driver for “Realtek HD Audio” (currently SP156237)
- Delete the driver for “Intel XMM LTE” (currently SP151712)

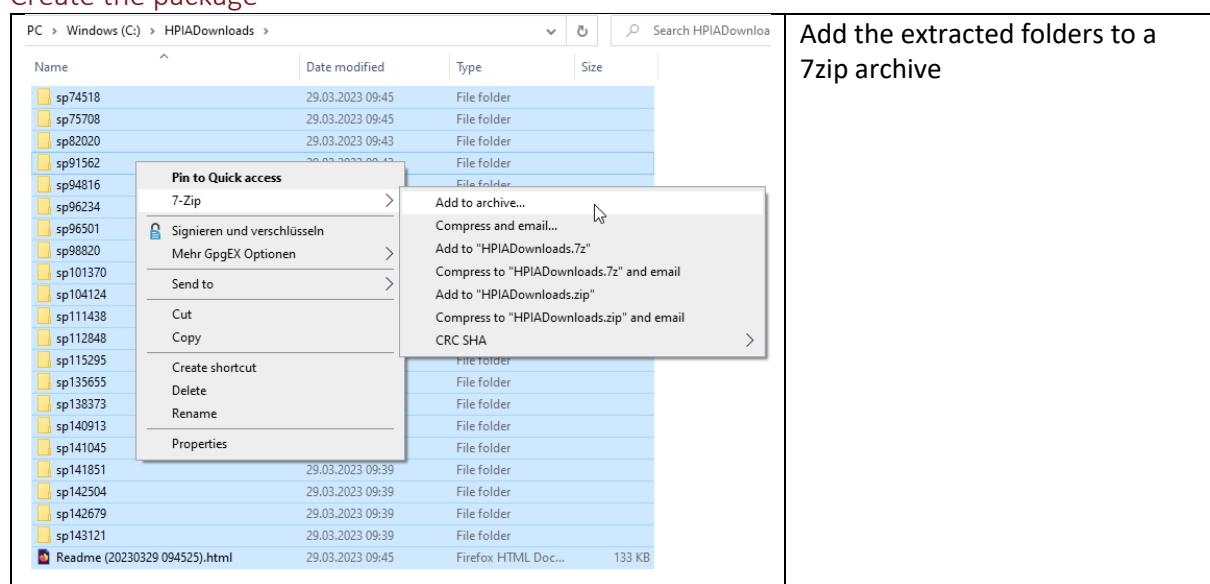
### HP ZBook Fury 16 G10

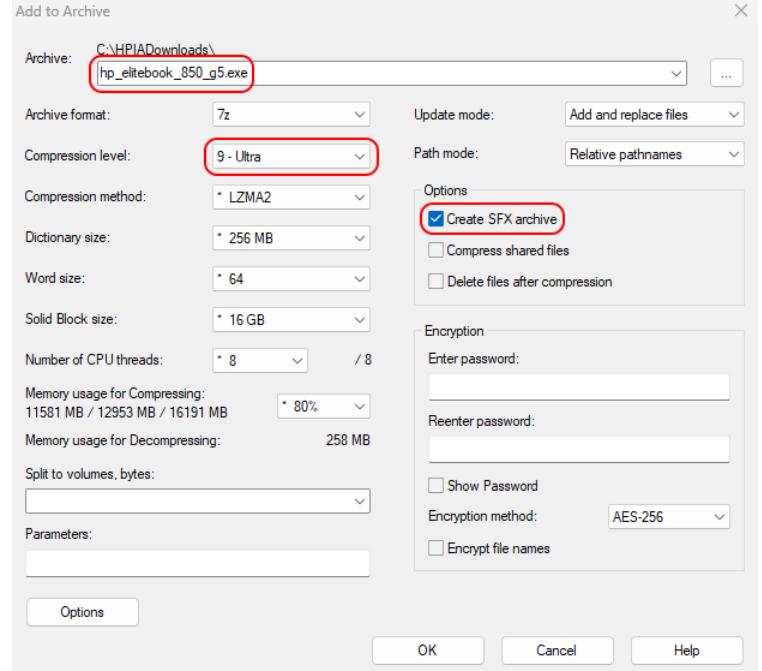
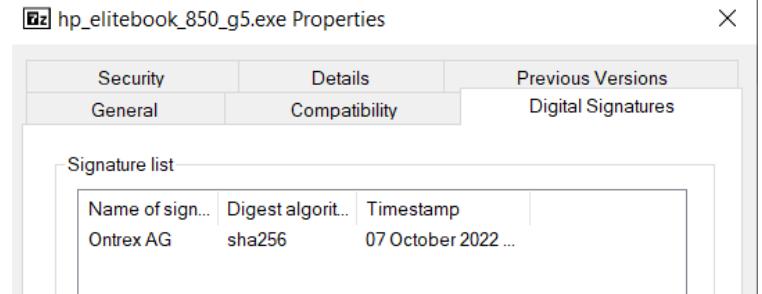
- Delete the driver for “Realtek HD Audio” (currently SP157063)
- Delete the driver for “Intel XMM” (currently SP155280)

### HP ZBook Fury 16 G11

- Delete the driver for “HP 5G Mobile Broadband” (currently SP160331)
- Delete the driver for “HP 4g LTE Mobile Broadband” (currently SP155066)

## Create the package



	<p>As self-extracting archive with ultra compression level, with the name of the laptop model</p>
	<p>Sign the finished archive (with timestamp)</p>

## 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.

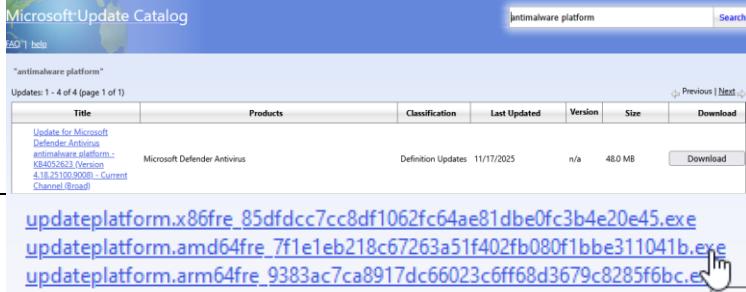
Then, apply the image again, and repeat the above step until Windows Update reports that no updates need to be installed on a freshly applied image.

## Windows

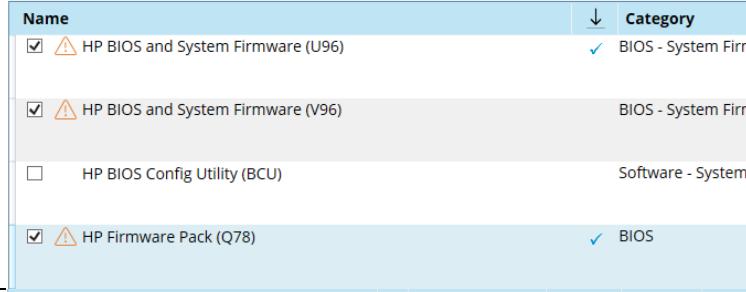
	<p>Go to <a href="https://catalog.update.microsoft.com/Home.aspx">https://catalog.update.microsoft.com/Home.aspx</a> and search for the KB article numbers in the top right</p> <p>For the monthly updates, download the regular cumulative update, not the dynamic one</p> <p>For .NET only download the 4.8.1 package, not the 4.8</p>
---	--

<table border="1"> <tr> <td><a href="#">Windows Malicious Software Removal Tool - v5.106 (KB890830)</a></td><td>Windows 7, Windows Server 2008</td><td>Update Rollups</td><td>10/11/2022</td></tr> <tr> <td><a href="#">Windows Malicious Software Removal Tool x64 - v5.106 (KB890830)</a></td><td>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</td><td>Update Rollups</td><td>10/11/2022</td></tr> <tr> <td><a href="#">Windows Malicious Software Removal Tool - v5.106 (KB890830)</a></td><td>Windows 8.1, Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later, Windows 11</td><td>Update Rollups</td><td>10/11/2022</td></tr> </table> <p><b>.NET Desktop Runtime 8.0.13</b></p> <p>The .NET Desktop Runtime enables you to run existing Windows desktop applications. <b>This release includes the .NET Runtime; you don't need to install it separately.</b></p> <table border="1"> <thead> <tr> <th>OS</th><th>Installers</th><th>Binaries</th></tr> </thead> <tbody> <tr> <td>Windows</td><td><a href="#">x64</a>   <a href="#">x86</a>   <a href="#">Arm64</a>   <a href="#">winget instructions</a></td><td></td></tr> </tbody> </table>	<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	OS	Installers	Binaries	Windows	<a href="#">x64</a>   <a href="#">x86</a>   <a href="#">Arm64</a>   <a href="#">winget instructions</a>		<p>For the malicious software removal tool, sort by date, then pick the newest package for Windows 10 64 bit</p> <p>For .NET 8, go to <a href="https://dotnet.microsoft.com/en-us/download/dotnet/8.0">https://dotnet.microsoft.com/en-us/download/dotnet/8.0</a> and download the newest “Desktop Runtime” for x64</p>
<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																
OS	Installers	Binaries																	
Windows	<a href="#">x64</a>   <a href="#">x86</a>   <a href="#">Arm64</a>   <a href="#">winget instructions</a>																		

## Microsoft Defender

<table border="1"> <tr> <td>Antimalware solution</td><td>Definition version</td></tr> <tr> <td>Microsoft Defender Antivirus for Windows 11, Windows 10, Windows 8.1, and Windows Server</td><td><a href="#">32-bit</a>   <a href="#">64-bit</a>   <a href="#">ARM</a></td></tr> </table> <p><b>Microsoft Update Catalog</b></p> 	Antimalware solution	Definition version	Microsoft Defender Antivirus for Windows 11, Windows 10, Windows 8.1, and Windows Server	<a href="#">32-bit</a>   <a href="#">64-bit</a>   <a href="#">ARM</a>	<p>On <a href="https://www.microsoft.com/en-us/wdsi/defenderupdates">https://www.microsoft.com/en-us/wdsi/defenderupdates</a></p> <p>Download the 64-bit Version for the antivirus definitions</p>
Antimalware solution	Definition version				
Microsoft Defender Antivirus for Windows 11, Windows 10, Windows 8.1, and Windows Server	<a href="#">32-bit</a>   <a href="#">64-bit</a>   <a href="#">ARM</a>				
	<p>For the antimalware update, download the newest “Definition Updates” package</p> <p>Pick the one for “amd64fre”</p>				

## BIOS

<p>2 Select from My Products List</p>  <p>3 Get SoftPaqs</p> <p>Analyze</p> 	<p>For HP, select all models, then press Analyze</p>
	<p>Filter for the word “bios”</p>
	<p>Then check all the BIOS updates and click “Download”</p>
	<p>For the “ZBook Fury 16 G11”, choose the “Non-Vpro” update</p>

<p>Download SoftPaqs</p> <p>Operation</p> <p><input checked="" type="radio"/> Download SoftPaq(s) only</p> <p><input type="radio"/> Download and extract SoftPaqs</p> <p>Folder preview</p> <p>Download C:\HPIADownloads\spXXXXX.exe</p> <p>Unpack C:\HPIADownloads\spXXXXX</p> <p style="text-align: right;"><b>Start</b></p>	<p>Choose “Download only”</p>																														
<p><input type="checkbox"/> Select all</p> <p><input type="checkbox"/> System</p> <p><input type="checkbox"/> 20JH [ ThinkPad Yoga 370 ]</p> <p><input checked="" type="checkbox"/> 20LC [ ThinkPad P52s ]</p>	<p>For Lenovo, select the model in Update Retriever, then search for updates</p>																														
<p>Type: <b>Bios</b></p> <p>Systems: <b>Select...</b> <b>Search</b></p>	<p>Filter for “Bios”</p>																														
<table border="1" data-bbox="192 1096 965 1167"> <thead> <tr> <th></th> <th>Title</th> <th>Update ID</th> <th>Severity</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>BIOS Update Utility - 10/11</td> <td>n27uj32w</td> <td>Recommended</td> <td>Bios</td> </tr> </tbody> </table> <p>PC &gt; DVD Drive (E:) CES_X64FREV_DE-DE_DV9 &gt; configuration &gt; biosupdates</p> <table border="1" data-bbox="192 1167 965 1340"> <thead> <tr> <th>Name</th> <th>Date modified</th> <th>Type</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>hp_elitebook_850_g5_sp152771.exe</td> <td>25.06.2024 19:04</td> <td>Application</td> <td>16'795 KB</td> </tr> <tr> <td>hp_zbook_fury_16_g9_sp153119.exe</td> <td>25.06.2024 19:04</td> <td>Application</td> <td>23'575 KB</td> </tr> <tr> <td>hp_zbook_fury_16_g10_sp151263.exe</td> <td>25.03.2024 09:33</td> <td>Application</td> <td>23'935 KB</td> </tr> <tr> <td>lenovo_thinkpad_p52s_n27uj32w.exe</td> <td>25.06.2024 16:43</td> <td>Application</td> <td>12'910 KB</td> </tr> </tbody> </table>		Title	Update ID	Severity	Type	<input checked="" type="checkbox"/>	BIOS Update Utility - 10/11	n27uj32w	Recommended	Bios	Name	Date modified	Type	Size	hp_elitebook_850_g5_sp152771.exe	25.06.2024 19:04	Application	16'795 KB	hp_zbook_fury_16_g9_sp153119.exe	25.06.2024 19:04	Application	23'575 KB	hp_zbook_fury_16_g10_sp151263.exe	25.03.2024 09:33	Application	23'935 KB	lenovo_thinkpad_p52s_n27uj32w.exe	25.06.2024 16:43	Application	12'910 KB	<p>Then download the BIOS update</p> <p>Rename them with their respective models, and copy them to the “biosupdates” directory under customization</p>
	Title	Update ID	Severity	Type																											
<input checked="" type="checkbox"/>	BIOS Update Utility - 10/11	n27uj32w	Recommended	Bios																											
Name	Date modified	Type	Size																												
hp_elitebook_850_g5_sp152771.exe	25.06.2024 19:04	Application	16'795 KB																												
hp_zbook_fury_16_g9_sp153119.exe	25.06.2024 19:04	Application	23'575 KB																												
hp_zbook_fury_16_g10_sp151263.exe	25.03.2024 09:33	Application	23'935 KB																												
lenovo_thinkpad_p52s_n27uj32w.exe	25.06.2024 16:43	Application	12'910 KB																												

## Hardening

To harden the OS installation, we are using settings sets from both Microsoft, the Swiss Post, and the CIS benchmark, as well as some settings from ourselves.

### Microsoft security baselines

<p>Choose the download you want</p> <p><input type="checkbox"/> File Name</p> <p><input type="checkbox"/> Windows 11 version 22H2 Security Baseline.zip</p> <p><input checked="" type="checkbox"/> LGPO.zip</p> <p><input type="checkbox"/> Windows 10 version 21H1 Security Baseline.zip</p> <p><input checked="" type="checkbox"/> Windows 10 version 21H2 Security Baseline.zip</p> <p><input type="checkbox"/> Windows 11 Security Baseline.zip</p>	<p>On <a href="https://www.microsoft.com/en-us/download/details.aspx?id=55319">https://www.microsoft.com/en-us/download/details.aspx?id=55319</a> download LGPO.exe</p>
	<p>And the baselines for 21H2</p>

er PC > Windows (C:) > temp2 > GPOs			
Name	Änderungsdatum	Typ	Extract the baseline zip file
{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	

## Swiss Post recommendations

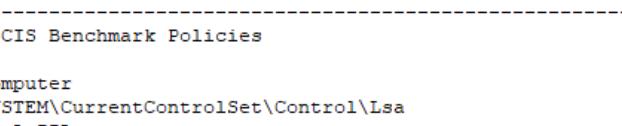
```

52 log " Set Hardening rules from Swiss Post"
53 log " Set Registry keys"
54
55 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer", "NoAddPrinter", 1)
56 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentControlSet\Control\Print\Providers\LocalPrint Services\Server", "AddPrinterOr
57 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry", "Start", 4)
58 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\LocalMachine", "SecurityLevel", 0)
59 #[Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer", "NtAuthz", 1)
60 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\PrivateProfile", "DefaultInboundPolicy", 1)
61 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\PublicProfile", "DefaultInboundPolicy", 1)
62 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\PublicProfile", "DefaultInbound", 1)
63 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\PublicProfile", "DefaultOutbound", 1)
64 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\LocalProfile", "DefaultInbound", 1)
65 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\LocalProfile", "DefaultOutbound", 1)
66 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\LocalProfile", "DefaultInboundPolicy", 0)
67 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Network\Connections", "Nc_SharedAccessSess", 0)
68 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Network\Connections", "Nc_SharedAccess", 0)
69 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Network\Connections", "Nc_SharedAccessSess", 0)
70 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Network\Connections", "Nc_SharedAccess", 0)
71 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Network\Connections", "Nc_SharedAccessSess", 0)
72 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Windows\System", "EnableIab", 1)
73 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Windows\System", "CommitmentBehaviorAdmin", 2)
74
75 log " Disable Teredo"
76 netsh interface teredo set state disabled
77 netsh interface teredo set state disabled
78 log " Block ICMP"
79 log " Disable guest user"
80 log " result $LASTEXITCODE"
81
82 log " Change Audit Policy"
83 auditpol /se /subcategory:"Autentifizierungsrichtlinieneränderung" /success:enable /failure:disable
84 auditpol /se /subcategory:"Autentifizierungsrichtlinieneränderung" /success:enable /failure:enable
85 auditpol /se /subcategory:"Richtlinieneränderungen überwachen" /success:enable /failure:enable
86
87 log " Block ICMP"
88 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\FirewallRules", "Custom-Block-ICMPv4", "0", 30)
89 [Microsoft.win32.Registry]: SetValue("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Firewall\FirewallRules", "Custom-Block-ICMPv6", "0", 30)

```

The security settings from the Swiss Post have been implemented as PowerShell commands inside the customization.ps1

## CIS Benchmark



The settings from the CIS benchmark have been implemented as LGPO exports in the file cis.txt

```
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
```

## 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

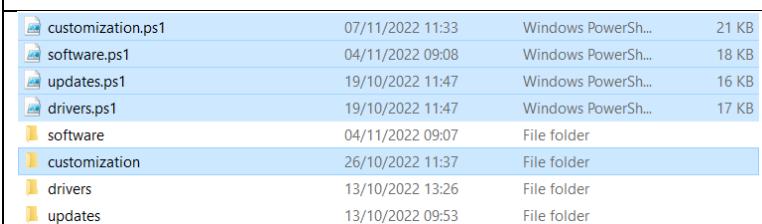
## Adjustments for Windows 11 pilot

As preparation for a change to a Windows 11 LTSC based image, we are currently running a pilot version of the E-Voting image based on this OS. This image has the following changes compared to the productive Windows 10 one:

- Windows User Experience Package is not removed (it doesn't exist anymore)
- The 7-Zip MSI is manually signed with the Ontrex certificate (to prevent long delays during installation)
- The monthly Windows cumulative update package is different
- The .NET 4.8 cumulative update package is different
- Language packs need to be installed with a /limitaccess switch, otherwise there is a long delay during installation. This switch doesn't exist yet in the Windows 10 version of DISM.

## Create documentation to publish

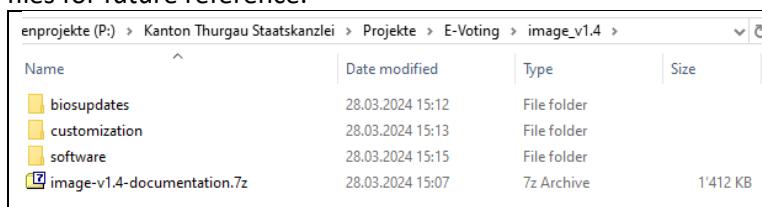
We need to make available a collection of files to the public to document what we've done and allow some transparency to the voters. We create an archive of script and documentation files and provide that to the customer who takes care of the publishing itself.

 <pre>PS C:\&gt; ls E:\configuration\ -Recurse   select FullName, Length, LastWriteTime   Export-Csv C:\temp\thurgau\documentation\filelist.csv -NoTypeInformation -Encoding UTF8 PS C:\&gt; .</pre>	<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>																																				
 <table border="1"> <thead> <tr> <th></th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td></td><td>customization.ps1</td><td>07/11/2022 11:33</td><td>Windows PowerSh...</td> </tr> <tr> <td></td><td>software.ps1</td><td>04/11/2022 09:08</td><td>Windows PowerSh...</td> </tr> <tr> <td></td><td>updates.ps1</td><td>19/10/2022 11:47</td><td>Windows PowerSh...</td> </tr> <tr> <td></td><td>drivers.ps1</td><td>19/10/2022 11:47</td><td>Windows PowerSh...</td> </tr> <tr> <td></td><td>software</td><td>04/11/2022 09:07</td><td>File folder</td> </tr> <tr> <td></td><td>customization</td><td>26/10/2022 11:37</td><td>File folder</td> </tr> <tr> <td></td><td>drivers</td><td>13/10/2022 13:26</td><td>File folder</td> </tr> <tr> <td></td><td>updates</td><td>13/10/2022 09:53</td><td>File folder</td> </tr> </tbody> </table>						customization.ps1	07/11/2022 11:33	Windows PowerSh...		software.ps1	04/11/2022 09:08	Windows PowerSh...		updates.ps1	19/10/2022 11:47	Windows PowerSh...		drivers.ps1	19/10/2022 11:47	Windows PowerSh...		software	04/11/2022 09:07	File folder		customization	26/10/2022 11:37	File folder		drivers	13/10/2022 13:26	File folder		updates	13/10/2022 09:53	File folder	<p>Archive the four PowerShell files and the entire “customization” directory into a 7z file...</p>
	customization.ps1	07/11/2022 11:33	Windows PowerSh...																																		
	software.ps1	04/11/2022 09:08	Windows PowerSh...																																		
	updates.ps1	19/10/2022 11:47	Windows PowerSh...																																		
	drivers.ps1	19/10/2022 11:47	Windows PowerSh...																																		
	software	04/11/2022 09:07	File folder																																		
	customization	26/10/2022 11:37	File folder																																		
	drivers	13/10/2022 13:26	File folder																																		
	updates	13/10/2022 09:53	File folder																																		

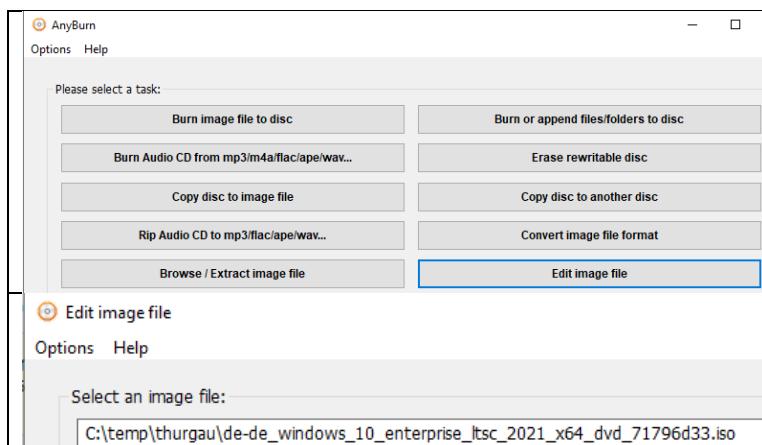
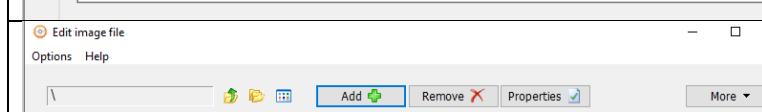
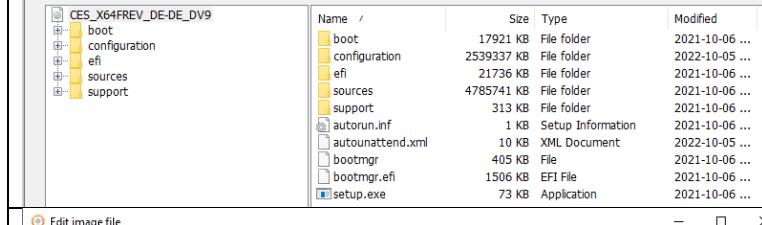
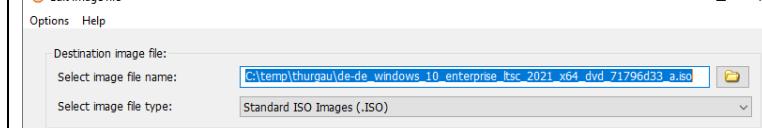
<table border="1"> <thead> <tr> <th colspan="4">C:\temp\thurgau\documentation\image-v1.0-documentation.7z\</th></tr> <tr> <th>Name</th><th>Size</th><th>Packed Size</th><th>Modified</th></tr> </thead> <tbody> <tr> <td>customization</td><td>588 014</td><td>208 804</td><td>2023-01-10 10:29</td></tr> <tr> <td>autounattend.xml</td><td>9 659</td><td>1 831</td><td>2022-10-24 17:21</td></tr> <tr> <td>customization.ps1</td><td>21 280</td><td></td><td>2023-01-10 11:01</td></tr> <tr> <td>drivers.ps1</td><td>17 158</td><td></td><td>2023-01-11 14:19</td></tr> <tr> <td>filelist.csv</td><td>3 732</td><td>1 154</td><td>2023-01-13 09:55</td></tr> <tr> <td>software.ps1</td><td>18 115</td><td></td><td>2023-01-10 11:56</td></tr> <tr> <td>updates.ps1</td><td>15 614</td><td></td><td>2022-10-19 10:47</td></tr> <tr> <td>verify-image_v1.0.ps1</td><td>24 799</td><td>12 971</td><td>2023-01-13 10:11</td></tr> <tr> <td>Windows Image.pdf</td><td>1 388 348</td><td>1 242 976</td><td>2023-01-13 11:26</td></tr> </tbody> </table>	C:\temp\thurgau\documentation\image-v1.0-documentation.7z\				Name	Size	Packed Size	Modified	customization	588 014	208 804	2023-01-10 10:29	autounattend.xml	9 659	1 831	2022-10-24 17:21	customization.ps1	21 280		2023-01-10 11:01	drivers.ps1	17 158		2023-01-11 14:19	filelist.csv	3 732	1 154	2023-01-13 09:55	software.ps1	18 115		2023-01-10 11:56	updates.ps1	15 614		2022-10-19 10:47	verify-image_v1.0.ps1	24 799	12 971	2023-01-13 10:11	Windows Image.pdf	1 388 348	1 242 976	2023-01-13 11:26	<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>
C:\temp\thurgau\documentation\image-v1.0-documentation.7z\																																													
Name	Size	Packed Size	Modified																																										
customization	588 014	208 804	2023-01-10 10:29																																										
autounattend.xml	9 659	1 831	2022-10-24 17:21																																										
customization.ps1	21 280		2023-01-10 11:01																																										
drivers.ps1	17 158		2023-01-11 14:19																																										
filelist.csv	3 732	1 154	2023-01-13 09:55																																										
software.ps1	18 115		2023-01-10 11:56																																										
updates.ps1	15 614		2022-10-19 10:47																																										
verify-image_v1.0.ps1	24 799	12 971	2023-01-13 10:11																																										
Windows Image.pdf	1 388 348	1 242 976	2023-01-13 11:26																																										
 <a href="#">image-v0.5-documentation.7z</a>	Upload the resulting file																																												

## 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>

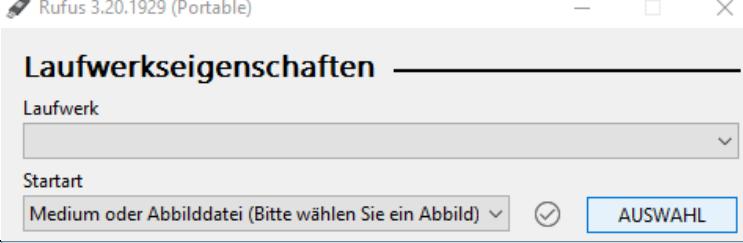
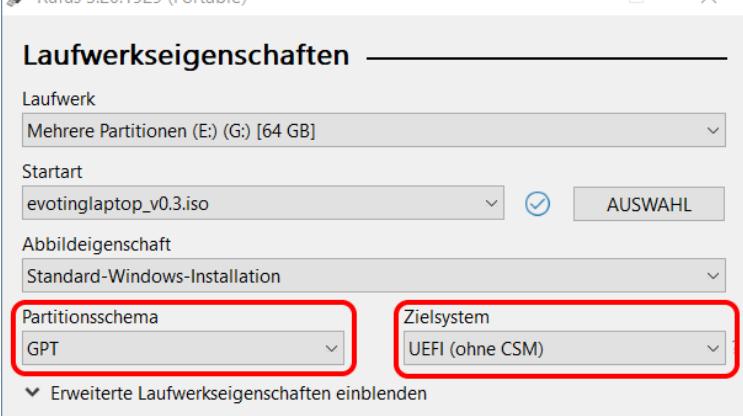
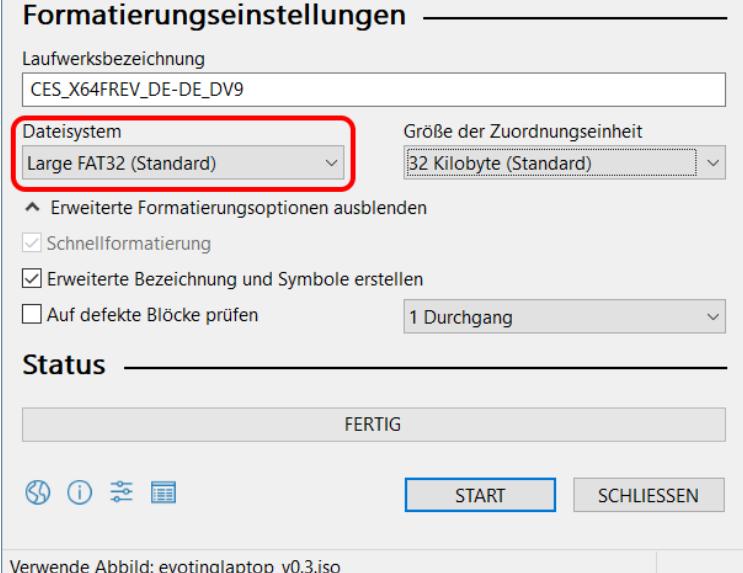
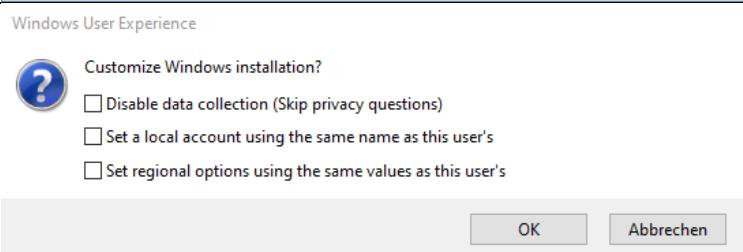
<p>Edit image file</p> <p>Options Help</p> <p>Information:</p> <table border="1"> <thead> <tr> <th>Time</th><th>Message</th></tr> </thead> <tbody> <tr> <td>10:57:49</td><td>Destination image file: C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71...</td></tr> <tr> <td>10:57:49</td><td>Scanning and optimizing files layout...</td></tr> <tr> <td>10:57:49</td><td>Start writing image file...</td></tr> <tr> <td>11:00:45</td><td>Creating image file finished successfully.</td></tr> </tbody> </table>	Time	Message	10:57:49	Destination image file: C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71...	10:57:49	Scanning and optimizing files layout...	10:57:49	Start writing image file...	11:00:45	Creating image file finished successfully.	<p>Wait until it's finished</p>
Time	Message										
10:57:49	Destination image file: C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71...										
10:57:49	Scanning and optimizing files layout...										
10:57:49	Start writing image file...										
11:00:45	Creating image file finished successfully.										

## Upload the image

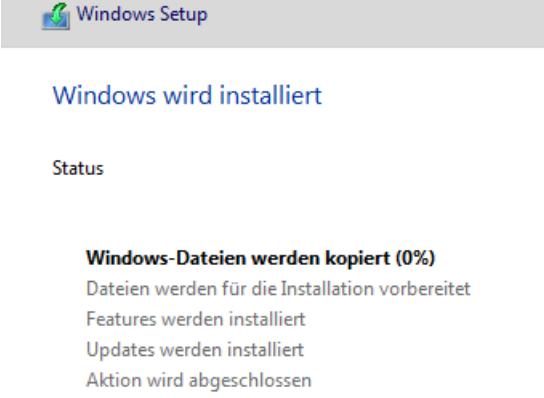
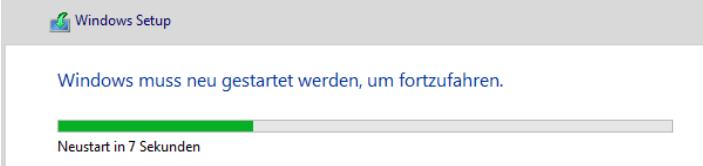
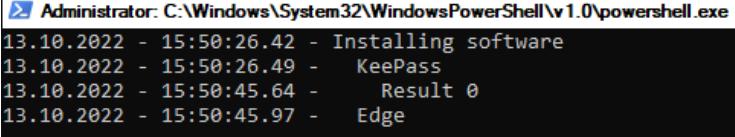
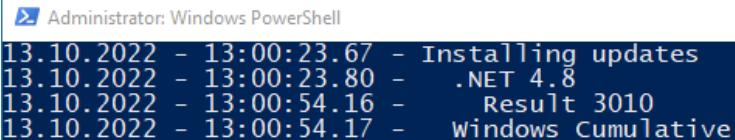
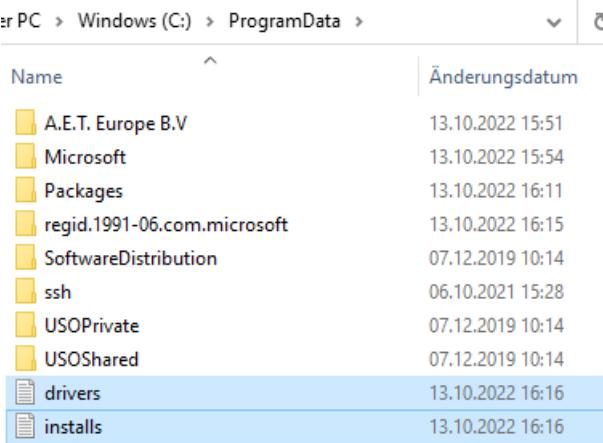
 <p>evotinglaptop_v0 .5.iso</p>	<p>Rename the resulting image to evotinglaptop_vx.y.iso</p>
<p>All Files &gt; Kiteworks &gt; Kanton Thurgau</p> <p><input type="checkbox"/> Name ^</p> <p><input type="checkbox"/>  Upload</p> <p><input type="checkbox"/>  evotinglaptop_v0.5.iso</p>	<p>And upload it to the Kiteworks share</p> <p><a href="https://kiteworks.ontrex.ch/#/folde...45666f755d19">https://kiteworks.ontrex.ch/#/folde...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

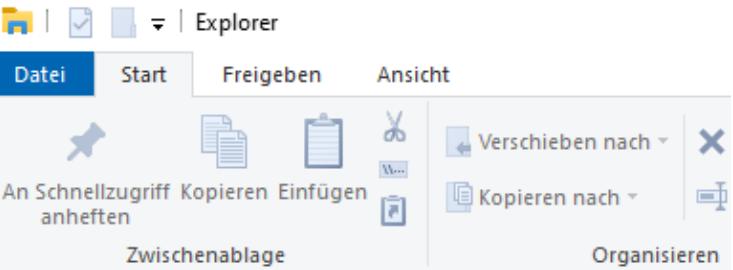
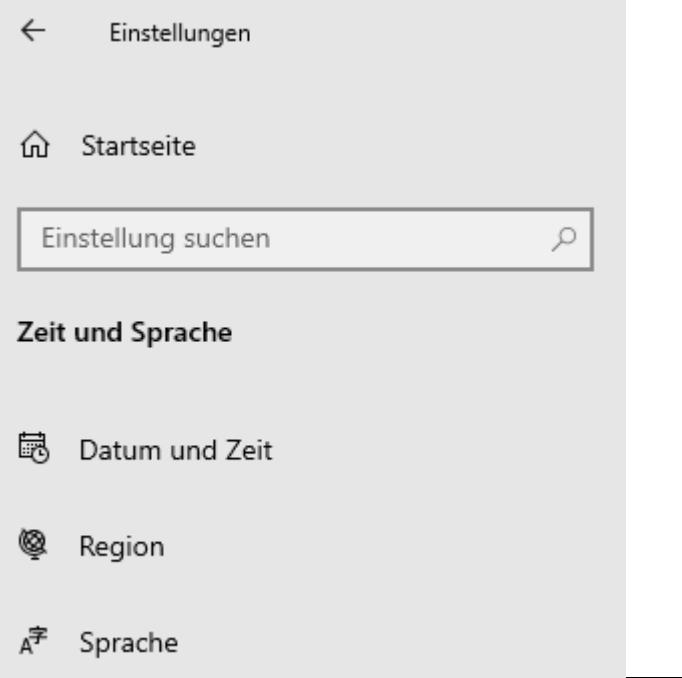
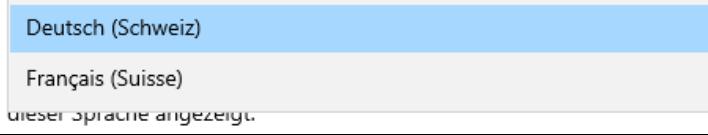
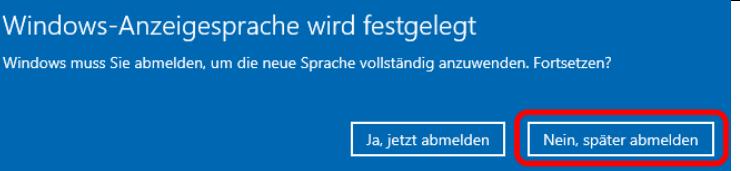
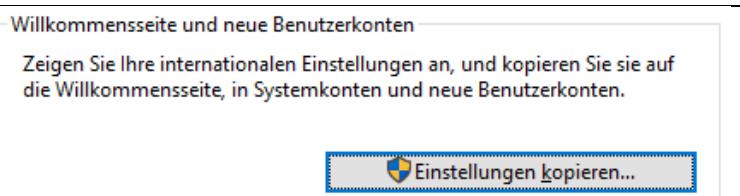
 <p>Windows wird installiert</p> <p>Status</p> <p><b>Windows-Dateien werden kopiert (0%)</b></p> <p>Dateien werden für die Installation vorbereitet</p> <p>Features werden installiert</p> <p>Updates werden installiert</p> <p>Aktion wird abgeschlossen</p>	<p>Boot the laptop from the USB stick by pressing either F9 for HP, F12 for Lenovo and Dell, or Esc for Panasonic early in the boot process.</p> <p>The Windows Setup will then automatically start</p>																						
 <p>Windows muss neu gestartet werden, um fortzufahren.</p> <p>Neustart in 7 Sekunden</p>	<p>After a while it'll reboot...</p>																						
 <pre>Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe 13.10.2022 - 15:50:26.42 - Installing software 13.10.2022 - 15:50:26.49 - KeePass 13.10.2022 - 15:50:45.64 - Result 0 13.10.2022 - 15:50:45.97 - Edge</pre>	<p>...and continue by installing drivers, applications etc</p>																						
 <pre>Administrator: Windows PowerShell 13.10.2022 - 13:00:23.67 - Installing updates 13.10.2022 - 13:00:23.80 - .NET 4.8 13.10.2022 - 13:00:54.16 - Result 3010 13.10.2022 - 13:00:54.17 - Windows Cumulative</pre>	<p>When the computer is installing updates, the USB stick can be removed</p>																						
 <p>er PC &gt; Windows (C:) &gt; ProgramData &gt;</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Änderungsdatum</th> </tr> </thead> <tbody> <tr> <td>A.E.T. Europe B.V</td> <td>13.10.2022 15:51</td> </tr> <tr> <td>Microsoft</td> <td>13.10.2022 15:54</td> </tr> <tr> <td>Packages</td> <td>13.10.2022 16:11</td> </tr> <tr> <td>regid.1991-06.com.microsoft</td> <td>13.10.2022 16:15</td> </tr> <tr> <td>SoftwareDistribution</td> <td>07.12.2019 10:14</td> </tr> <tr> <td>ssh</td> <td>06.10.2021 15:28</td> </tr> <tr> <td>USOPrivate</td> <td>07.12.2019 10:14</td> </tr> <tr> <td>USOShared</td> <td>07.12.2019 10:14</td> </tr> <tr> <td>drivers</td> <td>13.10.2022 16:16</td> </tr> <tr> <td>installs</td> <td>13.10.2022 16:16</td> </tr> </tbody> </table>	Name	Änderungsdatum	A.E.T. Europe B.V	13.10.2022 15:51	Microsoft	13.10.2022 15:54	Packages	13.10.2022 16:11	regid.1991-06.com.microsoft	13.10.2022 16:15	SoftwareDistribution	07.12.2019 10:14	ssh	06.10.2021 15:28	USOPrivate	07.12.2019 10:14	USOShared	07.12.2019 10:14	drivers	13.10.2022 16:16	installs	13.10.2022 16:16	<p>Log files about the setup are created in the directory c:\programdata</p>
Name	Änderungsdatum																						
A.E.T. Europe B.V	13.10.2022 15:51																						
Microsoft	13.10.2022 15:54																						
Packages	13.10.2022 16:11																						
regid.1991-06.com.microsoft	13.10.2022 16:15																						
SoftwareDistribution	07.12.2019 10:14																						
ssh	06.10.2021 15:28																						
USOPrivate	07.12.2019 10:14																						
USOShared	07.12.2019 10:14																						
drivers	13.10.2022 16:16																						
installs	13.10.2022 16:16																						
 <p>Geräte und Laufwerke (2)</p> <p>Windows (C:)</p> <p>37.0 GB frei von 59.0 GB</p>	<p>The hard drive will not be immediately encrypted</p>																						
 <p>Geräte und Laufwerke (2)</p> <p>Windows (C:)</p> <p>37.0 GB frei von 59.0 GB</p>	<p>After a few reboots however it'll be encrypted (if the laptop is connected to a power supply)</p>																						

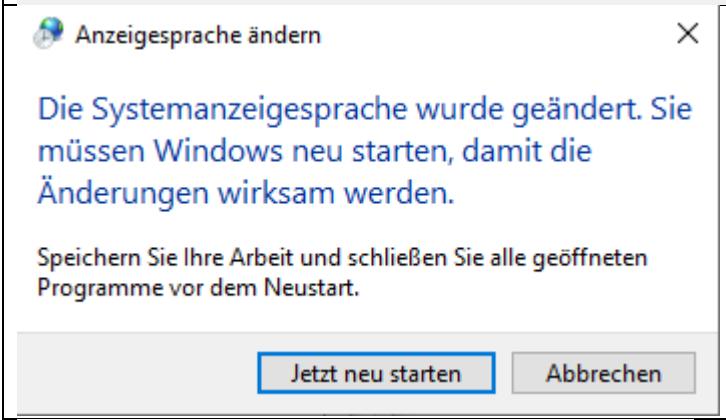
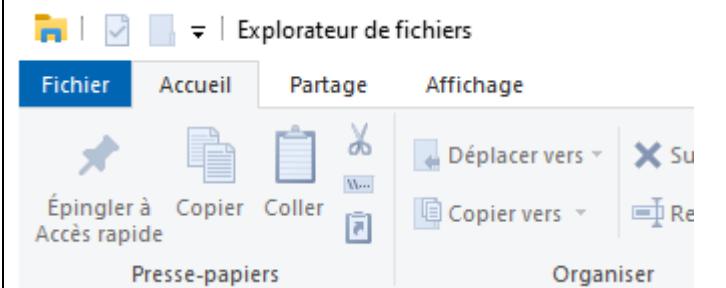
## Enable network connectivity

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>

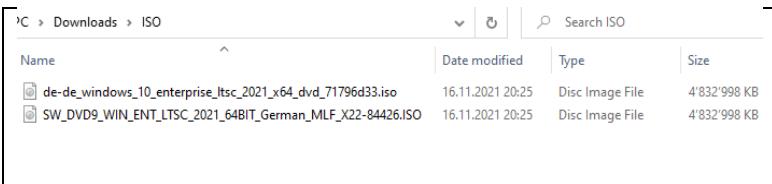
## Change language

	<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>Aktuelle Einstellungen für folgende Konten kopieren:</p> <p><input checked="" type="checkbox"/> Willkommensseite und Systemkonten</p> <p><input checked="" type="checkbox"/> Neue Benutzerkonten</p> <p style="text-align: center;"><b>OK</b> <b>Abbrechen</b></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>
<pre>PS C:\users\athman.boukhaoua\Documents\Kanton-Thurgau&gt; .\verify-image.ps1 -ReferenceISO "C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_7179633.iso" -ImageUSB d: Verifying Integrity of the reference ISO file Mounting reference ISO file Mounted to drive F: D:\System Volume Information\WPSSettings.dat not ok Results of the scan have been written to: C:\Users\athman.boukhaoua\Documents\evoting_imagecheck.csv</pre>	<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>
<pre>PS C:\users\athman.boukhaoua\Documents\Kanton-Thurgau&gt; .\verify-image.ps1 -ReferenceISO "C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_7179633.iso" -ImageUSB d: -DisplayPositiveResults Verifying Integrity of the reference ISO file Mounting reference ISO file Mounted to drive G: D:\autorun.inf ok because original D:\autorunattend.xml ok by hash D:\bootmgr ok because original D:\bootmgff ok because original D:\bootvbs ok because original D:\bootvbs.ok because original</pre>	<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			
2	3378723C1 original	ok		D:\autorun.inf			
3	E803F131A hash	ok		D:\autounattend.xml			
4	4EEAC11B original	ok		D:\bootmgr			
5	96B7EE39 original	ok		D:\bootmgr.efi			
6	30043368C original	ok		D:\setup.exe			
7	A6FB0A49 hash	failed		D:\System Volume Information\WPSettings.dat			
8	163271449 original	ok		D:\boot\bcd			
9	CD2C00CE original	ok		D:\boot\boot.sdi			
10	2F9C24282 original	ok		D:\boot\bootfix.bin			
11	55A47316 original	ok		D:\boot\bootsect.exe			
12	F425E135A 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			

The script will output a detailed report in the “Documents” directory that shows check results for all files

## 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

## v1.10

- Updates to BIOS, Windows and drivers for September 2025
- Updates to applications: 7-Zip 25.01, KeePass 2.59, Notepad++ 8.8.5, OpenSSL 3.5.2, PowerShell 7.4.12, TotalCommander 11.56

## v1.11

- Updates to BIOS, Windows and drivers for November 2025
- Updates to applications: KeePass 2.60, Notepad++ 8.8.8, OpenSSL 3.6.0, PowerShell 7.4.13

## 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/>