

Evoting – Basic installation and hardening

Version 1.10

Date 2025-09-12

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)

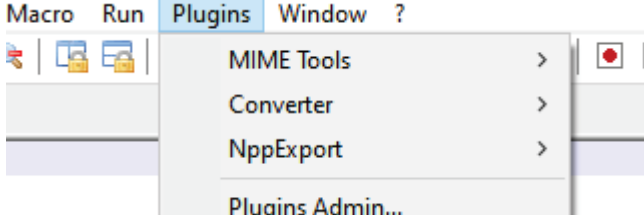
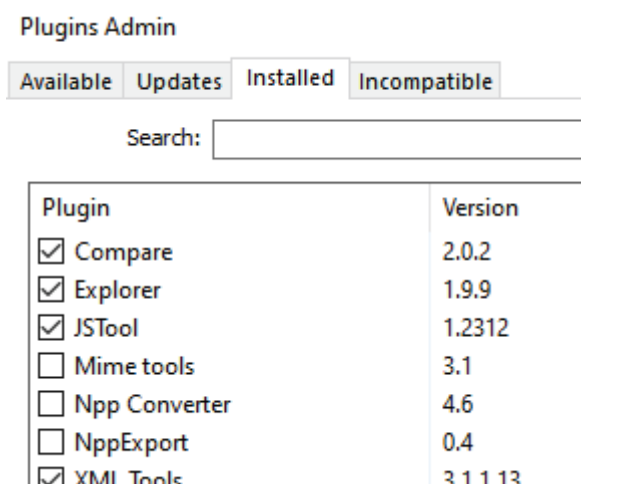
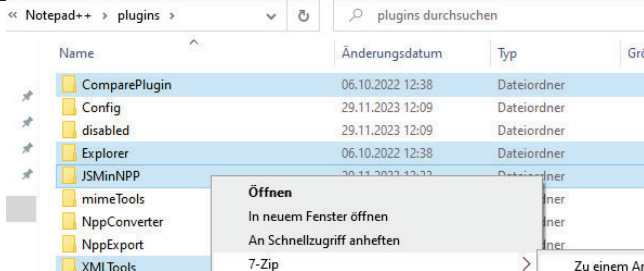
Edge

	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

 The screenshot shows the 'Plugins' menu in Notepad++. The menu items are: MIME Tools, Converter, NppExport, and Plugins Admin... The 'Plugins Admin...' option is highlighted.	On a test computer, install Notepad++ and start Plugins Admin																
 The screenshot shows the 'Plugins Admin' window. The 'Installed' tab is selected. A search bar is at the top. Below it is a table of installed plugins: <table border="1"> <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	Install «Compare», «Explorer», «XML Tools» and «JSTool»
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																
 The screenshot shows the 'plugins' folder in Notepad++. The folder contains several subfolders: ComparePlugin, Config, disabled, Explorer, JSMinNPP, mimeTools, NppConverter, NppExport, and XMLTools. A context menu is open over the 'XMLTools' folder, showing options: Öffnen, In neuem Fenster öffnen, An Schnellzugriff anheften, 7-Zip, and Zu einem Archiv hinzufügen...	Then package the four plugins as a self-extracting 7z archive																

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 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>

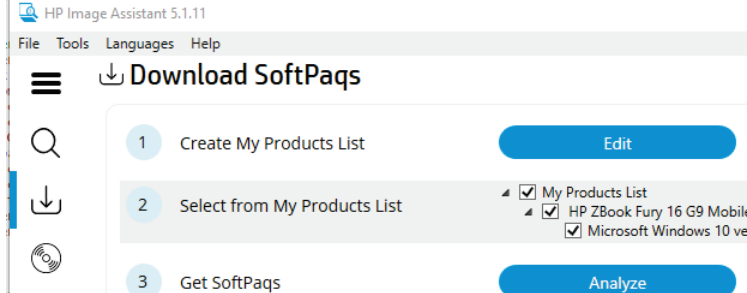
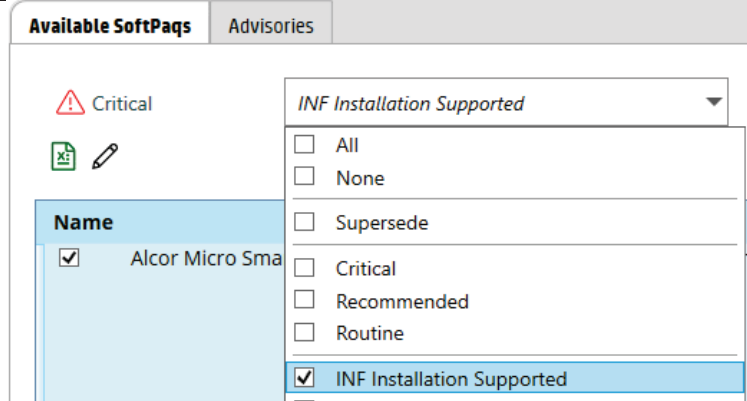
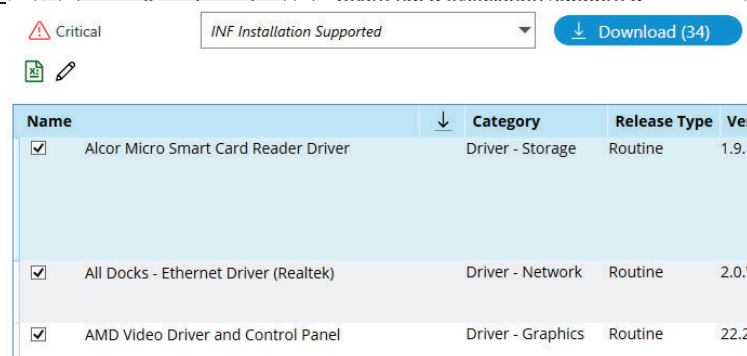
Drivers

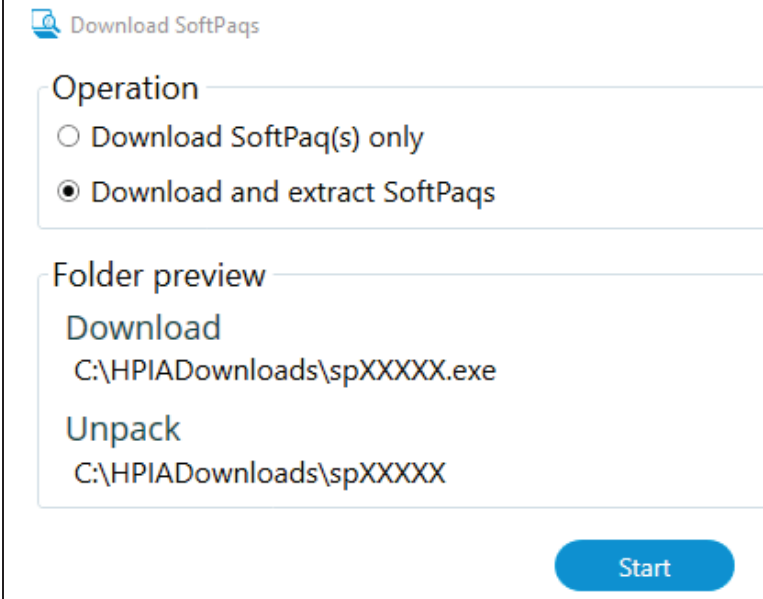
Supported models

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

	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
	Check "Inf Install supported" to filter for only drivers (not application or BIOS)
	Then click "Download"



Download SoftPaqs

Operation

☐ Download SoftPaq(s) only

☒ Download and extract SoftPaqs

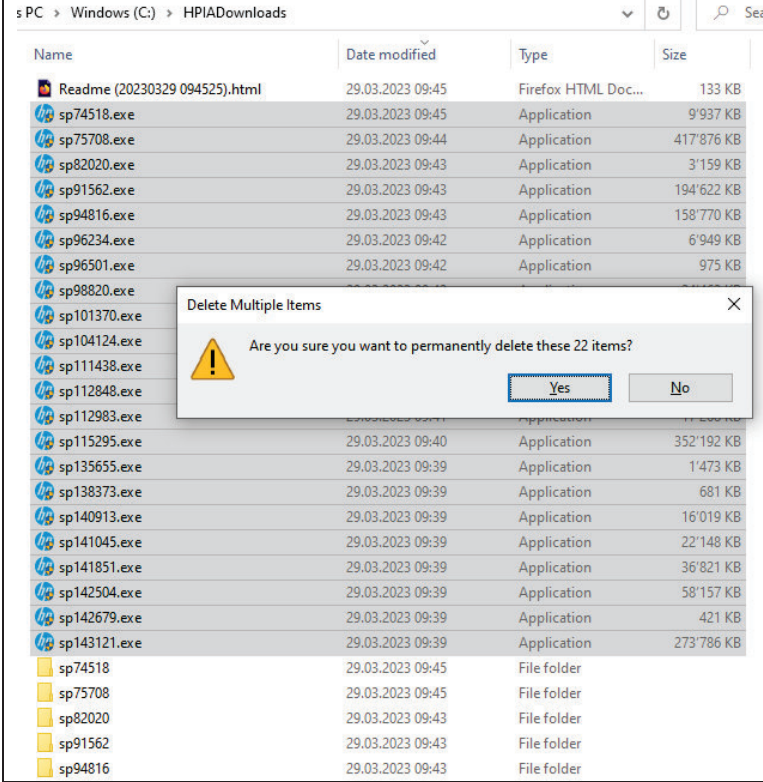
Folder preview

Download
C:\HPIADownloads\spXXXXX.exe

Unpack
C:\HPIADownloads\spXXXXX

Start

Choose "Download and Extract"



s PC > Windows (C:) > HPIADownloads

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	29.03.2023 09:42	Application	1'159 KB
sp101370.exe	29.03.2023 09:42	Application	1'159 KB
sp104124.exe	29.03.2023 09:40	Application	352'192 KB
sp111438.exe	29.03.2023 09:39	Application	1'473 KB
sp112848.exe	29.03.2023 09:39	Application	681 KB
sp112983.exe	29.03.2023 09:39	Application	16'019 KB
sp115295.exe	29.03.2023 09:39	Application	22'148 KB
sp135655.exe	29.03.2023 09:39	Application	36'821 KB
sp138373.exe	29.03.2023 09:39	Application	58'157 KB
sp140913.exe	29.03.2023 09:39	Application	421 KB
sp141045.exe	29.03.2023 09:39	Application	273'786 KB
sp141851.exe	29.03.2023 09:39	Application	
sp142504.exe	29.03.2023 09:39	Application	
sp142679.exe	29.03.2023 09:39	Application	
sp143121.exe	29.03.2023 09:39	Application	
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	

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

Lenovo

ThinkVantage Update Retriever

Hilfe

Zusammenfassung herunterladen

Neue Aktualisierungen abrufen

Repository verwalten

Treiberpakete verwalten

In Update Retriever, chose “Manage driver packages”

1 2 3

You can create a collection of hardware device drivers to be used in your operating system deployment activities. During this process, the selected current SCCM, MDT, or used as the source for a standard package.

Specify the folder where the driver pack contents will be stored.

Folder:

Specify the model to find drivers for and then click Next.

Brand: Series: Model: Operating System:

☒ Select All

	Title	File Name	Size	Version
☒	NVIDIA Video Features Driver 11 (Version 21H2 or later) 10 (Version 21H2 or later)	nzada08w.exe	920.67 MB	32.0.15.7240
☒	Intel Graphics Driver 11 (Version 21H2 or later)	nzadr14w.exe	599.42 MB	32.0.101.6733
☒	Integrated Camera Driver 11 (Version 21H2 or later) 10 (Version 21H2 or later)	nz2cd03w_nox13g4.exe	173.37 MB	5.0.18.261/ 10.0.22000.20364/ 10.13.22621.33
☒	Intel Management Engine Software 11 (Version 21H2 or later) 10 (Version 21H2 or later)	nzara04w.exe	66.35 MB	2505.7.2.0
☒	Quectel EM05-G Wireless WAN Driver 11 (Version 21H2 or later) 10 (Version 20H2 or later)	nzaws06w.exe	53.19 MB	1.0.0.36
☒	Quectel EM05-CN Wireless WAN Driver package 11 (Version 21H2 or later) 10 (Version 21H1 or later)	nzawr07w.exe	52.08 MB	1.0.0.18
☒	Fibocom L860-GL-16 Wireless WAN Driver 10 (Version 20H2 or later)	nzawj05w.exe	35.99 MB	3.8.00.3044
☒	Lenovo View Driver 11 (Version 22H2 or later) 10 (Version 21H2 or later)	n3xld12w.exe	25.23 MB	3.1.32.1
☒	Intel Dynamic Tuning Technology Driver 11 (Version 21H2 or later)	nzahd03w.exe	17.89 MB	9.0.11404.51148 /1.0.11404.41023 /2.1.10300.31
☒	Intel(R) Connectivity Performance Suite Driver	icps_4.1024.1009.5.exe	17.32 MB	4.1024.1009.5
☒	Intel AX211 WLAN Driver 11 (Version 21H2 or later)	nzawl07w.exe	13.18 MB	23.130.1.1

☒ Connecting to update repository
☒ Downloading updates (13 of 26)

Downloading: Goodix Fingerprint Reader Driver 11 (21H2 or later) 10 (Version 21H2 or later)

Overall progress: 46%

ThinkVantage Update Retriever has finished downloading the selected drivers for the system you specified.

26 drivers were downloaded successfully.

Contents located here:

<C:\LenovoDriverPacks\ThinkPad T14 Gen 4 Type 21HD 21HE win10>

Enter a path, and select a computer model and operating system

Press “Next”

In the list of drivers, use “Select all”

Check for duplicate drivers here, sometimes multiple copies of a graphics driver make the package needlessly large

Press “Next, then Finish”

Wait for the downloads to finish

Then you can open the result directory

To see the downloaded drivers

This PC > Windows (C:) > LenovoDriverPacks > ThinkPad T14 Gen 4 Type 21HD 21HE win10 >

Name	Date modified	Type	Size
Bluetooth	26.06.2025 15:47	File folder	
Camera	26.06.2025 15:47	File folder	
Card_Reader	26.06.2025 15:47	File folder	
Chipset	26.06.2025 15:47	File folder	
Display	26.06.2025 15:53	File folder	
Ethernet	26.06.2025 15:47	File folder	
Input	26.06.2025 15:47	File folder	
Security	26.06.2025 15:47	File folder	
Unknown	26.06.2025 15:47	File folder	
USB	26.06.2025 15:47	File folder	
Wireless	26.06.2025 15:48	File folder	
DownloadDrivers.csv	26.06.2025 15:55	CSV File	6 KB

Driver package adjustments

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

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

HP 850 G5:

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

HP ZBook Fury 16 G9:

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

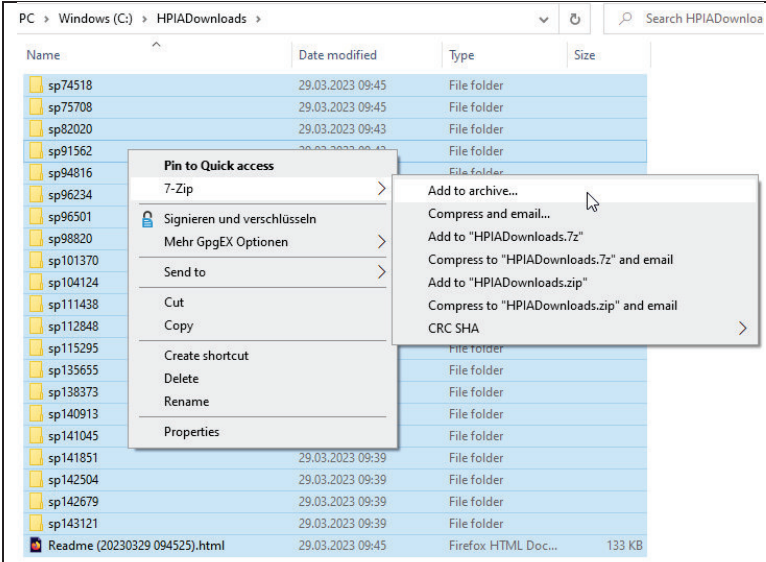
HP ZBook Fury 16 G10:

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

HP ZBook Fury 16 G11:

- Delete the driver for “HP Mobile Broadband” (currently SP160331)

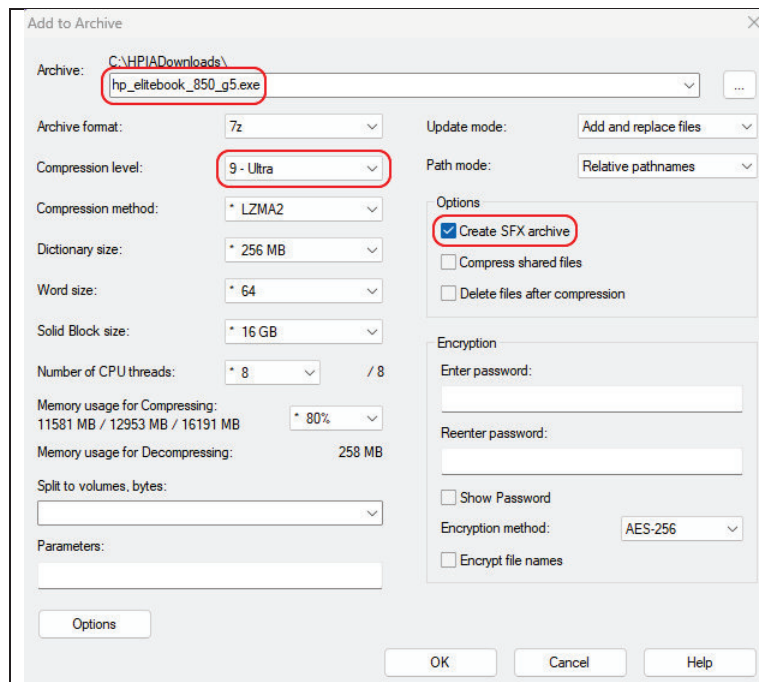
Create the package



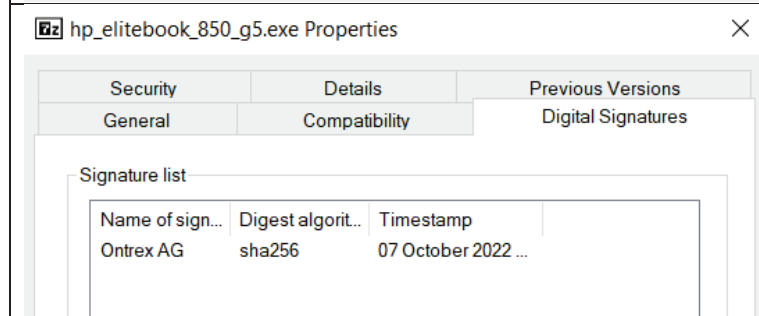
PC > Windows (C:) > HPIADownloads >

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

Add the extracted folders to a 7zip archive



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



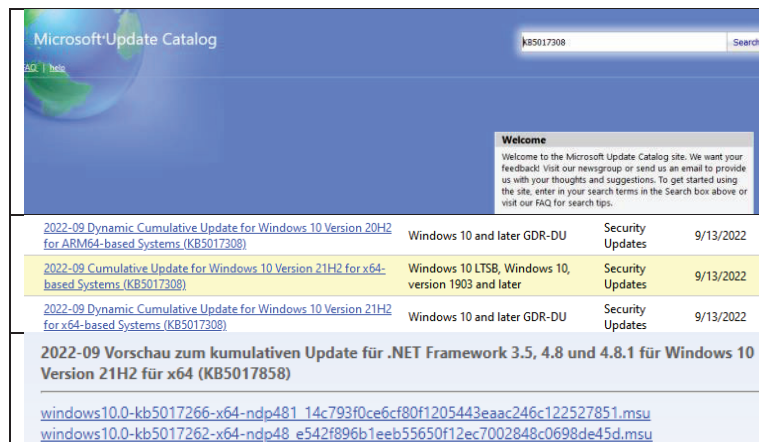
Sign the finished archive (with timestamp)

Updates

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

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

Windows



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

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

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

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

.NET Desktop Runtime 8.0.13

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

OS	Installers	Binaries
Windows	x64 x86 Arm64 winget instructions	

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

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

Microsoft Defender

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

BIOS

2 Select from My Products List My Products List ☒ HP ZBook Fury 16 G10 Mobile Workstation PC ☒ Microsoft Windows 10 version 21H2 (64-bit) ☒ HP ZBook Fury 16 G9 Mobile Workstation PC ☒ Microsoft Windows 10 version 21H2 (64-bit) ☒ HP EliteBook 850 G5 Notebook PC ☒ Microsoft Windows 10 version 21H2 (64-bit)	For HP, select all models, then press Analyze										
3 Get SoftPaqs Analyze											
bios	Filter for the word "bios"										
Critical Select Components to Download/Apply Download (3) <table border="1"> <thead> <tr> <th>Name</th><th>Category</th></tr> </thead> <tbody> <tr> <td>☒ HP BIOS and System Firmware (U96)</td><td>BIOS - System Firm</td></tr> <tr> <td>☒ HP BIOS and System Firmware (V96)</td><td>BIOS - System Firm</td></tr> <tr> <td>☐ HP BIOS Config Utility (BCU)</td><td>Software - System</td></tr> <tr> <td>☒ HP Firmware Pack (Q78)</td><td>BIOS</td></tr> </tbody> </table>	Name	Category	☒ HP BIOS and System Firmware (U96)	BIOS - System Firm	☒ HP BIOS and System Firmware (V96)	BIOS - System Firm	☐ HP BIOS Config Utility (BCU)	Software - System	☒ HP Firmware Pack (Q78)	BIOS	Then check all the BIOS updates and click "Download"
Name	Category										
☒ HP BIOS and System Firmware (U96)	BIOS - System Firm										
☒ HP BIOS and System Firmware (V96)	BIOS - System Firm										
☐ HP BIOS Config Utility (BCU)	Software - System										
☒ HP Firmware Pack (Q78)	BIOS										

er PC > Windows (C:) > temp2 > GPOs			Extract the baseline zip file	
Name	Änderungsdatum	Typ		
{4B6589C2-0290-4764-8058-9825B56B4169}	04.10.2022 09:04	Dateiordner		
{7AD4F62E-9296-4FEA-9765-C4E3EEAAEC1}	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		
{C94113FA-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		
<pre>PS C:\temp2\GPOs> lgp /parse /m ".\{23DEF82E-039F-40D5-BBCC-35444958D065}\DomainSysvol\GPO\Machine\registry.pol" /q > ie_computer.txt PS C:\temp2\GPOs> lgp /parse /m ".\{4B6589C2-0290-4764-8058-9825B56B4169}\DomainSysvol\GPO\User\registry.pol" /q > user.txt PS C:\temp2\GPOs> lgp /parse /m ".\{7AD4F62E-9296-4FEA-9765-C4E3EEAAEC1}\DomainSysvol\GPO\Machine\registry.pol" /q > d redentialguard.txt PS C:\temp2\GPOs> lgp /parse /m ".\{B669E0C6-C1E3-4582-B797-FE384B21CD01}\DomainSysvol\GPO\Machine\registry.pol" /q > d efender.txt PS C:\temp2\GPOs> lgp /parse /m ".\{B697C660-A87B-4AF1-B37D-9440912605E7}\DomainSysvol\GPO\Machine\registry.pol" /q > b itlocker.txt PS C:\temp2\GPOs> lgp /parse /m ".\{C94113FA-C027-4F5F-8210-85F4AC2C6082}\DomainSysvol\GPO\User\registry.pol" /q > ie_u ser.txt PS C:\temp2\GPOs> lgp /parse /m ".\{DD304A7D-15A7-42B7-AB52-2338F4ECE2C7}\DomainSysvol\GPO\Machine\registry.pol" /q > c</pre>			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.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer", "NoAddPrinter", 1
56 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\Lanman Print Services\Servers", "AddPrinter", "Start", 4
57 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\Lanman Print Services\Servers", "SecurityLevel", 0
58 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer", "NoName", 1
59 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer", "NoPrintProduction", 1
60 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Firewall\PrivateProfile", "DenyAllExceptions", 1
61 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Firewall\PrivateProfile", "DenyAllInboundExceptions", 1
62 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Firewall\PrivateProfile", "DenyAllOutboundExceptions", 1
63 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Firewall\PublicProfile", "DenyAllExceptions", 1
64 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Firewall\PublicProfile", "DenyAllInboundExceptions", 1
65 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Firewall\PublicProfile", "DenyAllOutboundExceptions", 1
66 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{4D96E23A-4786-41CD-A009-6076F21928EA}\DomainProfiles", "NoDomainProfiles", 1
67 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections", "NoShowShareAndAccess", 0
68 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{4D96E23A-4786-41CD-A009-6076F21928EA}\TCPParameters", "NoShowShareAndAccess", 0
69 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Policies\System", "NoConnectDefault", 0
70 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Policies\System", "NoConnectDefault", 0
71 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Policies\System", "EnableLUA", 1
72 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "ConsentPromptBehaviorAdmin", 2)
73
74 log " Disable Torado"
75 netsh interface torado set state disabled
76 log " Result: %$EXITCODE%"
77
78 log " Disable Guest user"
79 net user /add /y /no
80 log " Result: %$EXITCODE%"
81
82 log " Changing Audit Policy"
83 auditpol /set /subcategory "Authentifizierungsrichtlinienänderung" /success:enable /failure:disable
84 auditpol /set /subcategory "Autorisierungsrichtlinienänderung" /success:enable /failure:disable
85 auditpol /set /subcategory "Richtlinienänderungen überachen" /success:enable /failure:disable
86
87 log " Block POP"
88 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\FirewallRules", "Custom-Block-POPp", "v2, 30 acti
89 [Microsoft.Windows2_Registry]::Set-Value "HKY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Firewall\FirewallRules", "Custom-Block-POPp", "v2, 30 acti

```

CIS Benchmark

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

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

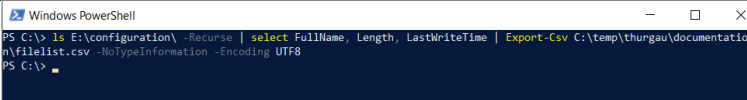
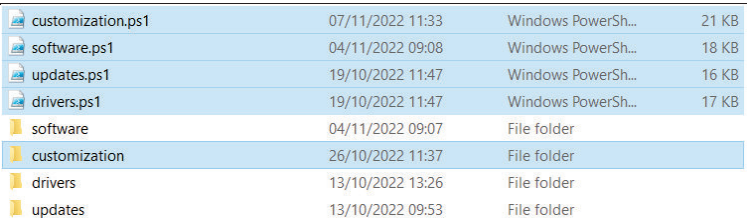
Adjustments for Windows 11 pilot

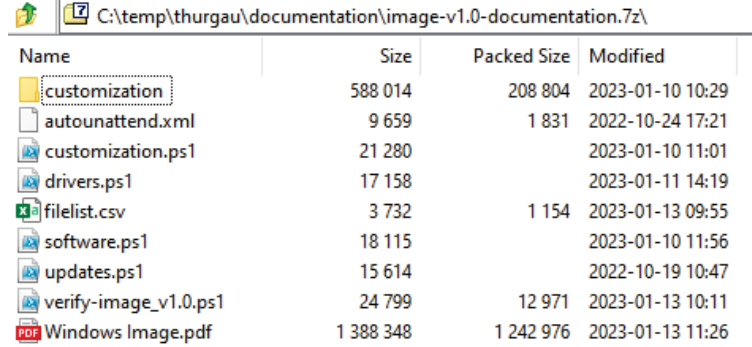
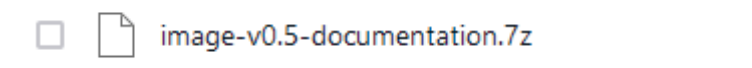
As preparation for a change to a Windows 11 LTSC based image, we are currently running a pilot version of the E-Voting image based on this OS. This image has the following changes compared to the productive Windows 10 one:

- 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.

				Export a list of all the customized files to a CSV file using the command:
				<pre>ls E:\configuration\ -Recurse select FullName, Length, LastWriteTime Export-Csv C:\data\thurgau\documentation\ filelist.csv - NoTypeInformation -Encoding UTF8</pre>
				Archive the four PowerShell files and the entire "customization" directory into a 7z file...

 File Explorer window showing the contents of 'C:\temp\thurgau\documentation\image-v1.0-documentation.7z\'. The table below lists the files and folders: <table><tr><th>Name</th><th>Size</th><th>Packed Size</th><th>Modified</th></tr><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></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	...and add: • 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.

enprojekte (P:) > Kanton Thurgau Staatskanzlei > Projekte > E-Voting > image_v1.4 >

Name	Date modified	Type	Size
 biosupdates	28.03.2024 15:12	File folder	
 customization	28.03.2024 15:13	File folder	
 software	28.03.2024 15:15	File folder	
 image-v1.4-documentation.7z	28.03.2024 15:07	7z Archive	1'412 KB

Create a subdirectory for the current image version, and copy the documentation 7z, as well as the directories: *customization*, *software* and *biosupdates*

Create the bootable ISO

The screenshot shows the AnyBurn application window. At the top, there's a menu bar with 'Options' and 'Help'. Below it, a section titled 'Please select a task:' contains several buttons. The button 'Edit image file' at the bottom right is highlighted with a blue border. Other buttons include 'Burn image file to disc', 'Burn or append files/folders to disc', 'Burn Audio CD from mp3/m4a/flac/ape/wav...', 'Erase rewritable disc', 'Copy disc to image file', 'Copy disc to another disc', 'Rip Audio CD to mp3/flac/ape/wav...', and 'Browse / Extract image file'.

Start Anyburn, then choose "Edit Image"

The screenshot shows the 'Edit image file' dialog box. It has a menu bar with 'Options' and 'Help'. The main area is titled 'Select an image file:' and contains a text input field with the path 'C:\temp\thurgau\de-de_windows_10_enterprise_lts_2021_x64_dvd_71796d33.iso'.

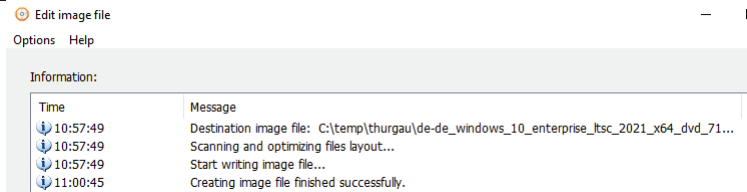
Open a bootable ISO file

The screenshot shows the 'Edit image file' dialog box. It has a menu bar with 'Options' and 'Help'. The main area is titled 'Select image file:' and contains a text input field with the path 'C:\temp\thurgau\de-de_windows_10_enterprise_lts_2021_x64_dvd_71796d33.a.iso'. Below the text field, there's a dropdown menu for 'Select image file type:' which is currently set to 'Standard ISO Images (.ISO)'. To the left of the text field, there's a file explorer view showing the contents of the ISO file, including folders like 'boot', 'configuration', 'efi', 'sources', 'support' and files like 'autorun.inf', 'autounattend.xml', 'bootmgr', 'bootmgr.efi', and 'setup.exe'.

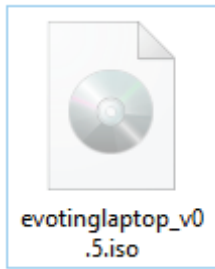
Add the "autounattend.xml" and the "configuration" directory

The screenshot shows the 'Edit image file' dialog box. It has a menu bar with 'Options' and 'Help'. The main area is titled 'Destination image file:' and contains a text input field with the path 'C:\temp\thurgau\de-de_windows_10_enterprise_lts_2021_x64_dvd_71796d33.a.iso'. Below the text field, there's a dropdown menu for 'Select image file type:' which is currently set to 'Standard ISO Images (.ISO)'.

Save under a different name

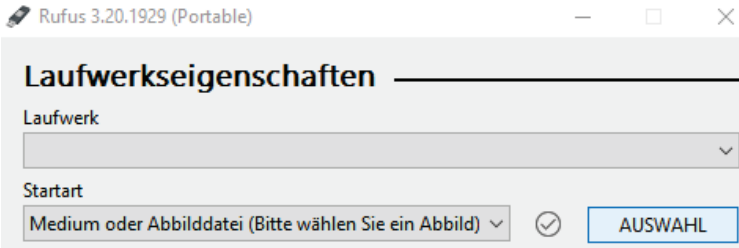
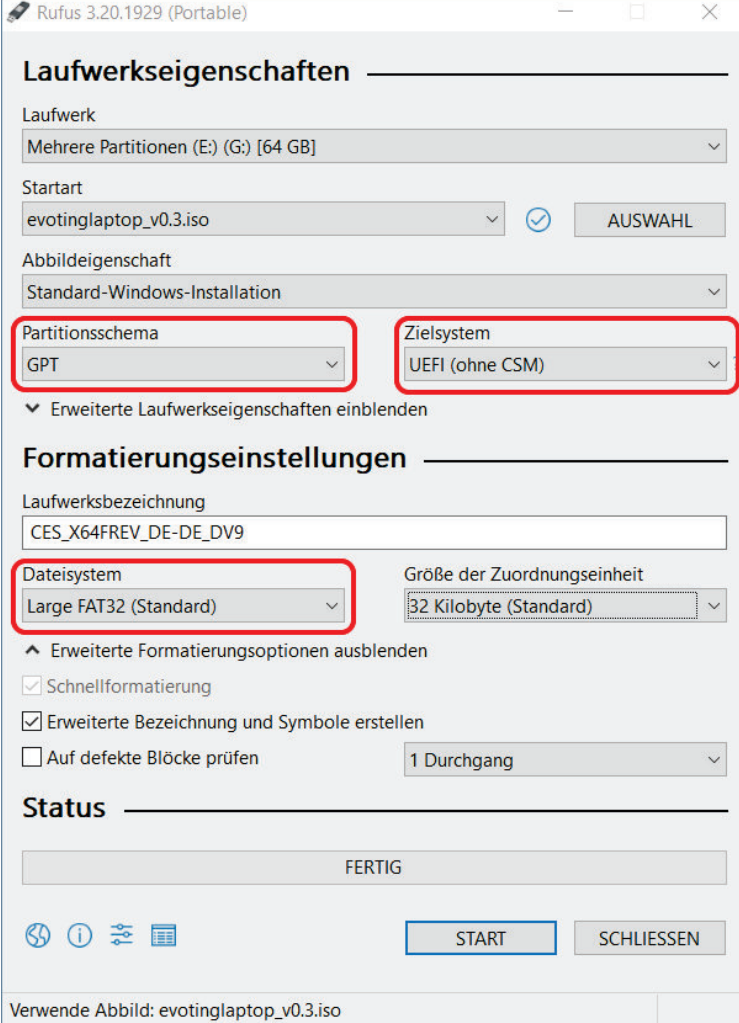
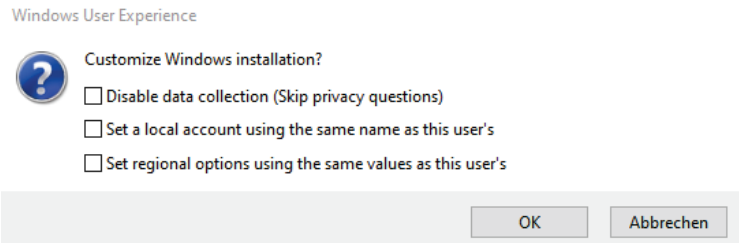
	Wait until it's finished
---	---------------------------------

Upload the image

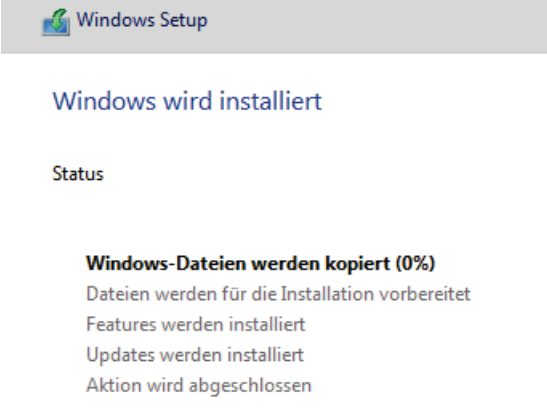
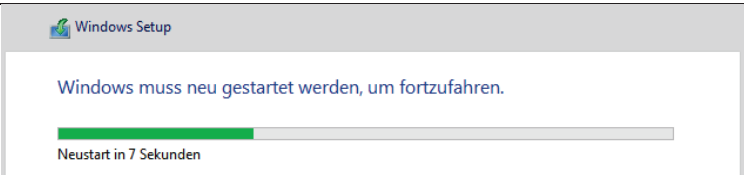
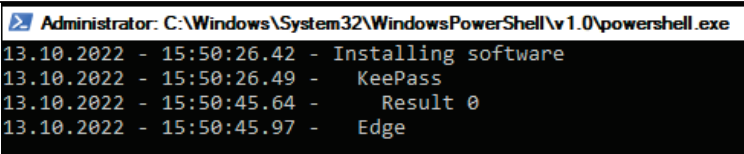
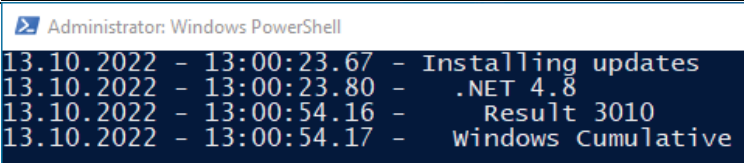
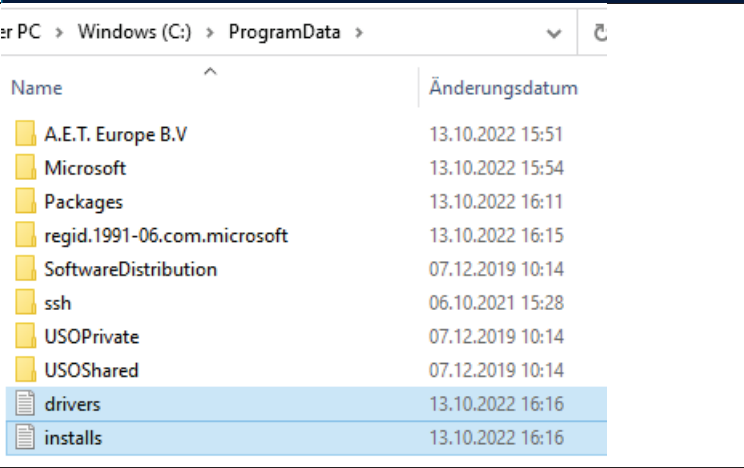
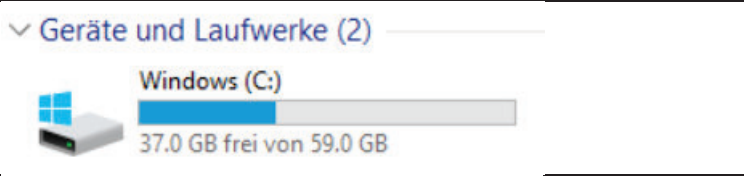
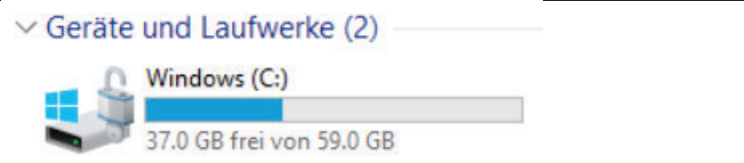
	Rename the resulting image to evotinglaptop_vx.y.iso
All Files > Kiteworks > Kanton Thurgau ☐ Name ^ ☐  Upload ☐  evotinglaptop_v0.5.iso	And upload it to the Kiteworks share https://kiteworks.ontrex.ch/#/folder/8666a49b-a3d7-4831-9d02-45666f755d19

User Guide

Extract the ISO to a USB Stick

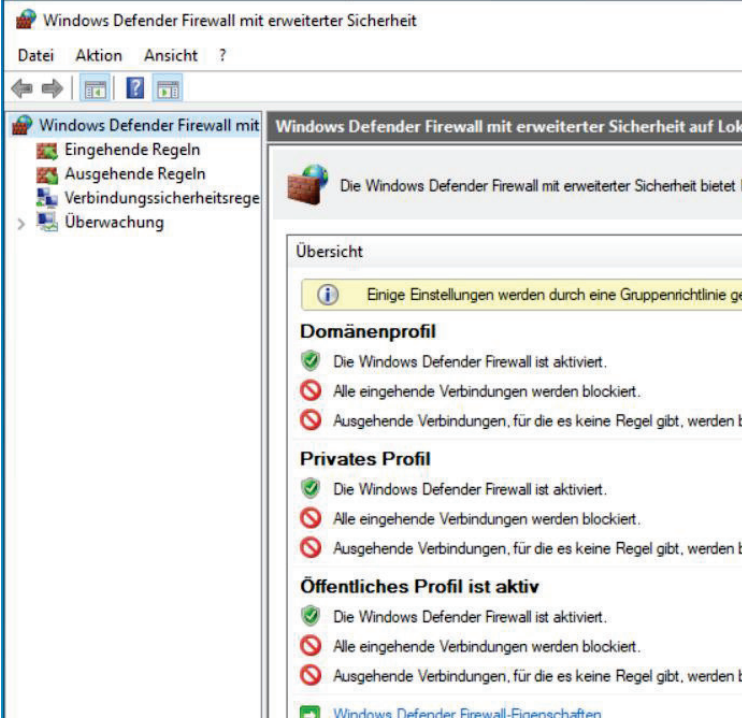
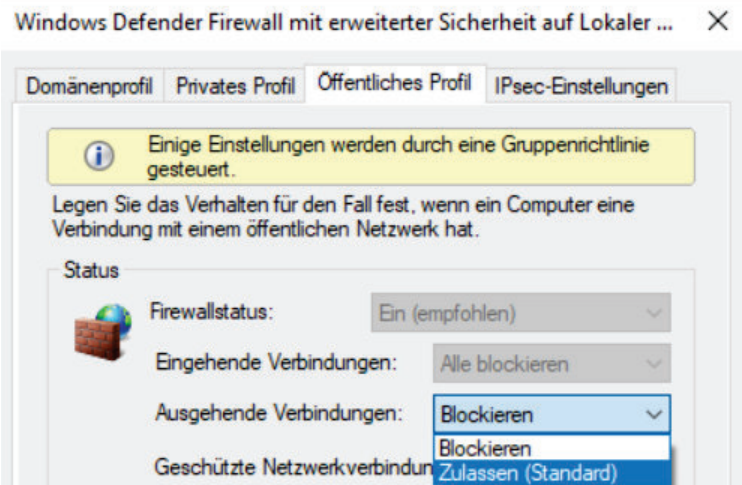
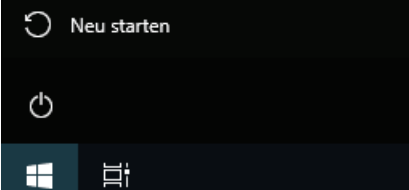
	Start Rufus and select the ISO file
	Use GPT, UEFI (without CSM) and Large FAT32 as options Do not modify the drive name, it has to stay on the default value
	Do not let Rufus do any adjustments to the Windows installation

Apply the image to a computer

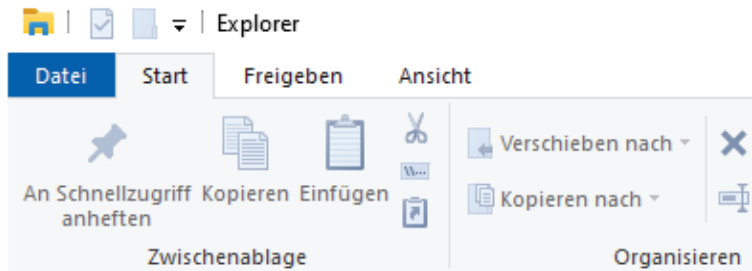
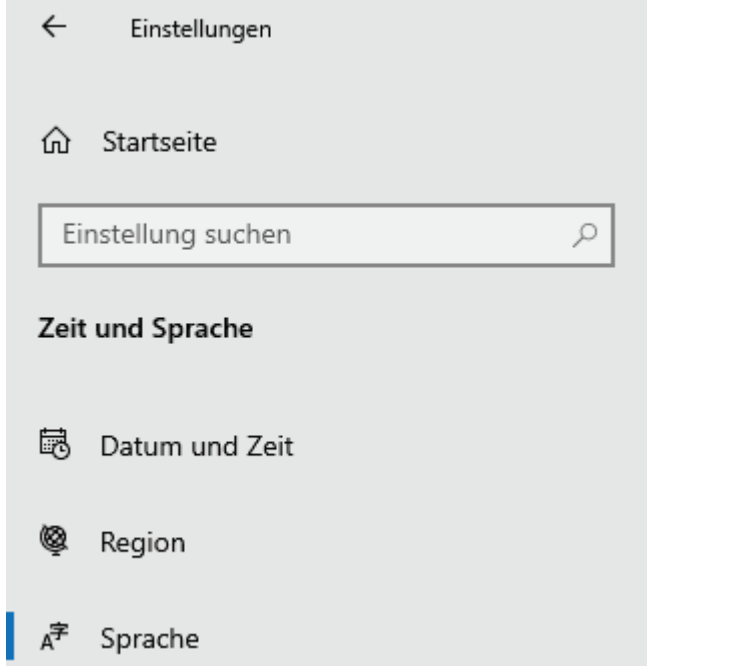
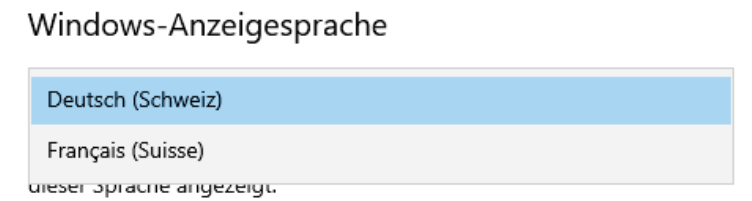
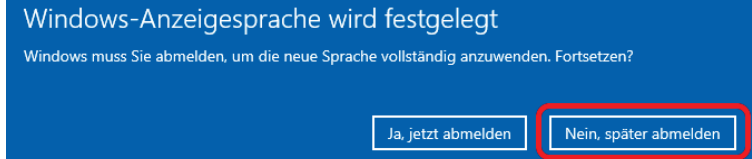
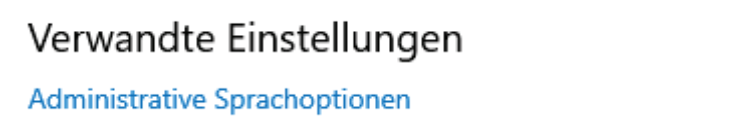
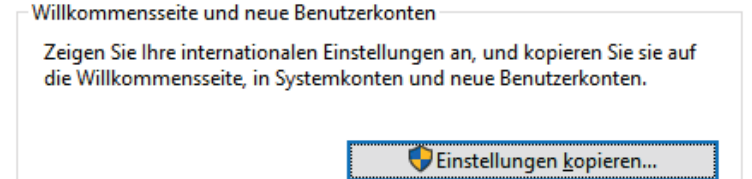
	Boot the laptop from the USB stick by pressing either F9 for HP, F12 for Lenovo, or Esc for Panasonic early in the boot process. The Windows Setup will then automatically start
	After a while it'll reboot...
	...and continue by installing drivers, applications etc
	When the computer is installing updates,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

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.

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

Change language

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

Aktuelle Einstellungen für folgende Konten kopieren: ☒ Willkommenseite und Systemkonten ☒ Neue Benutzerkonten OK Abbrechen	Set the checkboxes on the login page and the new user accounts, then press OK
Anzeigesprache ändern Die Systemanzeigesprache wurde geändert. Sie müssen Windows neu starten, damit die Änderungen wirksam werden. Speichern Sie Ihre Arbeit und schließen Sie alle geöffneten Programme vor dem Neustart. Jetzt neu starten Abbrechen	Confirm the restart
Explorateur de fichiers Fichier Accueil Partage Affichage Épingler à Accès rapide Copier Coller Déplacer vers Copier vers Suivre le lien Presse-papiers Organiser	After that, Windows is in French

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.

PC > Downloads > ISO Search ISO <table><thead><tr><th>Name</th><th>Date modified</th><th>Type</th><th>Size</th></tr></thead><tbody><tr><td> de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71796d33.iso</td><td>16.11.2021 20:25</td><td>Disc Image File</td><td>4'832'998 KB</td></tr><tr><td> SW_DVD9_WIN_ENT_LTSC_2021_64BIT_German_MLF_X22-84426.ISO</td><td>16.11.2021 20:25</td><td>Disc Image File</td><td>4'832'998 KB</td></tr></tbody></table>	Name	Date modified	Type	Size	 de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71796d33.iso	16.11.2021 20:25	Disc Image File	4'832'998 KB	 SW_DVD9_WIN_ENT_LTSC_2021_64BIT_German_MLF_X22-84426.ISO	16.11.2021 20:25	Disc Image File	4'832'998 KB	Download the German Windows LTSC 2021 ISO from an official Microsoft source, like the VLSC, the partner download portal or Visual Studio Downloads.
Name	Date modified	Type	Size										
 de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71796d33.iso	16.11.2021 20:25	Disc Image File	4'832'998 KB										
 SW_DVD9_WIN_ENT_LTSC_2021_64BIT_German_MLF_X22-84426.ISO	16.11.2021 20:25	Disc Image File	4'832'998 KB										
<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\WPS\Settings.dat not ok Results of the scan have been written to: C:\Users\athman.boukhaoua\Documents\evoting_imagecheck.csv</pre>	Run the script with the parameter -ReferenceISO pointing to the above ISO file, and -ImageUSB set to the USB drive that should be checked												
<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:\bootup.exe ok because original</pre>	Optionally, the parameter “-DisplayPositiveResults” can be used to show correctly checked files in green												

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

Version History

v0.1

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

v0.2

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

v0.3

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

v0.4

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

v0.5

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

v1.0

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

v1.1

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

v1.1.1

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

v1.2

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

v1.3

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

v1.3.1

- Added support for laptop model HP ZBook Fury 16 G10

v1.4

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

v1.5

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

v1.6

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

v1.7

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

v1.8

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

v1.9

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

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

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

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/>