Evoting – Basic installation and hardening

Version   1.5   Date   2024-06-27

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
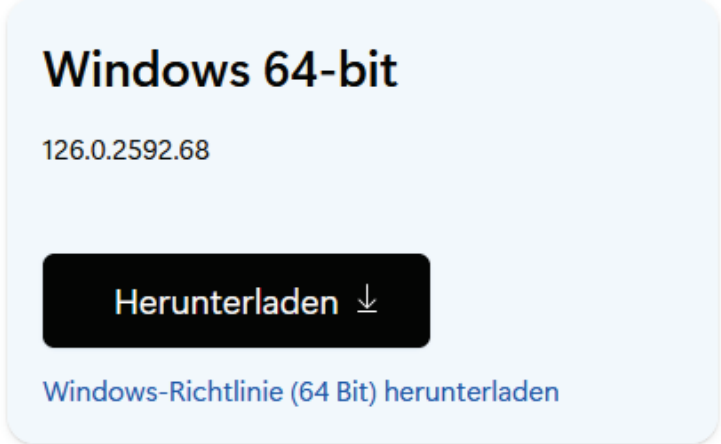
KeePass

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

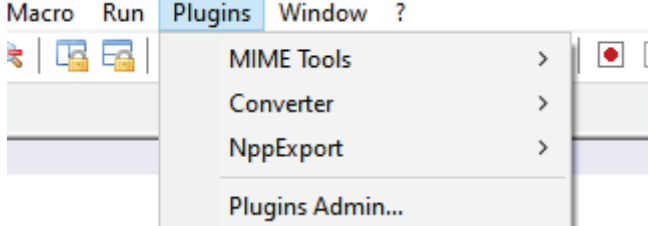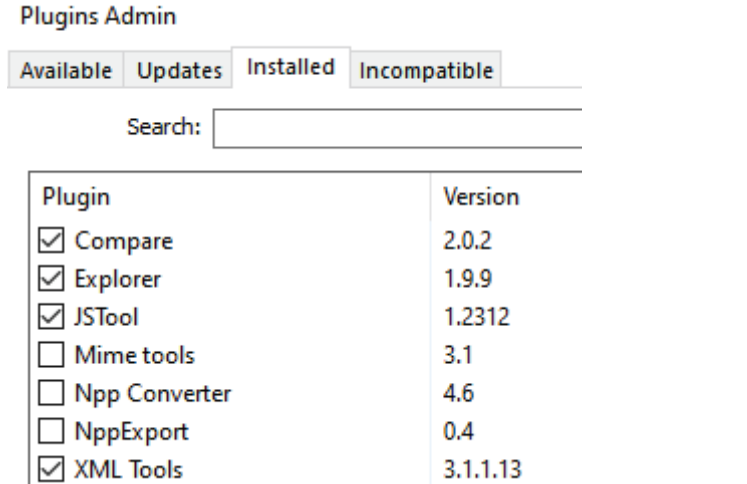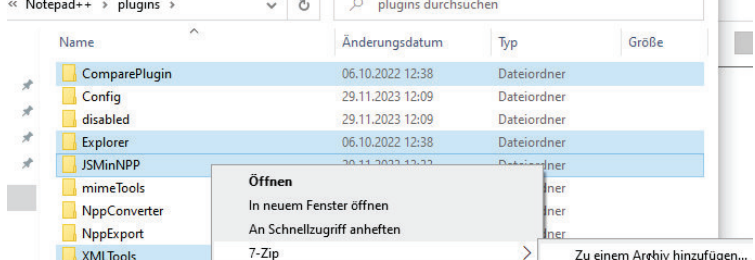|	
Windows 64-bit 126.0.2592.68 **Herunterladen ↓** Windows-Richtlinie (64 Bit) herunterladen	https://www.microsoft.com/de-de/edge/business/download Download 64-bit package

Notepad++

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

Notepad++ Plugins

	On a test computer, install Notepad++ and start Plugins Admin
	Install «Compare», «Explorer», «XML Tools» and «JSTool»
	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 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

TotalCommander

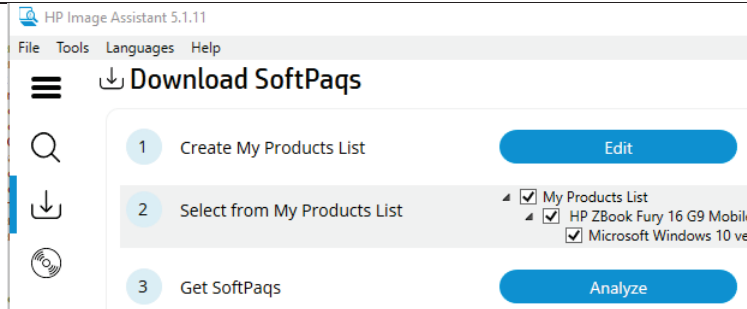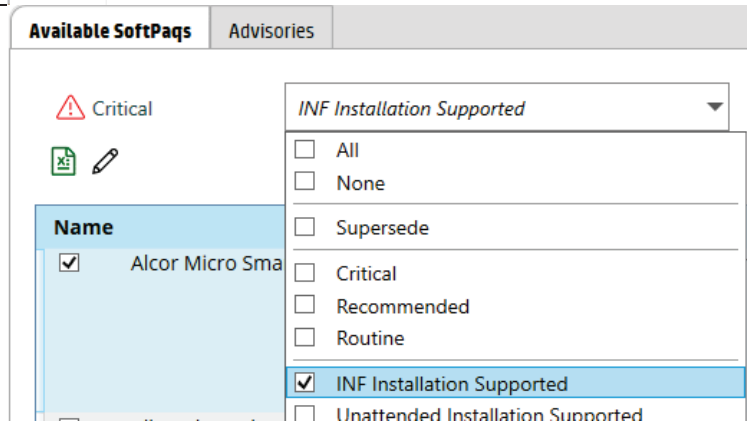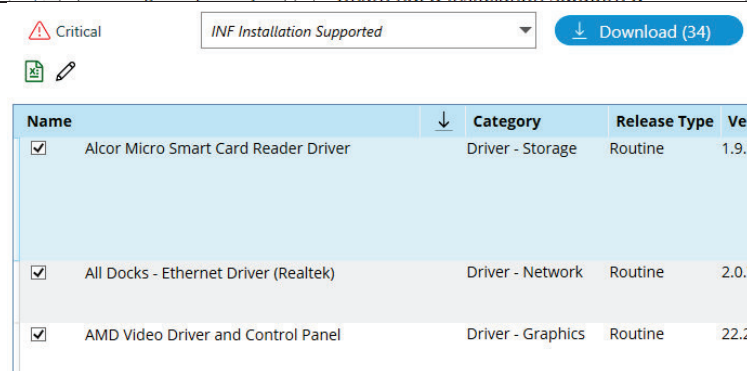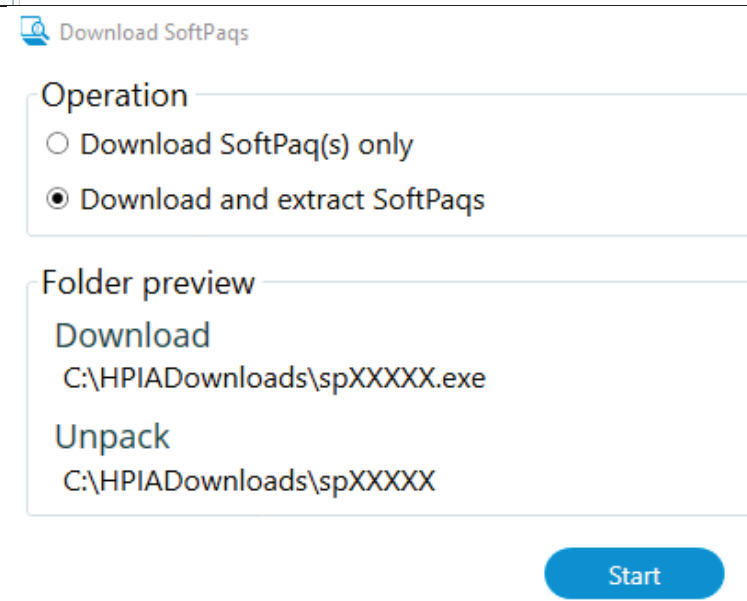Download 64-Bit Installer from https://www.ghisler.com/download.htm

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

HP

HP Image Assistant 5.1.11 File Tools Languages Help ☰ ⬇ Download SoftPaqs Q ⬇ ◎ ① Create My Products List — [Edit] ② Select from My Products List — ☑ My Products List / ☑ HP ZBook Fury 16 G9 Mobile / ☑ Microsoft Windows 10 ver ③ Get SoftPaqs — [Analyze]	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
Available SoftPaqs Advisories ⚠ Critical INF Installation Supported ▼ ☒ ✎ ☐ All ☐ None ☐ Supersede ☐ Critical ☐ Recommended ☐ Routine ☑ INF Installation Supported ☐ Unattended Installation Supported **Name** ☑ Alcor Micro Sma	Check "Inf Install supported" to filter for only drivers (not application or BIOS)
⚠ Critical INF Installation Supported ▼ [⬇ Download (34)] ☒ ✎ **Name** ↓ **Category** **Release Type** **Ver** ☑ Alcor Micro Smart Card Reader Driver — Driver - Storage — Routine — 1.9.1 ☑ All Docks - Ethernet Driver (Realtek) — Driver - Network — Routine — 2.0.V ☑ AMD Video Driver and Control Panel — Driver - Graphics — Routine — 22.2(	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"

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

Lenovo

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

Press "Continue", then "Yes"

Add the laptop model you want to get drivers for

Then select it and press "Next"

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

Select All — View que[r] Total selected: 42 updates, 2.21 GB *(driver list with checkboxes: Intel Dynamic Plat..., Integrated Camera..., Intel Bluetooth Dri..., NXP NFC Driver..., Fibocom L830-EB..., Synaptics UltraNav..., Intel Chipset Drive..., Intel PRO/1000 LA..., Realtek Media Car...)* Changes since last search: (+)Added (△)Changed (-)Removed Hide Option / This version / This version and all future versions	Select all drivers and press "Next"
Select All 20LC [ThinkPad P52s]-Windows 10 *(driver list: Alcor Smart Card Reader Driver, Fibocom L830-EB Wireless WAN Driver, Fibocom L850-GL Wireless WAN Driver, Generic DisplayLink Driver, Integrated Camera Driver, Intel 8265 Wireless LAN Driver, Intel Bluetooth Driver, Intel Chipset Driver, Intel Dynamic Platform and Thermal Framework, Intel Gigabit Ethernet Driver, Intel Graphics Driver, Intel Management Engine Software, Intel PRO/1000 LAN Adapter Software, Intel Serial IO Driver)* 42 updates, 2.21 GB Back Finish	"Finish"
ThinkVantage Update Retriever has finished downloading new updates Current Results (Click link to view details): 42 updates downloaded successfully.	Wait for the downloads to finish
PC > Windows (C:) > temp > retriever > n1fupa0w Name — Date modified — Type — Size n1fupa0w — 3/29/2023 10:07 AM — Application — 4,326 KB n1fupa0w — 3/29/2023 10:07 AM — Text Document — 44 KB n1fupa0w_2_ — 3/29/2023 10:05 AM — XML Document — 11 KB	This will create a lot of directories with drivers inside executable archives
(Administrator: Windows PowerShell window)	Use the following command in a window with admin rights to extract the packages: `ls C:\temp\retriever*.exe -Recurse	% { $_.BaseName; & $_ /VERYSILENT "/DIR=c:\temp\retriever2\$($_.BaseName)" /extract=yes	Out-Null }`

This extracts the archive to usable file collections

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 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 SP152918)
- Delete the driver for "Realtek HD Audio" (currently SP153035)
- 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 SP153022)
- Delete the driver for "Intel XMM LTE" (currently SP152359)

Create the package

Add the extracted folders to a 7zip archive
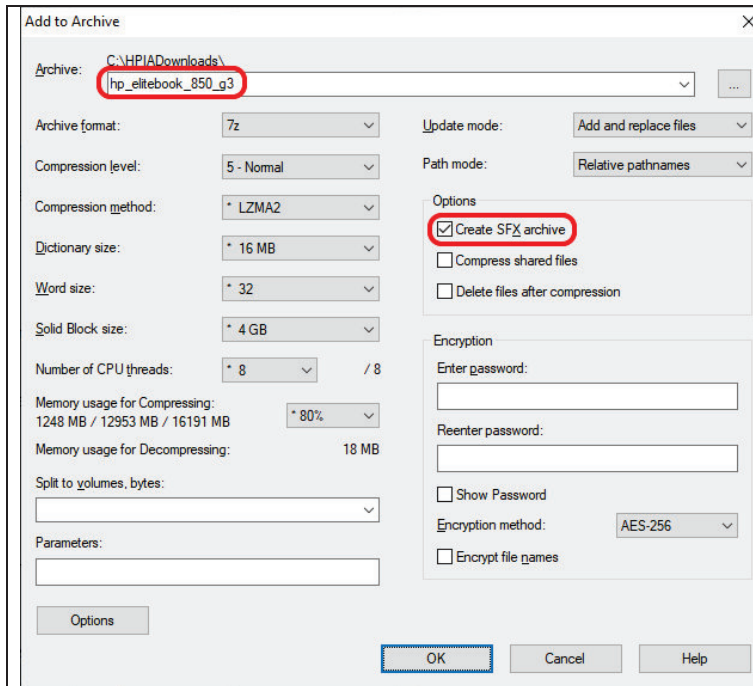
As self-extracting archive with the name of the laptop model
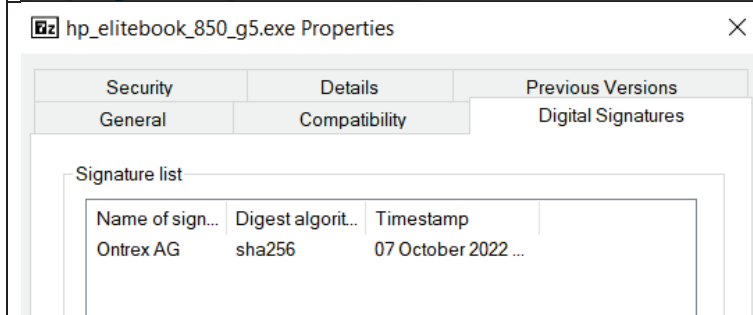
Sign the finished archive (with timestamp)

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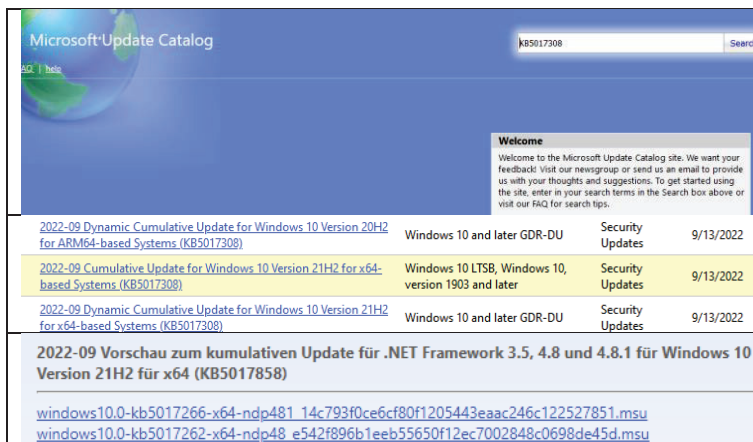
Go to https://catalog.update.microsoft.com/Home.aspx and search for the KB article numbers in the top right

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

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

---

.NET Desktop Runtime 6.0.15

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	Arm64 | x64 | x86 | winget instructions	

For .NET 6, go to https://dotnet.microsoft.com/en-us/download/dotnet/6.0 and download the newest "Desktop Runtime" for x64

Microsoft Defender

Antimalware solution	Definition version
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.e

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)

3 Get SoftPaqs   **Analyze**

For HP, select all models, then press Analyze

---

bios   ✕   📊 ✏️

Filter for the word "bios"

⚠ Critical   Select Components to Download/Apply ▾   ⬇ Download (3)

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"

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 only"
☐ Select all ▲ System ☐ 20JH [ThinkPad Yoga 370] ☑ 20LC [ThinkPad P52s]	For Lenovo, select the model in Update Retriever, then search for updates
Type: **Bios** Systems: Select... Search	Filter for "Bios"
☑ Title: BIOS Update Utility - 10/11 Update ID: n27uj32w Severity: Recommended Type: Bios	Then download the BIOS update
PC > DVD Drive (E:) CES_X64FREV_DE-DE_DV9 > configuration > biosupdates Name / Date modified / Type / Size hp_elitebook_850_g5_sp152771.exe 25.06.2024 19:04 Application 16'795 KB hp_zbook_fury_16_g9_sp153119.exe 25.06.2024 19:04 Application 23'575 KB hp_zbook_fury_16_g10_sp151263.exe 25.03.2024 09:33 Application 23'935 KB lenovo_thinkpad_p52s_n27uj32w.exe 25.06.2024 16:43 Application 12'910 KB	Rename them with their respective models, and copy them to the "biosupdates" directory under customization

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

Choose the download you want ☐ File Name Size ☐ Windows 11 version 22H2 Security Baseline.zip 1.4 MB ☑ LGPO.zip 520 KB	On https://www.microsoft.com/en-us/download/details.aspx?id=55319 download LGPO.exe
☐ Windows 10 version 21H1 Security Baseline.zip 1.2 MB ☑ Windows 10 version 21H2 Security Baseline.zip 1.2 MB ☐ Windows 11 Security Baseline.zip 1.2 MB	And the baselines for 21H2

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

Swiss Post recommendations

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

CIS Benchmark

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

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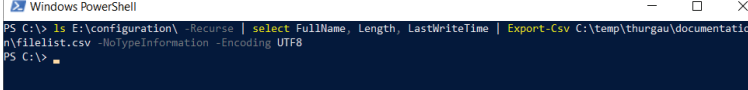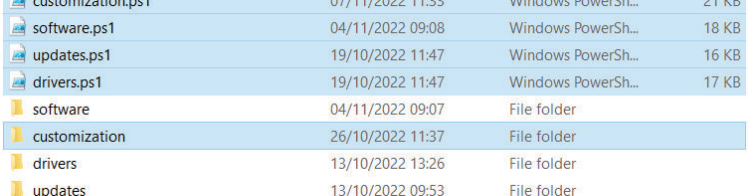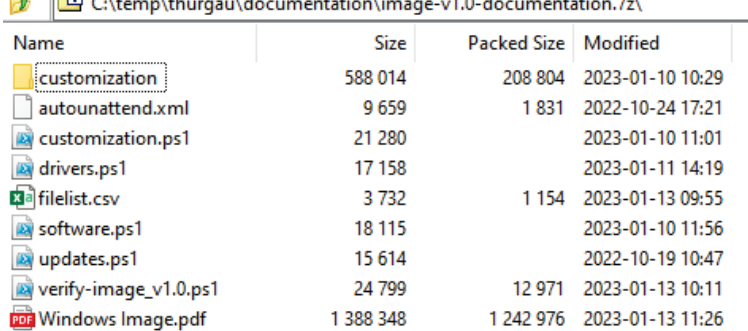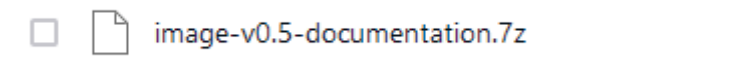
When a new version of the image has to be created, the following steps need to be executed:

- 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.
- 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.
- 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.
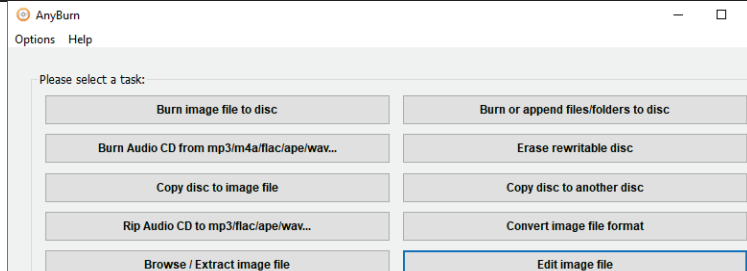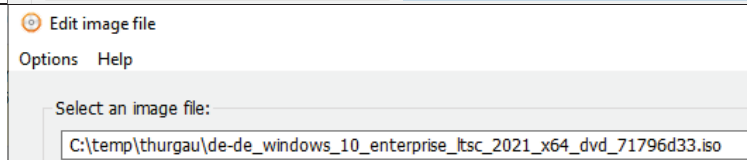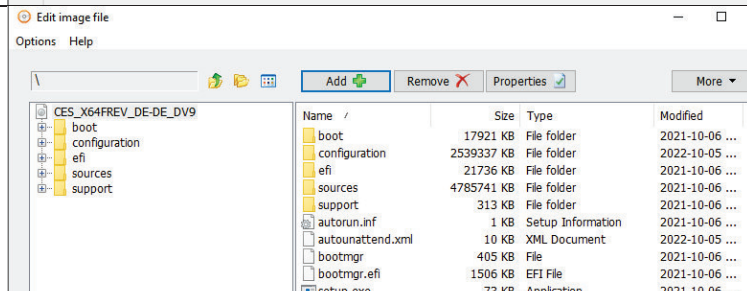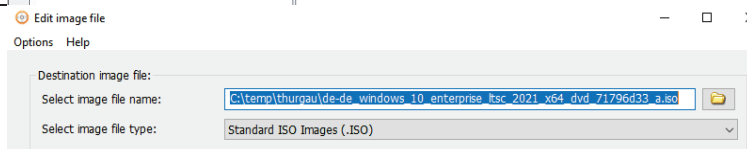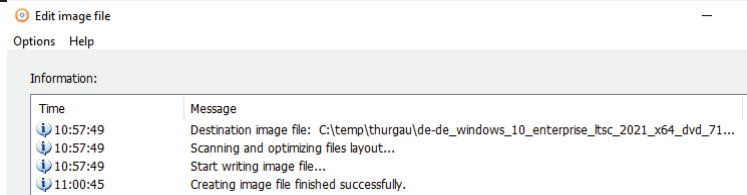
	Export a list of all the customized files to a CSV file using the command: `ls E:\configuration\ -Recurse	select FullName, Length, LastWriteTime	Export-Csv C:\temp\thurgau\documentation\filelist.csv -NoTypeInformation -Encoding UTF8`
	Archive the four PowerShell files and the entire "customization" directory into a zip file…
	…and add: • autounattend.xml • filelist.csv • the image verification script • image documentation Word file as a PDF
	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

AnyBurn — □ Options Help Please select a task: | 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...	Convert image file format
Browse / Extract image file	**Edit image file**		Start Anyburn, then choose "Edit Image"
Edit image file Options Help Select an image file: C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71796d33.iso	Open a bootable ISO file
Edit image file — □ Options Help \ 🔄 📁 ⊞ Add ➕ Remove ✖ Properties ✔ More ▾ 📁 CES_X64FREV_DE-DE_DV9 ⊞ boot ⊞ configuration ⊞ efi ⊞ sources ⊞ support Name ∕ Size Type Modified 📁 boot 17921 KB File folder 2021-10-06 ... 📁 configuration 2539337 KB File folder 2022-10-05 ... 📁 efi 21736 KB File folder 2021-10-06 ... 📁 sources 4785741 KB File folder 2021-10-06 ... 📁 support 313 KB File folder 2021-10-06 ... 📄 autorun.inf 1 KB Setup Information 2021-10-06 ... 📄 autounattend.xml 10 KB XML Document 2022-10-05 ... 📄 bootmgr 405 KB File 2021-10-06 ... 📄 bootmgr.efi 1506 KB EFI File 2021-10-06 ... 📄 setup.exe 73 KB Application 2021-10-06 ...	Add the "autounattend.xml" and the "configuration" directory
Edit image file — □ ✕ Options Help Destination image file: Select image file name: C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71796d33_a.iso 📁 Select image file type: Standard ISO Images (.ISO)	Save under a different name
Edit image file — □ Options Help Information: Time Message 🕐 10:57:49 Destination image file: C:\temp\thurgau\de-de_windows_10_enterprise_ltsc_2021_x64_dvd_71... 🕐 10:57:49 Scanning and optimizing files layout... 🕐 10:57:49 Start writing image file... 🕐 11:00:45 Creating image file finished successfully.	Wait until it's finished

Upload the image
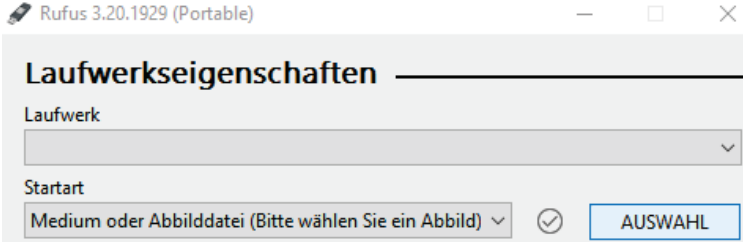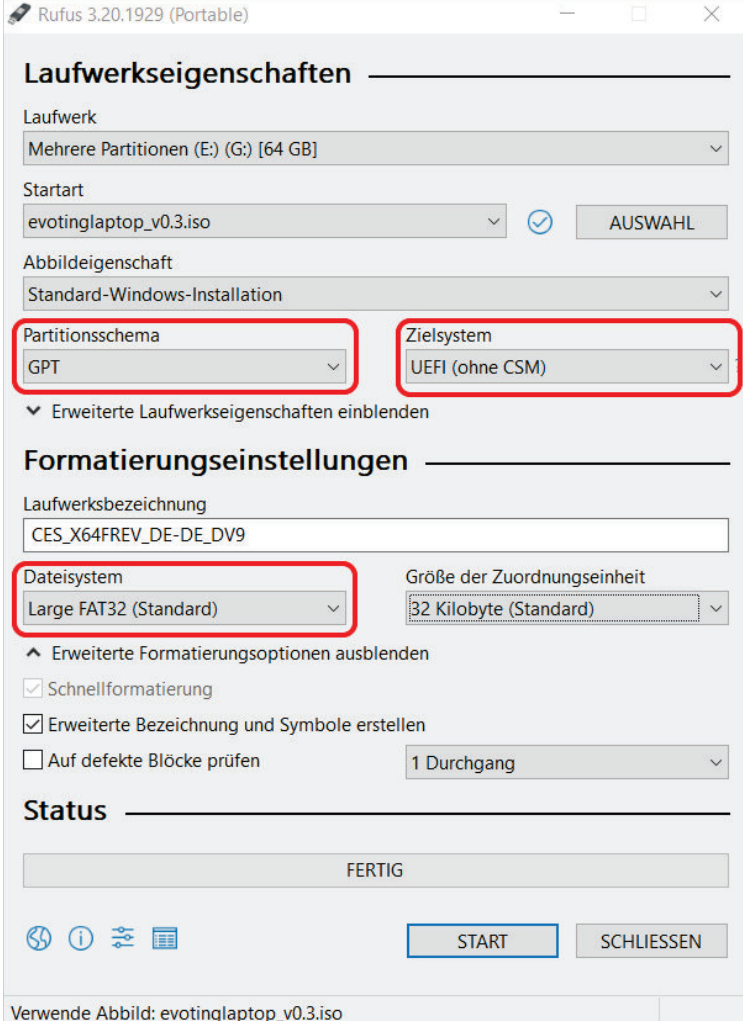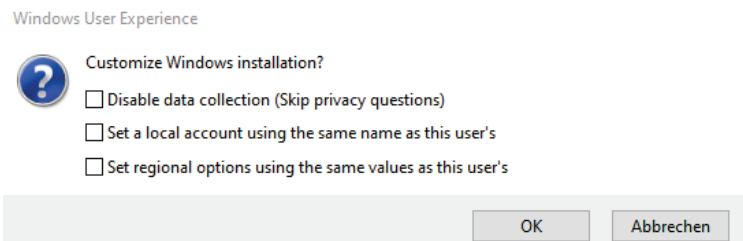
💿 evotinglaptop_v0.5.iso	Rename the resulting image to evotinglaptop_vx.y.iso

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
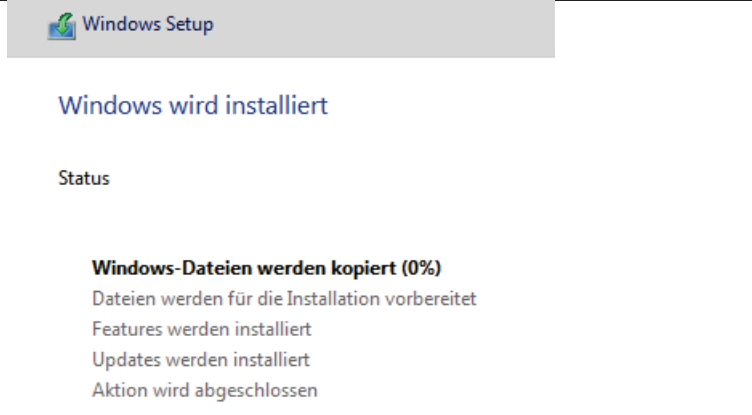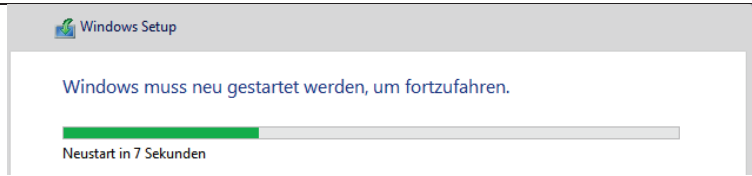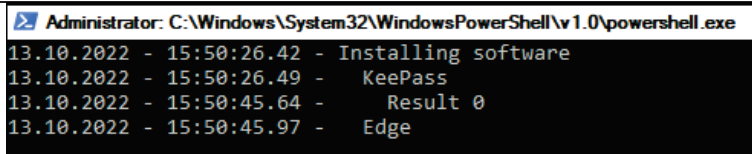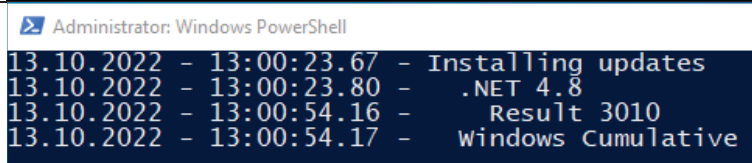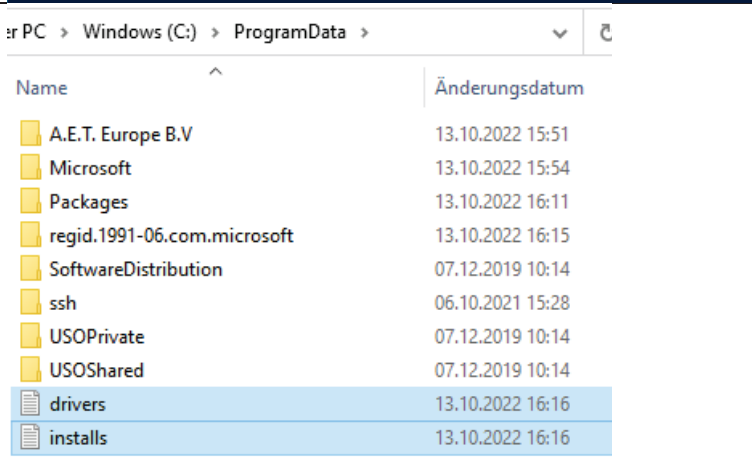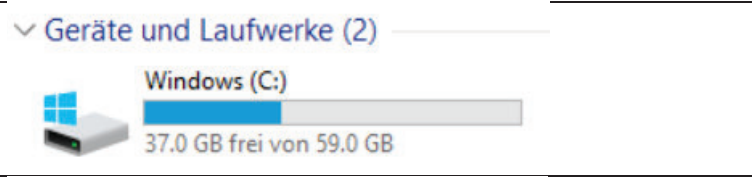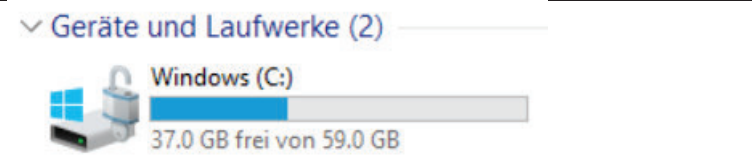
User Guide

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
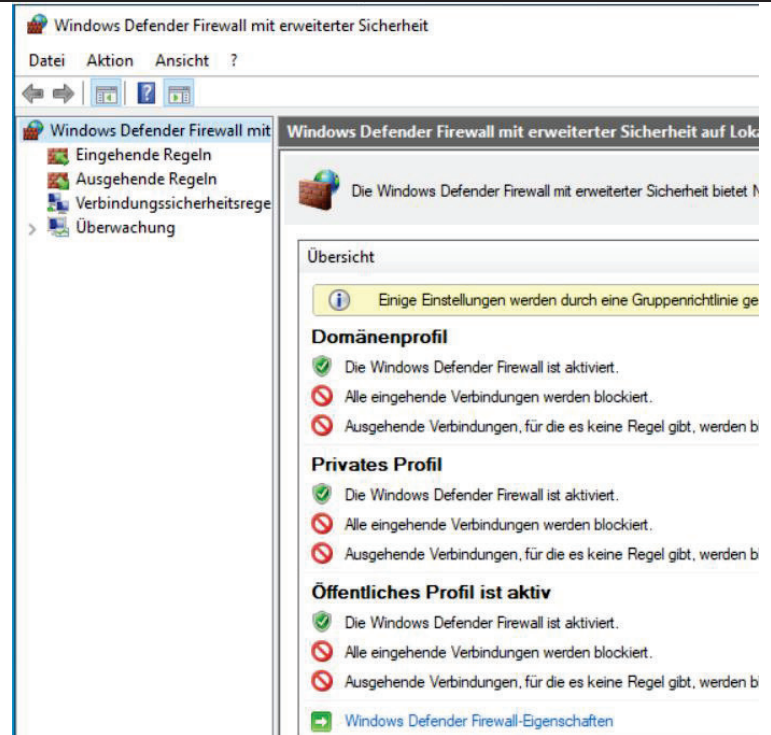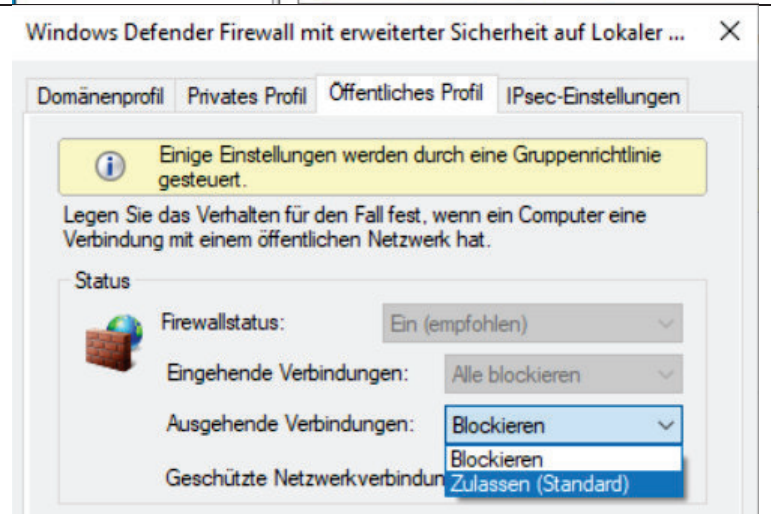
Apply the image to a computer

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

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.

	Download the German Windows LTSC 2021 ISO from an official Microsoft source, like the VLSC, the partner download portal or Visual Studio Downloads.
	Run the script with the parameter -ReferenceISO pointing to the above ISO file, and -ImageUSB set to the USB drive that should be checked
	Optionally, the parameter "-DisplayPositiveResults" can be used to show correctly checked files in green
	The script will output a detailed report in the "Documents" directory that shows check results for all files

ISO folder listing:

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

PowerShell output 1:
```
PS C:\users\athman.boukhaoua\Documents\Kanton-Thurgau> .\verify-image.ps1 -ReferenceISO "C:\temp\thurgau\de-de_windows_1
0_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
```

PowerShell output 2:
```
PS C:\users\athman.boukhaoua\Documents\Kanton-Thurgau> .\verify-image.ps1 -ReferenceISO "C:\temp\thurgau\de-de_windows_1
0_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
```

Report spreadsheet:

	A	B	C	D
1	Info	Reason	Result	FileName
2	3378723Cl	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

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/