

Evoting – Basic installation and hardening

Version 1.4

Date 2024-03-21

Windows image documentation

Prerequisites

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

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

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)

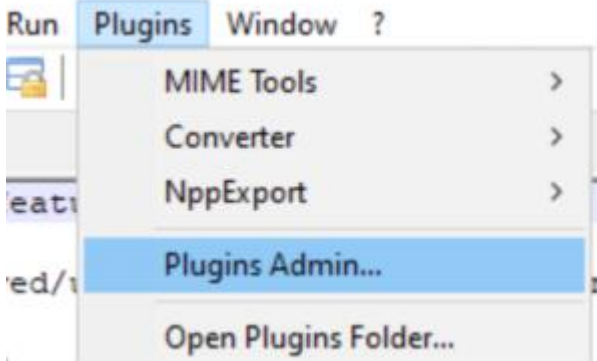
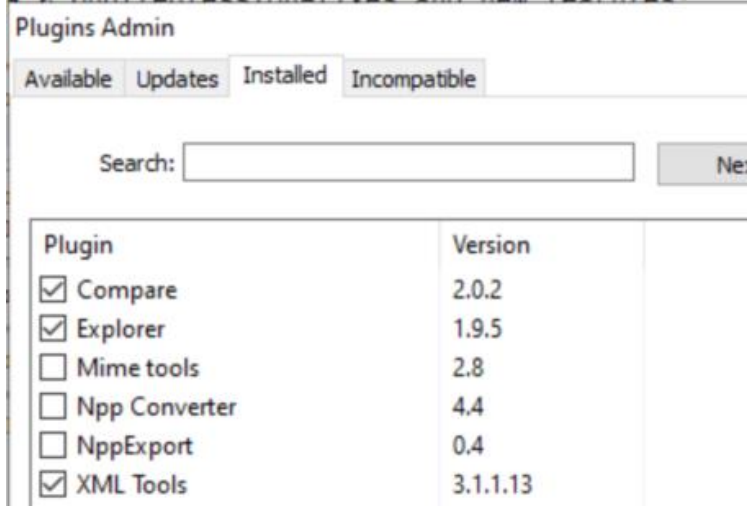
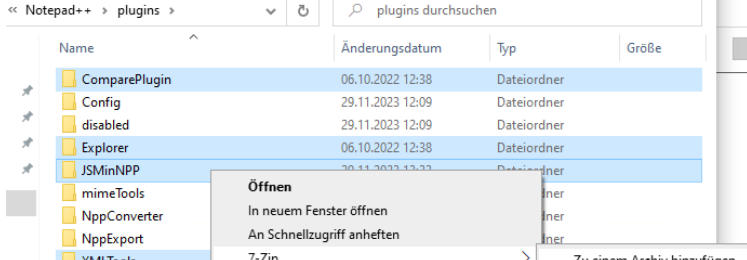
Edge

	<p>https://www.microsoft.com/de-de/edge/business/download</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++ with the following options: MIME Tools, Converter, NppExport, Plugins Admin... (highlighted), and Open Plugins Folder...</p>	<p>On a test computer, install Notepad++ and start Plugins Admin</p>																																								
 <p>The screenshot shows the 'Plugins Admin' dialog box with the 'Installed' tab selected. The following table lists the installed plugins:</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>1.9.5</td> </tr> <tr> <td><input type="checkbox"/> Mime tools</td> <td>2.8</td> </tr> <tr> <td><input type="checkbox"/> Npp Converter</td> <td>4.4</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	1.9.5	<input type="checkbox"/> Mime tools	2.8	<input type="checkbox"/> Npp Converter	4.4	<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	1.9.5																																								
<input type="checkbox"/> Mime tools	2.8																																								
<input type="checkbox"/> Npp Converter	4.4																																								
<input type="checkbox"/> NppExport	0.4																																								
<input checked="" type="checkbox"/> XML Tools	3.1.1.13																																								
 <p>The screenshot shows the file explorer view of the Notepad++ plugins folder. The following table lists the files:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Änderungsdatum</th> <th>Typ</th> <th>Größe</th> </tr> </thead> <tbody> <tr> <td>ComparePlugin</td> <td>06.10.2022 12:38</td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>Config</td> <td>29.11.2023 12:09</td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>disabled</td> <td>29.11.2023 12:09</td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>Explorer</td> <td>06.10.2022 12:38</td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>JSMInNPP</td> <td>29.11.2023 12:33</td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>mimeTools</td> <td></td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>NppConverter</td> <td></td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>NppExport</td> <td></td> <td>Dateiordner</td> <td></td> </tr> <tr> <td>XMLTools</td> <td></td> <td>Dateiordner</td> <td></td> </tr> </tbody> </table> <p>A context menu is open over the 'XMLTools' folder, showing options like 'Öffnen', 'In neuem Fenster öffnen', 'An Schnellzugriff anheften', '7-Zip', and 'Zu einem Archiv hinzufügen...'.</p>	Name	Änderungsdatum	Typ	Größe	ComparePlugin	06.10.2022 12:38	Dateiordner		Config	29.11.2023 12:09	Dateiordner		disabled	29.11.2023 12:09	Dateiordner		Explorer	06.10.2022 12:38	Dateiordner		JSMInNPP	29.11.2023 12:33	Dateiordner		mimeTools		Dateiordner		NppConverter		Dateiordner		NppExport		Dateiordner		XMLTools		Dateiordner		<p>Then package the four plugins as a self-extracting 7z archive</p>
Name	Änderungsdatum	Typ	Größe																																						
ComparePlugin	06.10.2022 12:38	Dateiordner																																							
Config	29.11.2023 12:09	Dateiordner																																							
disabled	29.11.2023 12:09	Dateiordner																																							
Explorer	06.10.2022 12:38	Dateiordner																																							
JSMInNPP	29.11.2023 12:33	Dateiordner																																							
mimeTools		Dateiordner																																							
NppConverter		Dateiordner																																							
NppExport		Dateiordner																																							
XMLTools		Dateiordner																																							

PowerShell 7

On <https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.4> download the current x64 PowerShell 7.x MSI

OpenSSL

On

http://wiki.overbyte.eu/wiki/index.php/ICS_Download#Download_OpenSSL_Binaries_.28required_for_SSL-enabled_components.29 download the latest Win-64 3.x version

SDelete

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

STunnel

Download the newest Win64 version from <https://www.stunnel.org/downloads.html>

TotalCommander

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

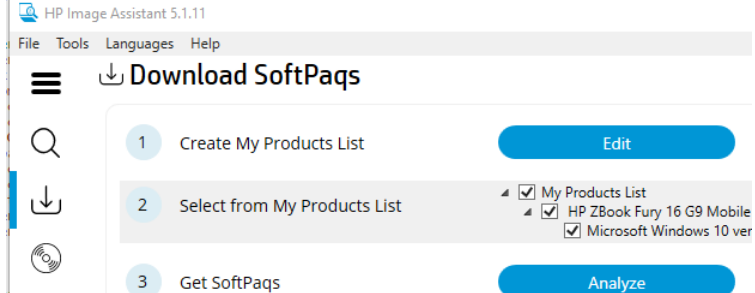
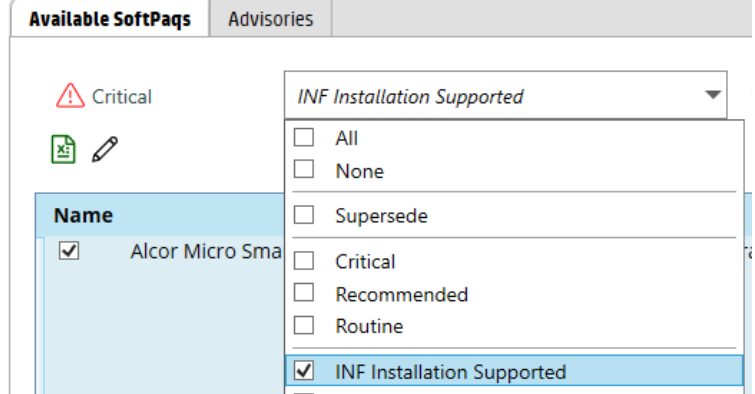
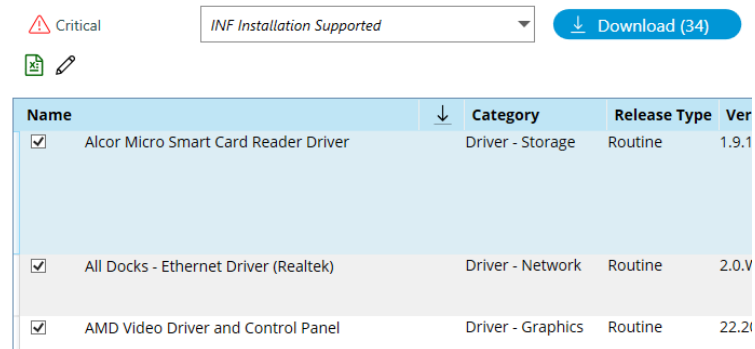
Drivers

Supported models

The following laptop models have to be supported, and their drivers integrated into the image:
EliteBook 850 G5, ThinkPad P52s (20LC), ZBook Fury 16 G9, ZBook Fury 16 G10

Additionally, we use one model for internal tests, currently that is:
ThinkPad Yoga 370 (20JH)

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>																
 <table border="1" data-bbox="207 1355 957 1601"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Release Type</th> <th>Ver</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Alcor Micro Smart Card Reader Driver</td> <td>Driver - Storage</td> <td>Routine</td> <td>1.9.1</td> </tr> <tr> <td><input checked="" type="checkbox"/> All Docks - Ethernet Driver (Realtek)</td> <td>Driver - Network</td> <td>Routine</td> <td>2.0.V</td> </tr> <tr> <td><input checked="" type="checkbox"/> AMD Video Driver and Control Panel</td> <td>Driver - Graphics</td> <td>Routine</td> <td>22.2f</td> </tr> </tbody> </table>	Name	Category	Release Type	Ver	<input checked="" type="checkbox"/> Alcor Micro Smart Card Reader Driver	Driver - Storage	Routine	1.9.1	<input checked="" type="checkbox"/> All Docks - Ethernet Driver (Realtek)	Driver - Network	Routine	2.0.V	<input checked="" type="checkbox"/> AMD Video Driver and Control Panel	Driver - Graphics	Routine	22.2f	<p>Then click "Download"</p>
Name	Category	Release Type	Ver														
<input checked="" type="checkbox"/> Alcor Micro Smart Card Reader Driver	Driver - Storage	Routine	1.9.1														
<input checked="" type="checkbox"/> All Docks - Ethernet Driver (Realtek)	Driver - Network	Routine	2.0.V														
<input checked="" type="checkbox"/> AMD Video Driver and Control Panel	Driver - Graphics	Routine	22.2f														

Download SoftPaqs
Choose "Download and Extract"

Operation

Download SoftPaq(s) only

Download and extract SoftPaqs

Folder preview

Download
C:\HPIADownloads\spXXXXX.exe

Unpack
C:\HPIADownloads\spXXXXX

Start

s PC > Windows (C:) > HPIADownloads
See

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	

Delete Multiple Items

Are you sure you want to permanently delete these 22 items?

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

Lenovo

Specify the folder, where you wish to have the repository stored.

Local repository

Packages will be hosted in a local directory or network share.

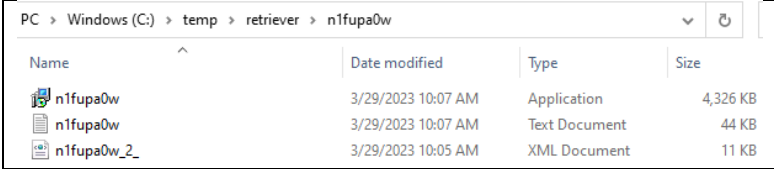
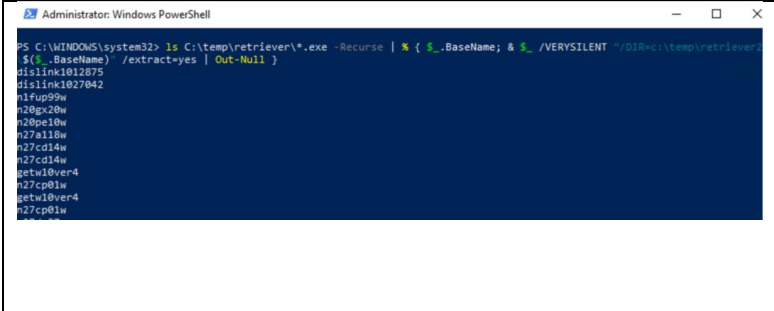
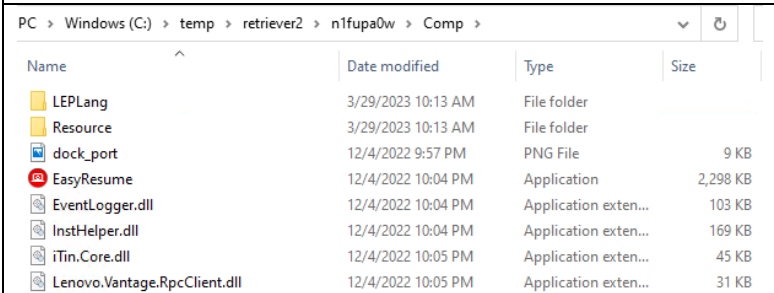
Lenovo cloud repository

Packages will be hosted by Lenovo and only the whitelist database will be stored in the local directory or network share.
Note: Lenovo System Update (version 5.07.0046 and later) supports this feature. Thin Installer does not support this feature.

Repository path:

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

	<p>Press "Continue", then "Yes"</p>																																																																																																																							
	<p>Add the laptop model you want to get drivers for</p>																																																																																																																							
	<p>Then select it and press "Next"</p>																																																																																																																							
	<p>After the search has finished, choose "Type=Driver" and press "Search"</p>																																																																																																																							
<table border="1"> <thead> <tr> <th>Title</th> <th>Update ID</th> <th>Severity</th> <th>Type</th> <th>Existing version</th> <th>Version</th> <th>Size</th> </tr> </thead> <tbody> <tr><td>Intel Dynamic Plat...</td><td>n27he01w</td><td>Recommended</td><td>Driver</td><td>-</td><td>8.3.10208.5644</td><td>3.31 MB</td></tr> <tr><td>Integrated Camera...</td><td>n27cp01w_rea</td><td>Recommended</td><td>Driver</td><td>-</td><td>10.0.16299.11319</td><td>6.70 MB</td></tr> <tr><td>Integrated Camera...</td><td>n27cp01w_sun</td><td>Recommended</td><td>Driver</td><td>-</td><td>3.5.18.32</td><td>6.70 MB</td></tr> <tr><td>Intel Bluetooth Dri...</td><td>n27ww02w</td><td>Recommended</td><td>Driver</td><td>-</td><td>20.60.0.4</td><td>1.95 MB</td></tr> <tr><td>NXP NFC Driver(W...</td><td>n27wv01w</td><td>Recommended</td><td>Driver</td><td>-</td><td>12.0.3.0</td><td>1.42 MB</td></tr> <tr><td>NXP NFC Driver (...</td><td>n27wb01w</td><td>Recommended</td><td>Driver</td><td>-</td><td>12.0.1.0</td><td>1.66 MB</td></tr> <tr><td>NXP NFC Driver (...</td><td>n27wa03w</td><td>Recommended</td><td>Driver</td><td>-</td><td>12.0.2.0</td><td>1.71 MB</td></tr> <tr><td>Fibocom L830-EB ...</td><td>n23wr01w</td><td>Recommended</td><td>Driver</td><td>-</td><td>3.2.0.1</td><td>1.37 MB</td></tr> <tr><td>Fibocom L830-EB ...</td><td>n23wr04w</td><td>Recommended</td><td>Driver</td><td>-</td><td>3.19041.2034.1</td><td>1.31 MB</td></tr> <tr><td>Intel Dynamic Plat...</td><td>n27hd06w</td><td>Recommended</td><td>Driver</td><td>-</td><td>8.4.11000.6436</td><td>3.51 MB</td></tr> <tr><td>Integrated Camera...</td><td>n27cd14w_rea</td><td>Recommended</td><td>Driver</td><td>-</td><td>10.0.19041.20176</td><td>20.50 MB</td></tr> <tr><td>Integrated Camera...</td><td>n27cd14w_sun</td><td>Recommended</td><td>Driver</td><td>-</td><td>5.0.18.88</td><td>20.50 MB</td></tr> <tr><td>Synaptics UltraNav...</td><td>n20gx20w</td><td>Critical</td><td>Driver</td><td>-</td><td>19.3.4.228</td><td>27.41 MB</td></tr> <tr><td>Intel Chipset Drive...</td><td>n27ic04w</td><td>Recommended</td><td>Driver</td><td>-</td><td>10.1.18228.8176</td><td>3.54 MB</td></tr> <tr><td>Intel PRO/1000 LA...</td><td>n27rw06w</td><td>Critical</td><td>Driver</td><td>-</td><td>12.18.9.11</td><td>1.57 MB</td></tr> <tr><td>Realtek Media Car...</td><td>n27x805w</td><td>Recommended</td><td>Driver</td><td>-</td><td>10.0.17134.31242</td><td>1.85 MB</td></tr> </tbody> </table>	Title	Update ID	Severity	Type	Existing version	Version	Size	Intel Dynamic Plat...	n27he01w	Recommended	Driver	-	8.3.10208.5644	3.31 MB	Integrated Camera...	n27cp01w_rea	Recommended	Driver	-	10.0.16299.11319	6.70 MB	Integrated Camera...	n27cp01w_sun	Recommended	Driver	-	3.5.18.32	6.70 MB	Intel Bluetooth Dri...	n27ww02w	Recommended	Driver	-	20.60.0.4	1.95 MB	NXP NFC Driver(W...	n27wv01w	Recommended	Driver	-	12.0.3.0	1.42 MB	NXP NFC Driver (...	n27wb01w	Recommended	Driver	-	12.0.1.0	1.66 MB	NXP NFC Driver (...	n27wa03w	Recommended	Driver	-	12.0.2.0	1.71 MB	Fibocom L830-EB ...	n23wr01w	Recommended	Driver	-	3.2.0.1	1.37 MB	Fibocom L830-EB ...	n23wr04w	Recommended	Driver	-	3.19041.2034.1	1.31 MB	Intel Dynamic Plat...	n27hd06w	Recommended	Driver	-	8.4.11000.6436	3.51 MB	Integrated Camera...	n27cd14w_rea	Recommended	Driver	-	10.0.19041.20176	20.50 MB	Integrated Camera...	n27cd14w_sun	Recommended	Driver	-	5.0.18.88	20.50 MB	Synaptics UltraNav...	n20gx20w	Critical	Driver	-	19.3.4.228	27.41 MB	Intel Chipset Drive...	n27ic04w	Recommended	Driver	-	10.1.18228.8176	3.54 MB	Intel PRO/1000 LA...	n27rw06w	Critical	Driver	-	12.18.9.11	1.57 MB	Realtek Media Car...	n27x805w	Recommended	Driver	-	10.0.17134.31242	1.85 MB	<p>Select all drivers and press "Next"</p>
Title	Update ID	Severity	Type	Existing version	Version	Size																																																																																																																		
Intel Dynamic Plat...	n27he01w	Recommended	Driver	-	8.3.10208.5644	3.31 MB																																																																																																																		
Integrated Camera...	n27cp01w_rea	Recommended	Driver	-	10.0.16299.11319	6.70 MB																																																																																																																		
Integrated Camera...	n27cp01w_sun	Recommended	Driver	-	3.5.18.32	6.70 MB																																																																																																																		
Intel Bluetooth Dri...	n27ww02w	Recommended	Driver	-	20.60.0.4	1.95 MB																																																																																																																		
NXP NFC Driver(W...	n27wv01w	Recommended	Driver	-	12.0.3.0	1.42 MB																																																																																																																		
NXP NFC Driver (...	n27wb01w	Recommended	Driver	-	12.0.1.0	1.66 MB																																																																																																																		
NXP NFC Driver (...	n27wa03w	Recommended	Driver	-	12.0.2.0	1.71 MB																																																																																																																		
Fibocom L830-EB ...	n23wr01w	Recommended	Driver	-	3.2.0.1	1.37 MB																																																																																																																		
Fibocom L830-EB ...	n23wr04w	Recommended	Driver	-	3.19041.2034.1	1.31 MB																																																																																																																		
Intel Dynamic Plat...	n27hd06w	Recommended	Driver	-	8.4.11000.6436	3.51 MB																																																																																																																		
Integrated Camera...	n27cd14w_rea	Recommended	Driver	-	10.0.19041.20176	20.50 MB																																																																																																																		
Integrated Camera...	n27cd14w_sun	Recommended	Driver	-	5.0.18.88	20.50 MB																																																																																																																		
Synaptics UltraNav...	n20gx20w	Critical	Driver	-	19.3.4.228	27.41 MB																																																																																																																		
Intel Chipset Drive...	n27ic04w	Recommended	Driver	-	10.1.18228.8176	3.54 MB																																																																																																																		
Intel PRO/1000 LA...	n27rw06w	Critical	Driver	-	12.18.9.11	1.57 MB																																																																																																																		
Realtek Media Car...	n27x805w	Recommended	Driver	-	10.0.17134.31242	1.85 MB																																																																																																																		
<table border="1"> <thead> <tr> <th>Title</th> <th>Update ID</th> <th>Severity</th> <th>Version</th> </tr> </thead> <tbody> <tr><td>Alcor Smart Card Reader Driver - 10 (1703 or later)/11(...</td><td>n27v104w</td><td>Recommended</td><td>1.7.46.1307</td></tr> <tr><td>Fibocom L830-EB Wireless WAN Driver - 10 (1709 or la...</td><td>n23wh04w</td><td>Recommended</td><td>3.19041.2034.1</td></tr> <tr><td>Fibocom L830-EB Wireless WAN Driver (Windows 10 B...</td><td>n23wr01w</td><td>Recommended</td><td>3.2.0.1</td></tr> <tr><td>Fibocom L850-GL Wireless WAN Driver - 10 (1709 or la...</td><td>n23wj37w_v1</td><td>Critical</td><td>2.0.1.112</td></tr> <tr><td>Generic DisplayLink Driver for ThinkPad USB 3.0 Ultra/...</td><td>dislink1012875</td><td>Recommended</td><td>10.1.2875.0</td></tr> <tr><td>Generic DisplayLink Driver for USB Docks and Adapter...</td><td>dislink1027042</td><td>Recommended</td><td>10.2.7042.0</td></tr> <tr><td>Integrated Camera Driver for Realtek - 10 (1709 or later...</td><td>n27cd14w_rea</td><td>Recommended</td><td>10.0.19041.20176</td></tr> <tr><td>Integrated Camera Driver for Realtek(Windows 10 Buil...</td><td>n27cp01w_rea</td><td>Recommended</td><td>10.0.16299.11319</td></tr> <tr><td>Integrated Camera Driver for Sunplus - 10 (1709 or late...</td><td>n27cd14w_sun</td><td>Recommended</td><td>5.0.18.88</td></tr> <tr><td>Integrated Camera Driver for Sunplus(Windows 10 Buil...</td><td>n27cp01w_sun</td><td>Recommended</td><td>3.5.18.32</td></tr> <tr><td>Intel 8265 Wireless LAN Driver - 10 (1809 or Later)/11(2...</td><td>n24w810w</td><td>Critical</td><td>20.70.30.1</td></tr> <tr><td>Intel 8265 Wireless LAN Driver (Windows 10 Version 18...</td><td>n24w807w</td><td>Critical</td><td>20.70.18.2</td></tr> <tr><td>Intel Bluetooth Driver - 10 (1709 or Later)/11 (21H2 or ...</td><td>n27ww11w</td><td>Critical</td><td>22.150.0.6</td></tr> <tr><td>Intel Bluetooth Driver(Windows 10 Build 1703) - 10 [64]</td><td>n27ww02w</td><td>Recommended</td><td>20.60.0.4</td></tr> <tr><td>Intel Chipset Driver - 10 /11 (21H2 or later)</td><td>n27ic04w</td><td>Recommended</td><td>10.1.18228.8176</td></tr> <tr><td>Intel Dynamic Platform and Thermal Framework - 10 (...</td><td>n27hd06w</td><td>Recommended</td><td>8.4.11000.6436</td></tr> <tr><td>Intel Dynamic Platform And Thermal Framework (Win...</td><td>n27he01w</td><td>Recommended</td><td>8.3.10208.5644</td></tr> <tr><td>Intel Gigabit Ethernet Driver - 10 (1809 or later)/11 (21...</td><td>n27rv06w</td><td>Recommended</td><td>12.19.1.37</td></tr> <tr><td>Intel Graphics Driver - 10 (1703 or Later)/11(21H2 or La...</td><td>n27dt22w</td><td>Critical</td><td>30.0.100.9865</td></tr> <tr><td>Intel Management Engine Software - 10 (1703 or Later)...</td><td>n27ra21w</td><td>Critical</td><td>2205.15.0.2623</td></tr> <tr><td>Intel PRO/1000 LAN Adapter Software(Windows 10 Ver...</td><td>n27rw06w</td><td>Critical</td><td>12.18.9.11</td></tr> <tr><td>Intel Serial IO Driver - 10 (1809 or Later)/11(21H2 or Lat...</td><td>n27j01w</td><td>Recommended</td><td>30.100.1841.2</td></tr> </tbody> </table>	Title	Update ID	Severity	Version	Alcor Smart Card Reader Driver - 10 (1703 or later)/11(...	n27v104w	Recommended	1.7.46.1307	Fibocom L830-EB Wireless WAN Driver - 10 (1709 or la...	n23wh04w	Recommended	3.19041.2034.1	Fibocom L830-EB Wireless WAN Driver (Windows 10 B...	n23wr01w	Recommended	3.2.0.1	Fibocom L850-GL Wireless WAN Driver - 10 (1709 or la...	n23wj37w_v1	Critical	2.0.1.112	Generic DisplayLink Driver for ThinkPad USB 3.0 Ultra/...	dislink1012875	Recommended	10.1.2875.0	Generic DisplayLink Driver for USB Docks and Adapter...	dislink1027042	Recommended	10.2.7042.0	Integrated Camera Driver for Realtek - 10 (1709 or later...	n27cd14w_rea	Recommended	10.0.19041.20176	Integrated Camera Driver for Realtek(Windows 10 Buil...	n27cp01w_rea	Recommended	10.0.16299.11319	Integrated Camera Driver for Sunplus - 10 (1709 or late...	n27cd14w_sun	Recommended	5.0.18.88	Integrated Camera Driver for Sunplus(Windows 10 Buil...	n27cp01w_sun	Recommended	3.5.18.32	Intel 8265 Wireless LAN Driver - 10 (1809 or Later)/11(2...	n24w810w	Critical	20.70.30.1	Intel 8265 Wireless LAN Driver (Windows 10 Version 18...	n24w807w	Critical	20.70.18.2	Intel Bluetooth Driver - 10 (1709 or Later)/11 (21H2 or ...	n27ww11w	Critical	22.150.0.6	Intel Bluetooth Driver(Windows 10 Build 1703) - 10 [64]	n27ww02w	Recommended	20.60.0.4	Intel Chipset Driver - 10 /11 (21H2 or later)	n27ic04w	Recommended	10.1.18228.8176	Intel Dynamic Platform and Thermal Framework - 10 (...	n27hd06w	Recommended	8.4.11000.6436	Intel Dynamic Platform And Thermal Framework (Win...	n27he01w	Recommended	8.3.10208.5644	Intel Gigabit Ethernet Driver - 10 (1809 or later)/11 (21...	n27rv06w	Recommended	12.19.1.37	Intel Graphics Driver - 10 (1703 or Later)/11(21H2 or La...	n27dt22w	Critical	30.0.100.9865	Intel Management Engine Software - 10 (1703 or Later)...	n27ra21w	Critical	2205.15.0.2623	Intel PRO/1000 LAN Adapter Software(Windows 10 Ver...	n27rw06w	Critical	12.18.9.11	Intel Serial IO Driver - 10 (1809 or Later)/11(21H2 or Lat...	n27j01w	Recommended	30.100.1841.2	<p>"Finish"</p>																											
Title	Update ID	Severity	Version																																																																																																																					
Alcor Smart Card Reader Driver - 10 (1703 or later)/11(...	n27v104w	Recommended	1.7.46.1307																																																																																																																					
Fibocom L830-EB Wireless WAN Driver - 10 (1709 or la...	n23wh04w	Recommended	3.19041.2034.1																																																																																																																					
Fibocom L830-EB Wireless WAN Driver (Windows 10 B...	n23wr01w	Recommended	3.2.0.1																																																																																																																					
Fibocom L850-GL Wireless WAN Driver - 10 (1709 or la...	n23wj37w_v1	Critical	2.0.1.112																																																																																																																					
Generic DisplayLink Driver for ThinkPad USB 3.0 Ultra/...	dislink1012875	Recommended	10.1.2875.0																																																																																																																					
Generic DisplayLink Driver for USB Docks and Adapter...	dislink1027042	Recommended	10.2.7042.0																																																																																																																					
Integrated Camera Driver for Realtek - 10 (1709 or later...	n27cd14w_rea	Recommended	10.0.19041.20176																																																																																																																					
Integrated Camera Driver for Realtek(Windows 10 Buil...	n27cp01w_rea	Recommended	10.0.16299.11319																																																																																																																					
Integrated Camera Driver for Sunplus - 10 (1709 or late...	n27cd14w_sun	Recommended	5.0.18.88																																																																																																																					
Integrated Camera Driver for Sunplus(Windows 10 Buil...	n27cp01w_sun	Recommended	3.5.18.32																																																																																																																					
Intel 8265 Wireless LAN Driver - 10 (1809 or Later)/11(2...	n24w810w	Critical	20.70.30.1																																																																																																																					
Intel 8265 Wireless LAN Driver (Windows 10 Version 18...	n24w807w	Critical	20.70.18.2																																																																																																																					
Intel Bluetooth Driver - 10 (1709 or Later)/11 (21H2 or ...	n27ww11w	Critical	22.150.0.6																																																																																																																					
Intel Bluetooth Driver(Windows 10 Build 1703) - 10 [64]	n27ww02w	Recommended	20.60.0.4																																																																																																																					
Intel Chipset Driver - 10 /11 (21H2 or later)	n27ic04w	Recommended	10.1.18228.8176																																																																																																																					
Intel Dynamic Platform and Thermal Framework - 10 (...	n27hd06w	Recommended	8.4.11000.6436																																																																																																																					
Intel Dynamic Platform And Thermal Framework (Win...	n27he01w	Recommended	8.3.10208.5644																																																																																																																					
Intel Gigabit Ethernet Driver - 10 (1809 or later)/11 (21...	n27rv06w	Recommended	12.19.1.37																																																																																																																					
Intel Graphics Driver - 10 (1703 or Later)/11(21H2 or La...	n27dt22w	Critical	30.0.100.9865																																																																																																																					
Intel Management Engine Software - 10 (1703 or Later)...	n27ra21w	Critical	2205.15.0.2623																																																																																																																					
Intel PRO/1000 LAN Adapter Software(Windows 10 Ver...	n27rw06w	Critical	12.18.9.11																																																																																																																					
Intel Serial IO Driver - 10 (1809 or Later)/11(21H2 or Lat...	n27j01w	Recommended	30.100.1841.2																																																																																																																					
	<p>Wait for the downloads to finish</p>																																																																																																																							

	<p>This will create a lot of directories with drivers inside executable archives</p>
	<p>Use the following command in a window with admin rights to extract the packages:</p> <pre>ls C:\temp\retriever*.exe - Recurse % { \$_.BaseName; & \$_ /VERYSILENT "/DIR=c:\temp\retriever2\\$(\$_. BaseName)"} /extract=yes Out- Null }</pre>
	<p>This extracts the archive to usable file collections</p>

Driver package adjustments

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

HP 850 G3:

- Delete the driver for “HP Universal Camera Driver” (currently SP112983)
- Delete the driver for “Conexant HD Audio Driver” (currently SP111438)

HP 850 G5:

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

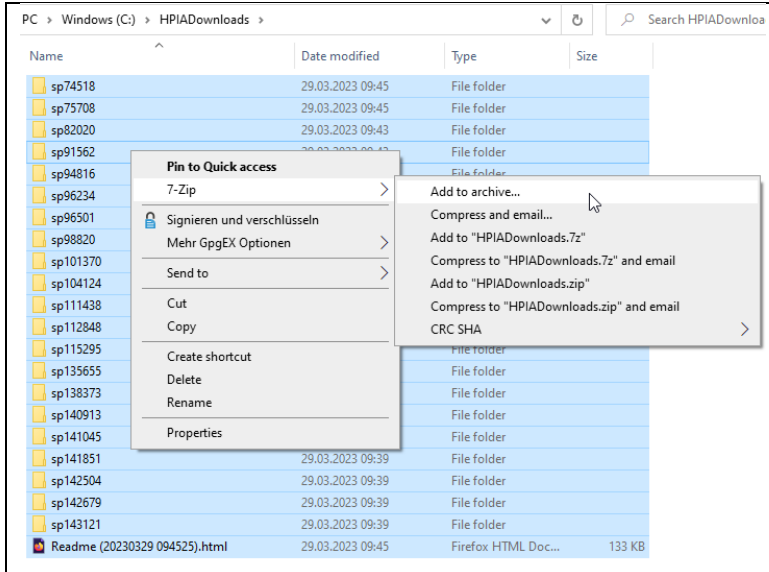
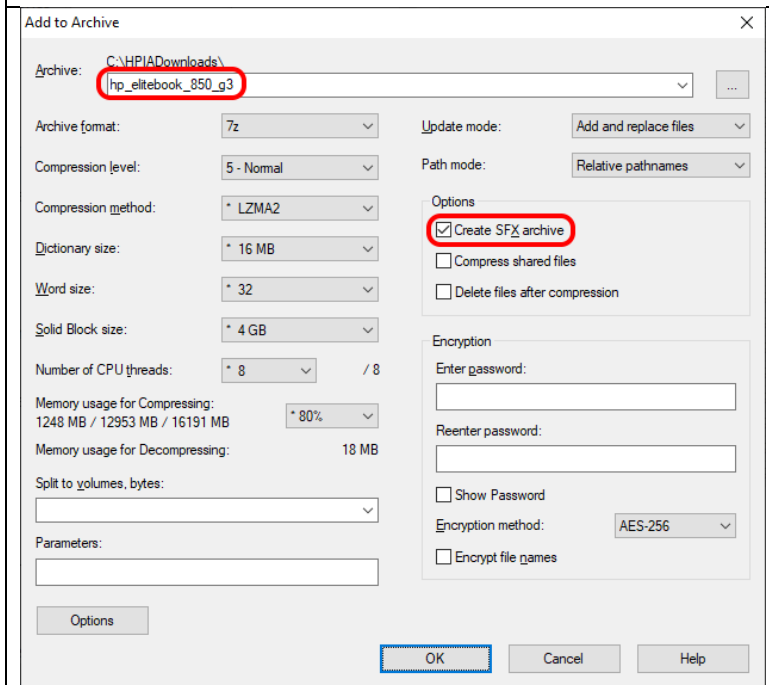
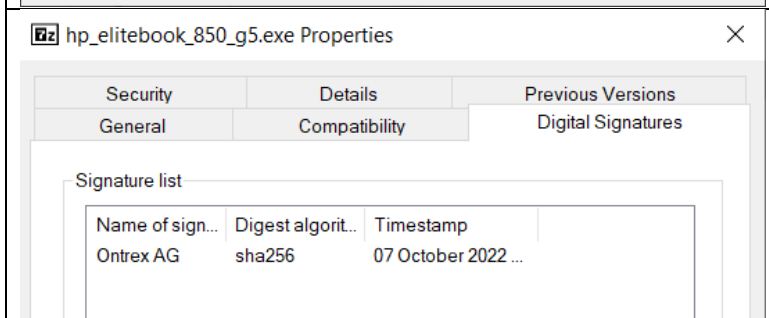
HP ZBook Fury 16 G9:

- Delete the driver for “AMD Video Driver” (currently SP149612)
- Delete the driver for “Realtek HD Audio” (currently SP149614)
- Delete the driver for “Intel XMM LTE” (currently SP145803)

HP ZBook Fury 16 G10:

- Delete duplicate Intel Video drivers
- Delete the driver for “Realtek HD Audio” (currently SP149617)
- Delete the driver for “Intel XMM LTE” (currently SP147369 and SP145373)

Create the package

	<p>Add the extracted folders to a 7zip archive</p>
	<p>As self-extracting archive 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 https://catalog.update.microsoft.com/Home.aspx and search for the KB article numbers in the top right</p>												
<table border="1"> <tr> <td>2022-09 Dynamic Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5017308)</td> <td>Windows 10 and later GDR-DU</td> <td>Security Updates</td> <td>9/13/2022</td> </tr> <tr> <td>2022-09 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5017308)</td> <td>Windows 10 LTSB, Windows 10, version 1903 and later</td> <td>Security Updates</td> <td>9/13/2022</td> </tr> <tr> <td>2022-09 Dynamic Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5017308)</td> <td>Windows 10 and later GDR-DU</td> <td>Security Updates</td> <td>9/13/2022</td> </tr> </table>	2022-09 Dynamic Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5017308)	Windows 10 and later GDR-DU	Security Updates	9/13/2022	2022-09 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5017308)	Windows 10 LTSB, Windows 10, version 1903 and later	Security Updates	9/13/2022	2022-09 Dynamic Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5017308)	Windows 10 and later GDR-DU	Security Updates	9/13/2022	<p>For the monthly updates, download the regular cumulative update, not the dynamic one</p>
2022-09 Dynamic Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5017308)	Windows 10 and later GDR-DU	Security Updates	9/13/2022										
2022-09 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5017308)	Windows 10 LTSB, Windows 10, version 1903 and later	Security Updates	9/13/2022										
2022-09 Dynamic Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5017308)	Windows 10 and later GDR-DU	Security Updates	9/13/2022										
<p>2022-09 Vorschau zum kumulativen Update für .NET Framework 3.5, 4.8 und 4.8.1 für Windows 10 Version 21H2 für x64 (KB5017858)</p> <p>windows10.0-kb5017266-x64-ndp481_14c793f0ce6cf80f1205443eaac246c122527851.msu windows10.0-kb5017262-x64-ndp48_e542f896b1eeb55650f12ec7002848c0698de45d.msu</p>	<p>For .NET only download the 4.8.1 package, not the 4.8</p>												
<table border="1"> <tr> <td>Windows Malicious Software Removal Tool - v5.106 (KB890830)</td> <td>Windows 7, Windows Server 2008</td> <td>Update Rollups</td> <td>10/11/2022</td> </tr> <tr> <td>Windows Malicious Software Removal Tool x64 - v5.106 (KB890830)</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>Windows Malicious Software Removal Tool - v5.106 (KB890830)</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>	Windows Malicious Software Removal Tool - v5.106 (KB890830)	Windows 7, Windows Server 2008	Update Rollups	10/11/2022	Windows Malicious Software Removal Tool x64 - v5.106 (KB890830)	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	Windows Malicious Software Removal Tool - v5.106 (KB890830)	Windows 8.1, Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later, Windows 11	Update Rollups	10/11/2022	<p>For the malicious software removal tool, sort by date, then pick the newest package for Windows 10 64 bit</p>
Windows Malicious Software Removal Tool - v5.106 (KB890830)	Windows 7, Windows Server 2008	Update Rollups	10/11/2022										
Windows Malicious Software Removal Tool x64 - v5.106 (KB890830)	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										
Windows Malicious Software Removal Tool - v5.106 (KB890830)	Windows 8.1, Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later, Windows 11	Update Rollups	10/11/2022										
<p>.NET Desktop Runtime 6.0.15</p> <p>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.</p> <table border="1"> <thead> <tr> <th>OS</th> <th>Installers</th> <th>Binaries</th> </tr> </thead> <tbody> <tr> <td>Windows</td> <td>Arm64 x64 x86 winget instructions</td> <td></td> </tr> </tbody> </table>	OS	Installers	Binaries	Windows	Arm64 x64 x86 winget instructions		<p>For .NET 6, go to https://dotnet.microsoft.com/en-us/download/dotnet/6.0 and download the newest "Desktop Runtime" for x64</p>						
OS	Installers	Binaries											
Windows	Arm64 x64 x86 winget instructions												

Microsoft Defender

	<p>On https://www.microsoft.com/en-us/wdsi/defenderupdates Download the 64-bit Version for the antivirus definitions</p>				
<table border="1"> <tr> <td>Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2211.5)</td> <td>Microsoft Defender Antivirus</td> <td>Definition Updates</td> <td>12/8/2022</td> </tr> </table>	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2211.5)	Microsoft Defender Antivirus	Definition Updates	12/8/2022	<p>For the antimalware update, download the newest "Definition Updates" package</p>
Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2211.5)	Microsoft Defender Antivirus	Definition Updates	12/8/2022		
<p>updateplatform.x86fre_85dfdcc7cc8df1062fc64ae81dbe0fc3b4e20e45.exe updateplatform.amd64fre_7f1e1eb218c67263a51f402fb080f1bbe311041b.exe updateplatform.arm64fre_9383ac7ca8917dc66023c6ff68d3679c8285f6bc.exe</p>	<p>Pick the one for "amd64fre"</p>				

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> <table border="1"> <thead> <tr> <th><input type="checkbox"/> File Name</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Windows 11 version 22H2 Security Baseline.zip</td> <td>1.4 MB</td> </tr> <tr> <td><input checked="" type="checkbox"/> LGPO.zip</td> <td>520 KB</td> </tr> <tr> <td><input type="checkbox"/> Windows 10 version 21H1 Security Baseline.zip</td> <td>1.2 MB</td> </tr> <tr> <td><input checked="" type="checkbox"/> Windows 10 version 21H2 Security Baseline.zip</td> <td>1.2 MB</td> </tr> <tr> <td><input type="checkbox"/> Windows 11 Security Baseline.zip</td> <td>1.2 MB</td> </tr> </tbody> </table>	<input type="checkbox"/> File Name	Size	<input type="checkbox"/> Windows 11 version 22H2 Security Baseline.zip	1.4 MB	<input checked="" type="checkbox"/> LGPO.zip	520 KB	<input type="checkbox"/> Windows 10 version 21H1 Security Baseline.zip	1.2 MB	<input checked="" type="checkbox"/> Windows 10 version 21H2 Security Baseline.zip	1.2 MB	<input type="checkbox"/> Windows 11 Security Baseline.zip	1.2 MB	<p>On https://www.microsoft.com/en-us/download/details.aspx?id=55319 download LGPO.exe</p>
<input type="checkbox"/> File Name	Size												
<input type="checkbox"/> Windows 11 version 22H2 Security Baseline.zip	1.4 MB												
<input checked="" type="checkbox"/> LGPO.zip	520 KB												
<input type="checkbox"/> Windows 10 version 21H1 Security Baseline.zip	1.2 MB												
<input checked="" type="checkbox"/> Windows 10 version 21H2 Security Baseline.zip	1.2 MB												
<input type="checkbox"/> Windows 11 Security Baseline.zip	1.2 MB												
	<p>And the baselines for 21H2</p>												

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> igpo /parse /m "\\(230EF82E-039F-40D5-BBCC-35444958D065)\DomainSysvol\GPO\Machine\registry.pol" /q > i
e_computer.txt
PS C:\temp2\GPOs> igpo /parse /m "\\(4B6589C2-0290-4764-8058-9825B56B4169)\DomainSysvol\GPO\User\registry.pol" /q > use
r.txt
PS C:\temp2\GPOs> igpo /parse /m "\\(7AD4F62E-9296-4FEA-9765-C4E3EEAAEC1)\DomainSysvol\GPO\Machine\registry.pol" /q >
credentialguard.txt
PS C:\temp2\GPOs> igpo /parse /m "\\(B669E0C6-C1E3-4582-B797-FE384B21CD01)\DomainSysvol\GPO\Machine\registry.pol" /q > d
efender.txt
PS C:\temp2\GPOs> igpo /parse /m "\\(B697C660-A87B-4AF1-B37D-9440912605E7)\DomainSysvol\GPO\Machine\registry.pol" /q > b
itlocker.txt
PS C:\temp2\GPOs> igpo /parse /m "\\(C94113F4-C027-4F5F-8210-85F4AC2C6082)\DomainSysvol\GPO\User\registry.pol" /q > ieu
ser.txt
PS C:\temp2\GPOs> igpo /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

```

52 log - Set hardening rules from Swiss Post"
53 log - Registry keys"
54
55 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer, "NoAddPrinter", 1)
56 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers, "AddPrinterB
57 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Wscntfy\Parameters, "Start", 0)
58 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole, "SecurityLevel", 0)
59 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer, "Narrow", 1)
60 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\PrivateProfile, "DefaultInboundAction", 1)
61 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\PrivateProfile, "DefaultInboundExceptions", 1)
62 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\PublicProfile, "DefaultInboundAction", 1)
63 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\PublicProfile, "DefaultInboundExceptions", 1)
64 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TopIP\Parameters, "DisableComponents", 0)
65 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections, "NC_ShowShareAccessUI", 0)
66 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, "NoConnectToWork", 1)
67 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, "NoConnectToWork", 1)
68 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, "NoConnectToWork", 1)
69 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, "NoConnectToWork", 1)
70 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, "NoConnectToWork", 1)
71 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, "NoConnectToWork", 1)
72 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, "NoConnectToWork", 1)
73
74 log - Disable Teredo"
75 netsh interface teredo set state disabled
76 log - Result SLASSTEXTCODE"
77
78 log - Disable guest user"
79 net user guest /active:no
80 log - Result SLASSTEXTCODE"
81
82 log - Changing Audit Policy"
83 auditpol /set /subcategory:"Authentifizierungsrichtlinienänderung" /success:enable /failure:disable
84 auditpol /set /subcategory:"Autorisierungsrichtlinienänderung" /success:enable /failure:enable
85 auditpol /set /subcategory:"Richtlinienänderungen überwachen" /success:enable /failure:enable
86
87 log - Block ICMP"
88 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\FirewallRules, "Custom-Block-ICMPv4", "v2.30Act1
89 [Microsoft.Windows.Common-UI::SetValue(HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\FirewallRules, "Custom-Block-ICMPv4", "v2.30Act1

```

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

CIS Benchmark

```

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

```

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

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

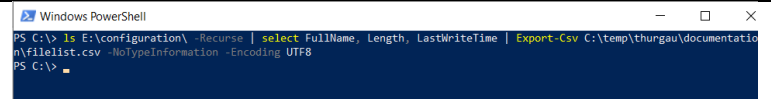
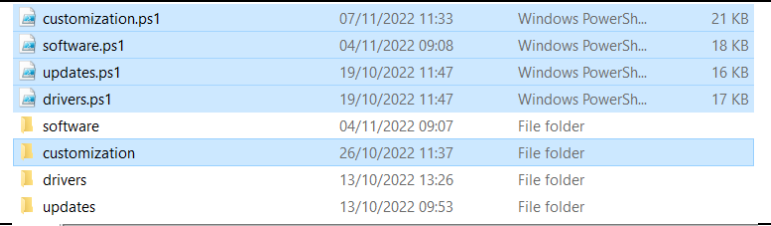
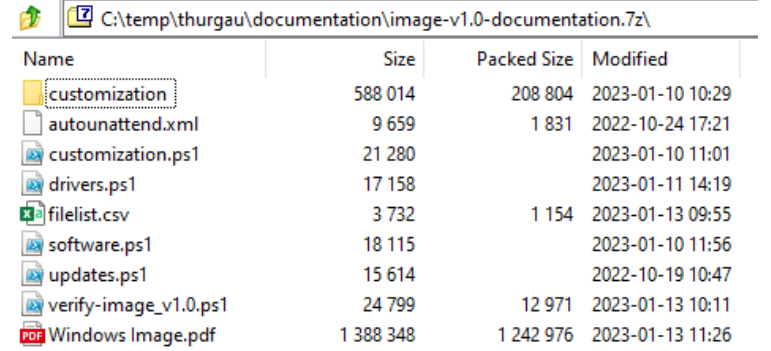
Checklist for image update



When a new version of the image has to be 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.
- 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,
- 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

Create documentation to publish

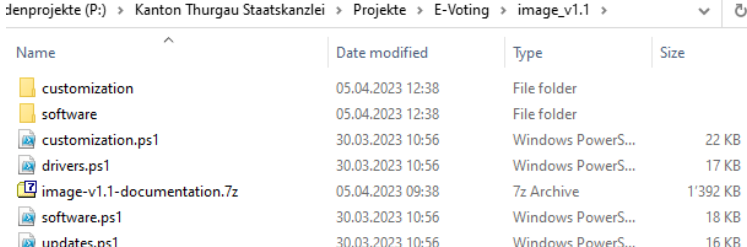
We need to make available a collection of files to the public to document what we've done and allow some transparency to the voters. We create an archive of script and documentation files and provide that to the customer who takes care of the publishing itself.

 <pre>PS C:\> ls E:\configuration\ -Recurse select FullName, Length, LastWriteTime Export-Csv C:\temp\thurgau\documentation\filelist.csv -NoTypeInformation -Encoding UTF8</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:\temp\thurgau\documentation\filelist.csv -NoTypeInformation -Encoding UTF8</pre>																																								
 <table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Modified</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>customization.ps1</td> <td>07/11/2022 11:33</td> <td>Windows PowerSh...</td> <td>21 KB</td> </tr> <tr> <td>software.ps1</td> <td>04/11/2022 09:08</td> <td>Windows PowerSh...</td> <td>18 KB</td> </tr> <tr> <td>updates.ps1</td> <td>19/10/2022 11:47</td> <td>Windows PowerSh...</td> <td>16 KB</td> </tr> <tr> <td>drivers.ps1</td> <td>19/10/2022 11:47</td> <td>Windows PowerSh...</td> <td>17 KB</td> </tr> <tr> <td>software</td> <td>04/11/2022 09:07</td> <td>File folder</td> <td></td> </tr> <tr> <td>customization</td> <td>26/10/2022 11:37</td> <td>File folder</td> <td></td> </tr> <tr> <td>drivers</td> <td>13/10/2022 13:26</td> <td>File folder</td> <td></td> </tr> <tr> <td>updates</td> <td>13/10/2022 09:53</td> <td>File folder</td> <td></td> </tr> </tbody> </table>	Name	Size	Modified	Type	customization.ps1	07/11/2022 11:33	Windows PowerSh...	21 KB	software.ps1	04/11/2022 09:08	Windows PowerSh...	18 KB	updates.ps1	19/10/2022 11:47	Windows PowerSh...	16 KB	drivers.ps1	19/10/2022 11:47	Windows PowerSh...	17 KB	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 zip file...</p>				
Name	Size	Modified	Type																																						
customization.ps1	07/11/2022 11:33	Windows PowerSh...	21 KB																																						
software.ps1	04/11/2022 09:08	Windows PowerSh...	18 KB																																						
updates.ps1	19/10/2022 11:47	Windows PowerSh...	16 KB																																						
drivers.ps1	19/10/2022 11:47	Windows PowerSh...	17 KB																																						
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>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>	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"> • autounattend.xml • filelist.csv • the image verification script • image documentation Word file as a PDF
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																																						

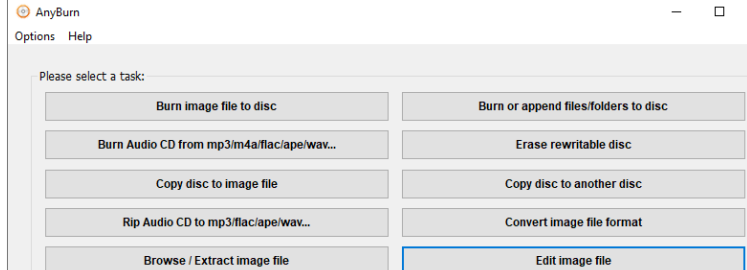
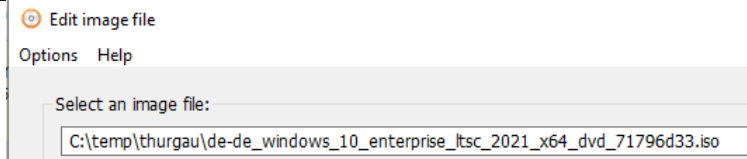
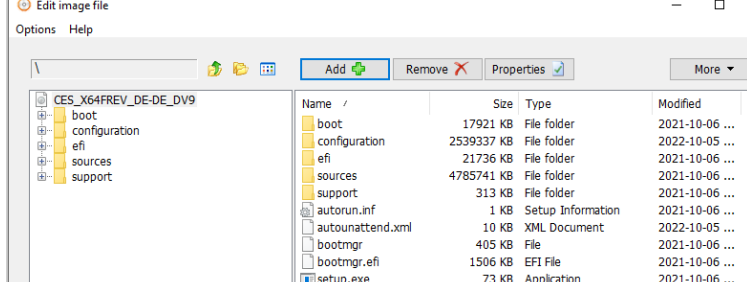
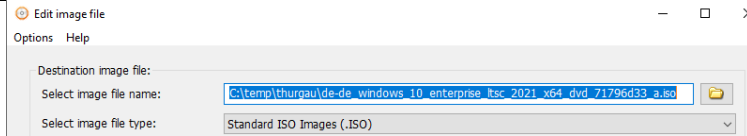
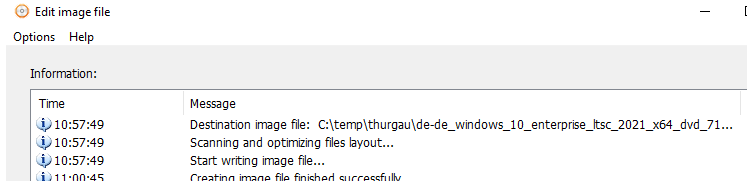
  image-v0.5-documentation.7z	Upload the resulting file
--	---------------------------

Archival

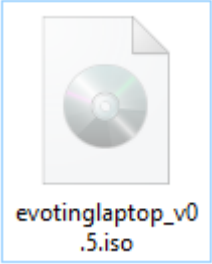


While we don't archive the full ISO files due to space issues, we want to archive the most important files for future reference.

	Create a subdirectory for the current image version, and copy the four ps1 files as well as the documentation 7z, as well as the full "customization" directory and the full "software" directory
---	---

Create the bootable ISO

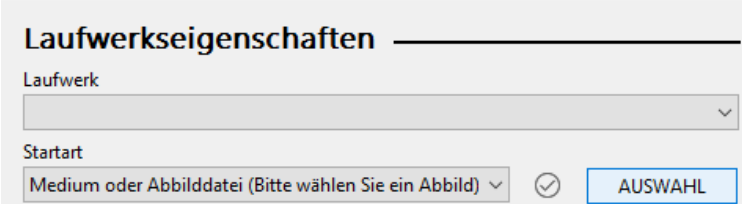
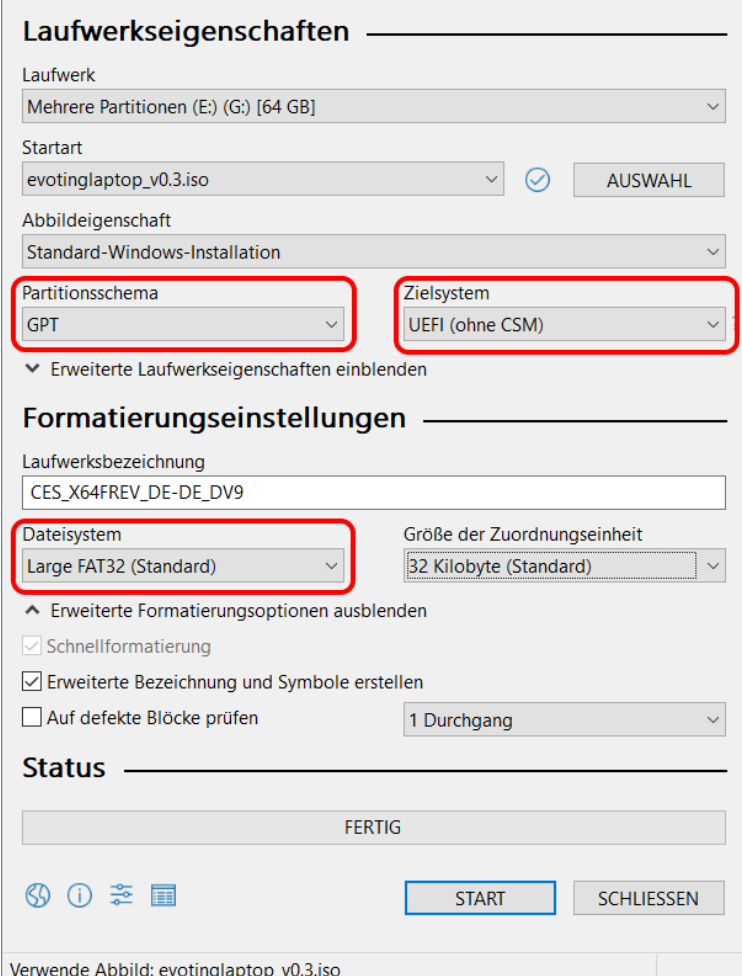
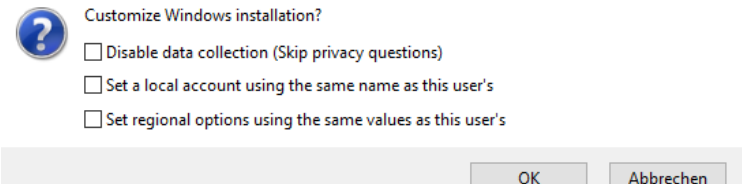
	Start Anyburn, then choose "Edit Image"
	Open a bootable ISO file
	Add the "autounattend.xml" and the "configuration" directory
	Save under a different name
	Wait until it's finished

Upload the image

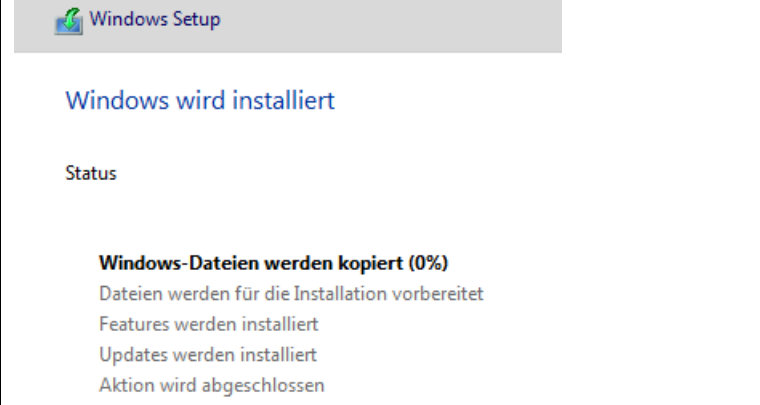
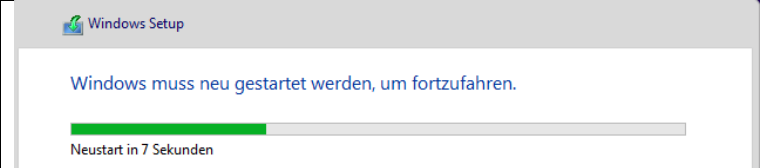
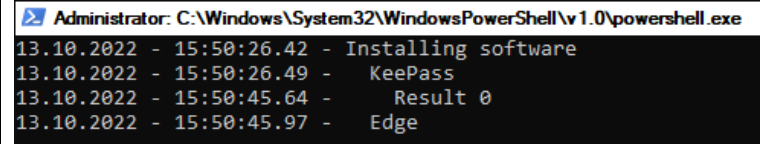
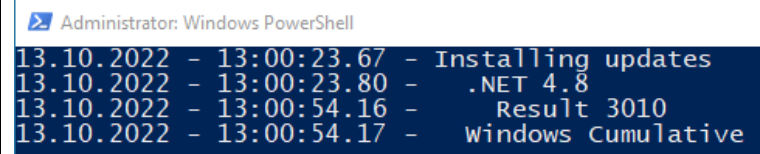
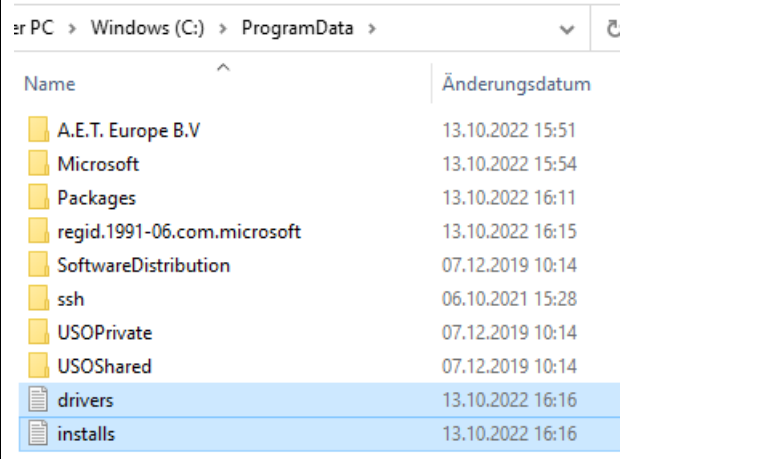
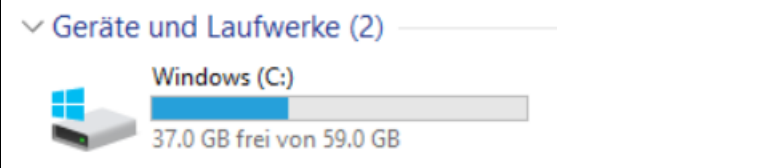
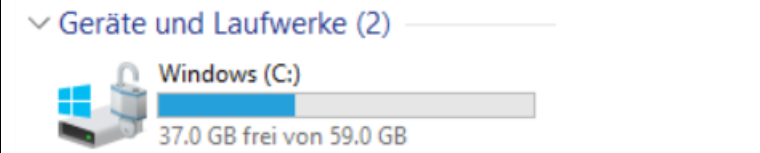
 <p>evotinglaptop_v0 .iso</p>	<p>Rename the resulting image to evotinglaptop_vx.y.iso</p>
<p>All Files > Kiteworks > Kanton Thurgau</p> <p><input type="checkbox"/> Name ^</p> <hr/> <p><input type="checkbox"/>  Upload</p> <hr/> <p><input type="checkbox"/>  evotinglaptop_v0.5.iso</p>	<p>And upload it to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

User Guide

Extract the ISO to a USB Stick

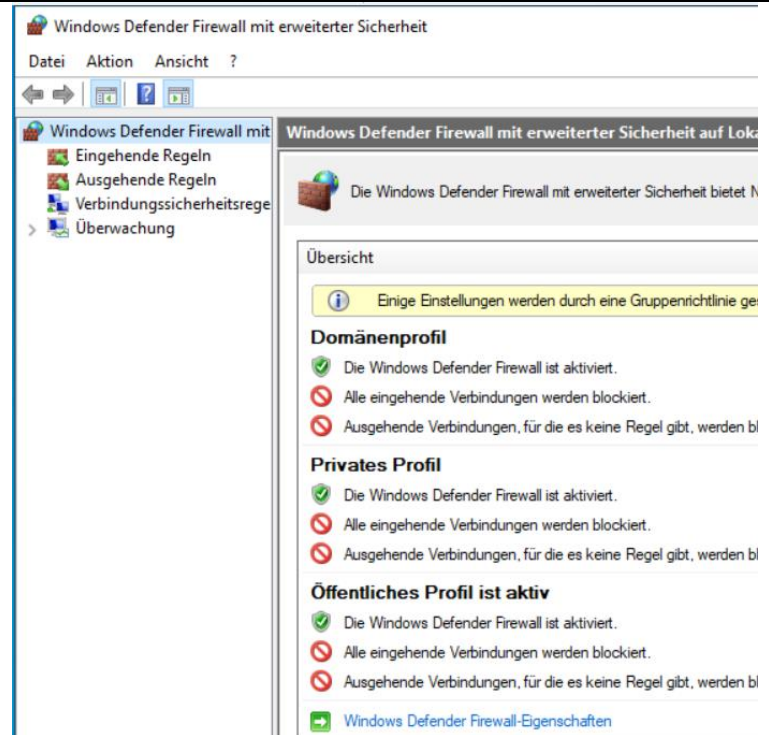
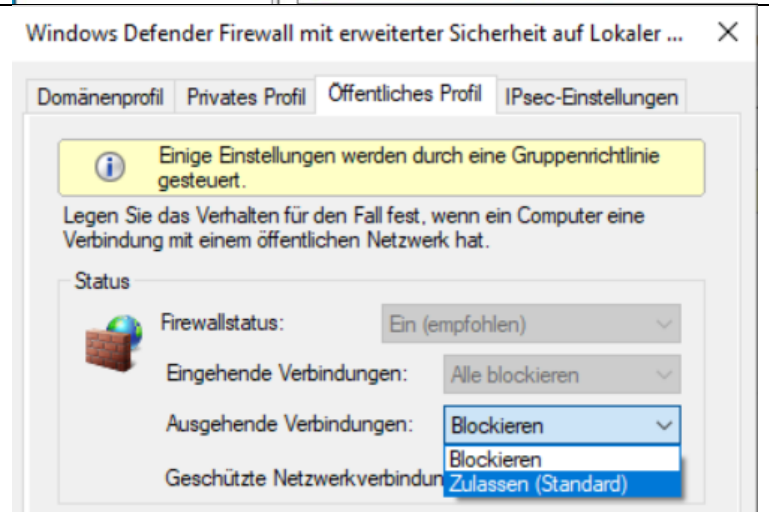

	<p>Start Rufus and select the ISO file</p>
	<p>Use GPT, UEFI (without CSM) and Large FAT32 as options</p> <p>Do not modify the drive name, it has to stay on the default value</p>
	<p>Do not let Rufus do any adjustments to the Windows installation</p>

Apply the image to a computer

	<p>Boot the laptop from the USB stick by pressing either F9 for HP or F12 for Lenovo 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>

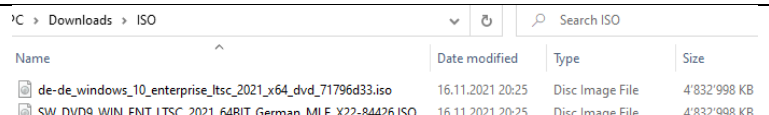
Enable network connectivity

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>

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 the Microsoft VLSC or partner download portal</p>
---	---

<pre>PS C:\users\athman.boukhaoua\Documents\Kanton-Thurgau> .\verify-image.ps1 -ReferenceISO "C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71796d33.iso" -ImageUSB d: Verifying integrity of the reference ISO file Mounting reference ISO file Mounted to drive F D:\System Volume Information\WPSettings.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> .\verify-image.ps1 -ReferenceISO "C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71796d33.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:\autounattend.xml ok by hash D:\bootmgr ok because original D:\bootmgr.efi ok because original D:\setup.exe ok because original</pre>	<p>Optionally, the parameter “-DisplayPositiveResults” can be used to show correctly checked files in green</p>																																																																																																																																							
<table border="1"> <thead> <tr> <th></th> <th>A</th> <th>B</th> <th>C</th> <th>D</th> <th>E</th> <th>F</th> <th>G</th> <th>H</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Info</td> <td>Reason</td> <td>Result</td> <td>FileName</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2</td> <td>3378723C</td> <td>original</td> <td>ok</td> <td>D:\autorun.inf</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>3</td> <td>E803F131</td> <td>hash</td> <td>ok</td> <td>D:\autounattend.xml</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>4</td> <td>4EEAC11B</td> <td>original</td> <td>ok</td> <td>D:\bootmgr</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>5</td> <td>96B7EE39</td> <td>original</td> <td>ok</td> <td>D:\bootmgr.efi</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>6</td> <td>30043368</td> <td>original</td> <td>ok</td> <td>D:\setup.exe</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>7</td> <td>A6FB0A49</td> <td>hash</td> <td>failed</td> <td>D:\System Volume Information\WPSettings.dat</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>8</td> <td>16327144</td> <td>original</td> <td>ok</td> <td>D:\boot\bcd</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>9</td> <td>CD2C00CE</td> <td>original</td> <td>ok</td> <td>D:\boot\boot.sdi</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>10</td> <td>2F9C2428</td> <td>original</td> <td>ok</td> <td>D:\boot\bootfix.bin</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>11</td> <td>55A47316</td> <td>original</td> <td>ok</td> <td>D:\boot\bootsect.exe</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>12</td> <td>F425E135</td> <td>original</td> <td>ok</td> <td>D:\boot\etfsboot.com</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>13</td> <td>BF8A9CC6</td> <td>original</td> <td>ok</td> <td>D:\boot\memtest.exe</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>14</td> <td>C89CDA7E</td> <td>original</td> <td>ok</td> <td>D:\boot\de-de\bootsect.exe.mui</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		A	B	C	D	E	F	G	H	1	Info	Reason	Result	FileName					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					<p>The script will output a detailed report in the “Documents” directory that shows check results for all files</p>
	A	B	C	D	E	F	G	H																																																																																																																																
1	Info	Reason	Result	FileName																																																																																																																																				
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

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 a 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/>