Evoting – Basic installation and hardening

Version 1.5 Date

2024-06-27

Ontrex

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	https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPIA.html
Assistant	
Lenovo Update	https://support.lenovo.com/ch/en/solutions/ht037099-download-
Retriever	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



Notepad++

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

Notepad++ F	lugins							
Macro Run	Plugins	Winde	ow ?					On a test computer, install
* 🖪 🖼		ME Tool nverter	s		> >		[Notepad++ and start Plugins Admin
	NppExport >				>			
	Plu	gins Ad	lmin					
		stalled	Incomp	atible				Install «Compare», «Explorer», «XML Tools» and «JSTool»
Plugin				Versio	n			
Compa	re			2.0.2				
Explore				1.9.9				
JSTool				1.2312	2			
Mime t	ools			3.1				
Npp Co	nverter			4.6				
				0.4				
XML To				3.1.1.1	13			
	5 >	5 v	,	urchsuchen				Then package the four plugins as
Name	^		Änderungsdatu	m 1	Гур		Größe	
ComparePlu	gin		06.10.2022 12:38	3 [Dateiordne	er		-
Config			29.11.2023 12:09		Dateiordne			
disabled			29.11.2023 12:09 06.10.2022 12:38		Dateiordne Dateiordne		_	
JSMinNPP			20 11 2022 12:30					
mimeTools		fnen			Ine	er		
NppConverte		neuem Fenste			Ine			
NppExport	An 7-2	Schnellzugrif Zip	annerten		> Ine		n Arehiv hinzufügen	
AIVIL 100IS					1	Zu einen	Rentality ninzurugen	

...

PowerShell 7

On https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-onwindows?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 f or 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	Start HP Image Assistant, click on
File Tools Languages Help	the download icon on the left,
Download SoftPaqs	then choose "Edit Product List",
Q 1 Create My Products List Edit	and add the computer model(s) we need drivers for, then click
2 Select from My Products List	analyse
3 Get SoftPaqs Analyze	
Available SoftPaqs Advisories	Check "Inf Install supported" to
	filter for only drivers (not application or BIOS)
Critical INF Installation Supported	application of BIOS)
All None	
Name Supersede	
Alcor Micro Sma	
Recommended	
Routine	
✓ INF Installation Supported	
Upattended Installation Supported	
A Critical INF Installation Supported ✓ Download (34)	Then click "Download"
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	
Q Download SoftPaqs	Choose "Download and Extract"
Operation	
 Download SoftPaq(s) only 	
Ownload and extract SoftPaqs	
Folder preview	
Download C:\HPIADownloads\spXXXXX.exe	
Unpack	
C:\HPIADownloads\spXXXX	
er (i i i i i bonniedde (epsodoor	



C > Windows (C:) > HPIADownloads			🗸 🖸 🔎 Sea	In the download directory, delet
Name	Date modified	Туре	Size	the driver packages, but keep th
				extracted directories and the
Readme (20230329 094525).html 4 sp74518.exe	29.03.2023 09:45 29.03.2023 09:45	Firefox HTML Do Application	c 133 KB 9'937 KB	
🕼 sp74518.exe	29.03.2023 09:45	Application	417'876 KB	readme file
sp82020.exe	29.03.2023 09:44	Application	3'159 KB	
sp02020.exe sp01562.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	
<pre>// sp96501.exe</pre>	29.03.2023 09:42	Application	975 KB	
1 sp98820.exe		the state of the s		
Delete Multiple I	tems		×	
	u sure you want to permanent	lu delete these 22 items	2	
(k) sp111438.exe	u sule you want to permanent	iy delete these 22 items	•	
// sp112848.exe		<u>Y</u> es	No	
🕼 sp112983.exe	L910912029 09111	Application	11 200 100	
🕼 sp115295.exe	29.03.2023 09:40	Application	352'192 KB	
🕼 sp135655.exe	29.03.2023 09:39	Application	1′473 KB	
(g) sp138373.exe	29.03.2023 09:39	Application	681 KB	
4 sp140913.exe	29.03.2023 09:39	Application	16'019 KB	
(g) sp141045.exe	29.03.2023 09:39	Application	22'148 KB	
sp141851.exe	29.03.2023 09:39	Application	36'821 KB	
<pre> sp142504.exe </pre>	29.03.2023 09:39	Application	58'157 KB	
<pre> sp142679.exe </pre>	29.03.2023 09:39	Application	421 KB	
<pre> sp143121.exe </pre>	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		
Packages will be hosted in a local	Packages will be host			
lirectory or network share.	database will be stored Note: Lenovo System supports this feature. 1	Update (version 5.07.0	or network share.)046 and later)	location to a local directory
-	database will be stored Note: Lenovo System supports this feature. T feature.	in the local directory Update (version 5.07.0	or network share.)046 and later)	
Repository path	database will be stored Note: Lenovo System supports this feature. 1 feature. triever	in the local directory Update (version 5.07.0	or network share. 1046 and later) support this	
Repository path C:\temp\rei ThinkVantage Update Ret Warning	database will be stored Note: Lenovo System supports this feature. I feature. triever	I in the local directory Update (version 5.07. Thin Installer does not	or network share. 1046 and later) support this X	Press "Continue", then "Yes"
Repository path c:\temp\ree ThinkVantage Update Ret	database will be stored Note: Lenovo System supports this feature. I feature. triever	I in the local directory Update (version 5.07. Thin Installer does not	or network share. 1046 and later) support this X	
Repository path c:\temp\ref ThinkVantage Update Ret Warning	database will be stored Note: Lenovo System supports this feature. I feature. triever riever	I in the local directory Update (version 5.07. Thin Installer does not	or network share. 1046 and later) support this X	
Repository path c:\temp\ref ThinkVantage Update Ret Warning The location you spec	database will be stored Note: Lenovo System supports this feature. I feature. triever riever	I in the local directory Update (version 5.07. Thin Installer does not in the second s	or network share. 1046 and later) support this	Press "Continue", then "Yes" Add the laptop model you want
ThinkVantage Update Ret Warning The location you spec isstem Machine Type (e.g. 4177) 20LC ThinkPad	database will be stored Note: Lenovo System supports this feature. I feature. triever cified does not exist. [Yes No (e.g. Thinkpad T520) Operating 2525 Windows	d in the local directory Update (version 5.07. Chin Installer does not in Do you want to c Default	or network share. 1046 and later) support this x reate it? Continue	Press "Continue", then "Yes" Add the laptop model you want to get drivers for
Repository path c:\temp\ref ThinkVantage Update Ret Warning The location you spec Asstern Machine Type (e.g. 4177) ? Description 20LC ThinkPad PS2s) W	database will be stored Note: Lenovo System supports this feature. I feature. triever riever sified does not exist. I Yes No (e.g. Thinkpad T520) Operating	d in the local directory Update (version 5.07. Chin Installer does not in Do you want to c Default	or network share. 1046 and later) support this x reate it? Add Remove	Press "Continue", then "Yes"
Repository path c:\temp\ref ThinkVantage Update Ret Warning The location you spec ystem Machine Type (e.g. 4177) ? Description 20LC ThinkPad P32s] W	database will be stored Note: Lenovo System supports this feature. I feature. triever cified does not exist. I Ves No (e.g. Thinkpad T520) Operating 352s Windows	d in the local directory Update (version 5.07. Chin Installer does not in Do you want to c Default	or network share. 1046 and later) support this x reate it? Continue Add	Press "Continue", then "Yes" Add the laptop model you want to get drivers for Then select it and press "Next"
Repository path c:\temp\ref ThinkVantage Update Ret Warning The location you spec ystem Machine Type (e.g. 4177) ? Description 20LC ThinkPad PS2s) W	database will be stored Note: Lenovo System supports this feature. I feature. triever cified does not exist. I Ves No (e.g. Thinkpad T520) Operating 352s Windows	d in the local directory Update (version 5.07. Chin Installer does not in Do you want to c Default	or network share. 1046 and later) support this x reate it? Add Remove	Press "Continue", then "Yes" Add the laptop model you want to get drivers for

Select	A 411							
X	t All						View que	Select all drivers and press "Next"
	Title	Update ID	Severity	Туре	Existing version	Version	Size	
	Intel Dynamic Plat	n27he01w	Recommended	Driver		8.3.10208.5644	3.31 MB	
	Integrated Camera		Recommended	Driver	1.00	10.0.16299.11319	6.70 MB	
			Recommended	Driver	-	3.5.18.32	6.70 MB	
	Intel Bluetooth Dri NXP NFC Driver(W	n27wv02w	Recommended Recommended	Driver		20.60.0.4	1.95 MB	
				Driver	-	12.0.3.0	1.42 MB	
	NXP NFC Driver (NXP NFC Driver (n27wb01w n27wa03w	Recommended Recommended	Driver Driver		12.0.1.0 12.0.2.0	1.66 MB 1.71 MB	
	Fibocom L830-EB	nz3wf01w	Recommended	Driver	-	3.2.0.1	1.37 MB	
	Fibocom L830-EB		Recommended	Driver		3.19041.2034.1	1.31 MB	
	Intel Dynamic Plat		Recommended	Driver	-	8.4.11000.6436	3.51 MB	
	Integrated Camera		Recommended	Driver	-	10.0.19041.20176	20.50 MB	
	Integrated Camera		Recommended	Driver	1772	5.0.18.88	20.50 MB	
Ø + 9	Synaptics UltraNav	n20gx20w	Critical	Driver	-	19.3.4.228	27.41 MB	
✓ + I	Intel Chipset Drive	n27ic04w	Recommended	Driver	120	10.1.18228.8176	3.54 MB	
	Intel PRO/1000 LA		Critical	Driver	100	12.18.9.11	1.57 MB	
	Realtek Media Car	n27x805w	Recommended	Driver	•	10.0.17134.31242	1.85 MB	
Total sele Hide O O This	version	21 GB	-				Show local p	
O This	s version and all future	e versions Hide				Ba	ick Next	
Select	All 20LC [ThinkPa	ad P52s]-Windows 1	D ~					"Finish"
Title			100000	in in	numiti se			
	or Smart Card Reader (Driver 10 (1702 - 1	Update		everity Version			
	or Smart Card Reader I com L830-EB Wireles				mmended 1.7.46.1307 mmended 3.19041.2034.1			
	com L830-EB Wireless				mmended 3.19041.2034.1 mmended 3.2.0.1			
	com L830-EB Wireles				ritical 2.0.1.112			
	eric DisplayLink Driver				mmended 10.1.2875.0			
	eric DisplayLink Driver				mmended 10.2.7042.0			
Integ	grated Camera Driver	for Realtek - 10 (1709	or later n27cd14w		mmended 10.0.19041.20176			
	grated Camera Driver		10 Buil n27cp01w	rea Reco	mmended 10.0.16299.11319			
	grated Camera Driver				mmended 5.0.18.88			
	grated Camera Driver				mmended 3.5.18.32			
	8265 Wireless LAN Dr				ritical 20.70.30.1			
	8265 Wireless LAN Di				critical 20.70.18.2			
	Bluetooth Driver - 10				ritical 22.150.0.6 mmended 20.60.0.4			
	l Bluetooth Driver(Win I Chipset Driver - 10 /1		- 10 [64] n27wv02 n27ic04		mmended 20.00.0.4 mmended 10.1.18228.8176			
	Dynamic Platform ar				mmended 8.4.11000.6436			
	Dynamic Platform A				mmended 8.3.10208.5644			
	Gigabit Ethernet Driv				mmended 12.19.1.37			
	Graphics Driver - 10 (w c	ritical 30.0.100.9865			
- · · ·	Management Engine	Software - 10 (1703	or Later) n27ra21	w C	ritical 2205.15.0.2623			
∠ Intel			101/ 27 0/					
	PRO/1000 LAN Adap	ter Software(Windov	/s 10 Ver n27rw06	w c	critical 12.18.9.11			
🗹 Intel					ritical 12.18.9.11 mmended 30.100.1841.2			
✓ Intel	l PRO/1000 LAN Adap I Serial IO Driver - 10 ('							
✓ Intel	PRO/1000 LAN Adap					Baci	Finish	
Intel	IPRO/1000 LAN Adap ISerial IO Driver - 10 (a, 2.21 GB inkVantag rrent Resu	e Update Its (Click	Retriever link to viev	has fini v detai	shed downloa			Wait for the downloads to finish
Intel Intel	ISerial IO Driver - 10 (s. 2.21 GB InkVantag rrent Resu	e Update Ilts (Click	Retriever link to view	w Reco has fini v detai	shed downloa		updates	
Intel Intel	ISerial IO Driver - 10 (s. 2.21 GB InkVantag rrent Resu	e Update Ilts (Click <u>es downloa</u> temp > re	Retriever link to viev	w Reco has fini v detai	shed downloa			This will create a lot of directories
Intel Intel	IPRO/IODILAN Adaps ISerial IO Driver - 10 (s, 2.21 GB inkVantag rrent Resu <u>42 update</u> Windows (C:)	e Update Ilts (Click	Retriever link to viev ded success	w Reco has fini v detai	shed downloa		updates	
	IPRO/IODILAN Adaps ISerial IO Driver - 10 (s, 2.21 GB inkVantag rrent Resu <u>42 update</u> Windows (C:)	e Update Ilts (Click <u>es downloa</u> temp > re	Retriever link to viev ded success	has fini v detai sfully.	shed downloa		updates	This will create a lot of directories with drivers inside executable
⊘ Intel ⊘ Intel ? updates Thi Cui	IPRO/IODILAN Adaps ISerial IO Driver - 10 (s, 2.21 GB inkVantag rrent Resu <u>42 update</u> Windows (C:)	e Update Ilts (Click <u>es downloa</u> temp > re	Retriever link to view ded success triever > n1fup D.	has fini v detai sfully.	shed downloa ls):	ding new	updates	This will create a lot of directories
© Intel ⊘ Intel 2 updates Thi Cui PC → Name	IPRO/TODILAN Adaps ISerial ID Driver - 10 (ink Vantag ink Vantag <u>42 update</u> Windows (C:) e 1fupa0w	e Update Ilts (Click <u>es downloa</u> temp > re	Retriever link to view ded success triever > n1fup D, 3/	w Reco has fini v detai sfully. aa0w ate modifi (29/2023 10	shed downloa ls): :07 AM Applic	ding new	v ð Size 4,326 KB	This will create a lot of directories with drivers inside executable
⊘ Intel ⊘ Intel 2 updates Thi Cur DC → Name ∰ n n] n	IPRO/TODI LAN Adaps ISerial ID Driver - 10 (ink Vantag rrrent Resu <u>42 update</u> Windows (C:) e 1fupa0w 1fupa0w	e Update Ilts (Click <u>es downloa</u> temp > re	Retriever link to view ded success triever > n1fup J, 3/ 3/	w Reco has fini v detai sfully. a0w ate modifi (29/2023 10 (29/2023 10)	ed Type 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2	ding new ation	v ð Size 4,326 KB 44 KB	This will create a lot of directories with drivers inside executable
⊘ Intel ⊘ Intel 2 updates Thi Cur DC → Name ∰ n n] n	IPRO/TODILAN Adaps ISerial ID Driver - 10 (ink Vantag ink Vantag <u>42 update</u> Windows (C:) e 1fupa0w	e Update Ilts (Click <u>es downloa</u> temp > re	Retriever link to view ded success triever > n1fup J, 3/ 3/	w Reco has fini v detai sfully. aa0w ate modifi (29/2023 10	ed Type 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2	ding new	v ð Size 4,326 KB	This will create a lot of directories with drivers inside executable
⊘ Intel ⊘ Intel 2 updates Thi Cur PC → Name n n n n	IPRO/TODI LAN Adaps ISerial ID Driver - 10 (ink Vantag rrrent Resu <u>42 update</u> Windows (C:) e 1fupa0w 1fupa0w	e Update Ilts (Click es downloa > temp > re	Retriever link to view ded success triever > n1fup J, 3/ 3/	w Reco has fini v detai sfully. a0w ate modifi (29/2023 10 (29/2023 10)	ed Type 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2	ding new ation	v ð Size 4,326 KB 44 KB	This will create a lot of directories with drivers inside executable archives
⊘ Intel	IPRO/1000 LAN Adap ISerial IO Driver - 10 (s, 2.21 GB INK Vantag Ink Vantag Vantag Vindows (C:) e 11 (upa0w 11 (upa0w 11 (upa0w 11 (upa0w)	e Update Ilts (Click es downloa > temp > re	Retriever link to view ided success triever > n1fup J 3/ 3/ 3/	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable
⊘ Intel	IPRO/1000 LAN Adap ISerial 10 Driver - 10 (s, 2.21 GB Ink Vantag rrent Resu <u>42 update</u> Windows (C:) e Ifupa0w Ifupa0w Ifupa0w 1fupa0w 1fupa0w 2_ inistrator: Windows F	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2 20100.1841.2	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a
<pre>⊘ Intel ⊘ Intel ♡ updates</pre>	IPRO/1000 LAN Adap ISerial IO Driver - 10 (s, 2.21 GB Ink Vantag Irrent Resu <u>42 update</u> Windows (C:) e 11fupa0w 11fupa0w 11fupa0w 11fupa0w 2_ inistrator: Windows F	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives
⊘ Intel ⊘ Intel vupdates vupdates Thi Cun PC → Name pn n n n Adm Adm Adm	IPRO/1000 LAN Adaps ISreial O Driver - 10 (ISreial O Driver - 10 (ISreial O Driver - 10 (InkVantag InkV	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to
<pre> Intel Intel Intel Intel Intel Intel Intel Thi Cun Cun Cun Cun Cun Intel Intel</pre>	IPRO/1000 LAN Adap ISerial 10 Driver - 10 (* s, 2.21 GB inkVantag rrent Resu 42 update Windows (C;) e 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 2_ inistrator: Windows F 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a
<pre> Intel Intel</pre>	IPRO/1000 LAN Adap ISerial 10 Driver - 10 (* s, 2.21 GB inkVantag rrrent Resu <u>42 update</u> Windows (C:) e Ifupa0w Ifupa0w Ifupa0w Ifupa0w Ifupa0w (************************************	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to
⊘ Intel ⊘ Intel ⊘ Intel ∴ updates Thi Cur Cur Cur Cur QC > Name QC > Name QC > Adm S C:VII Cur Adm S C:VII	IPRO/1000 LAN Adaps ISerial 10 Driver - 10 (1 s, 2.21 GB ink Vantag rrrent Resu 42 update Windows (C:) e 11upa0w 11upa0w 11upa0w 11upa0w 11upa0w 12upa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages:
Intelevent of the second s	IPRO/1000 LAN Adaps ISerial 10 Driver - 10 (ink Vantag ink Vantag rrrent Resu 42 update Windows (C:) e 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages:
Intel intel intel intel Cur Cur Cur Cur intel intel intel intel intel intel intel intel Cur intel i	IPRO/1000 LAN Adap ISerial IO Driver - 10 (ink Vantag rrent Resu <u>42 update</u> Windows (C:) e Ifupa0w Ifupa0w Ifupa0w Ifupa0w Ifupa0w Statastor: Windows F Statastor: Windows F St	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages: 1s C:\temp\retriever*.exe -
⊘ Intel ⊘ Intel ⊘ Intel ⊘ Intel Current Curent Current Current Current Current Current Current Cur	IPRO/1000 LAN Adap ISerial 10 Driver - 10 (ink Vantag ink Vantag rrent Resu 42 update Windows (C:) e 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w 1fupa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages:
Intel intel intel intel Cur Cur Cur Cur intel intel intel intel intel intel intel intel Cur intel i	IPRO/1000 LAN Adaps ISerial 10 Driver - 10 (1 s, 2.21 GB ink Vantag rrent Resu <u>42 update</u> Windows (C:) e 11upa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages: ls C:\temp\retriever*.exe - Recurse % { \$BaseName; &
⊘ Intel ⊘ Intel ⊘ Intel ⊘ Intel Cur Cur Cur PC → Name PC → Name PC Name PC → Name	IPRO/1000 LAN Adaps ISerial 10 Driver - 10 (1 s, 2.21 GB ink Vantag rrent Resu <u>42 update</u> Windows (C:) e 11upa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages: ls C:\temp\retriever*.exe - Recurse % { \$BaseName; & \$_ /VERYSILENT
⊘ Intel ⊘ Intel ⊘ Intel ⊘ Intel Cur Cur Cur PC → Name PC → Name PC Name PC → Name	IPRO/1000 LAN Adaps ISerial 10 Driver - 10 (1 s, 2.21 GB ink Vantag rrent Resu <u>42 update</u> Windows (C:) e 11upa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages: ls C:\temp\retriever*.exe - Recurse % { \$BaseName; &
⊘ Intel ⊘ Intel ⊘ Intel ⊘ Intel Cur Cur Cur PC → Name PC → Name PC Name PC → Name	IPRO/1000 LAN Adaps ISerial 10 Driver - 10 (1 s, 2.21 GB ink Vantag rrent Resu <u>42 update</u> Windows (C:) e 11upa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives 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\\$(\$
⊘ Intel ⊘ Intel ⊘ Intel ⊘ Intel Cur Cur Cur PC → Name PC → Name PC Name PC → Name	IPRO/1000 LAN Adaps ISerial 10 Driver - 10 (1 s, 2.21 GB ink Vantag rrent Resu <u>42 update</u> Windows (C:) e 11upa0w	e Update Ilts (Click es downloa > temp > re ^ PowerShell 14 C:\temp\ret	Retriever Iink to view ded success triever > n1fup D, 3/ 3/ 3/ 	w Reco has fini v detai sfully. pa0w ate modifi (29/2023 10 (29/2023 10) (29/2023 10)	ed Type 207 AM Applic 207 AM Text Do 207 AM XML D	ding new ation ocument	v ひ Size 4,326 KB 44 KB 11 KB	This will create a lot of directories with drivers inside executable archives Use the following command in a window with admin rights to extract the packages: ls C:\temp\retriever*.exe - Recurse % { \$BaseName; & \$_ /VERYSILENT



C → Windows (C:) → temp → retriever	r2 > n1fupa0w > Comp >	5 V	This extracts the archive to usable	
Name	Date modified	Туре	Size	file collections
LEPLang	3/29/2023 10:13 AM	File folder		
Resource	3/29/2023 10:13 AM	File folder		
dock_port	12/4/2022 9:57 PM	PNG File	9 KB	
EasyResume	12/4/2022 10:04 PM	Application	2,298 KB	
EventLogger.dll	12/4/2022 10:04 PM	Application exten	103 KB	
InstHelper.dll	12/4/2022 10:04 PM	Application exten	169 KB	
iTin.Core.dll	12/4/2022 10:05 PM	Application exten	45 KB	
Lenovo.Vantage.RpcClient.dll	12/4/2022 10:05 PM	Application exten	31 KB	

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

	12						Add the extracted folders to a
ime	^	Date modified	Туре	Size			7zip archive
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		20.02.2022.00.42	File folder				
sp94816	Pin to Quick acce	55	File folder				
sp96234	7-Zip	>	Add to archive	6			
sp96501	Signieren und vers	chlüsseln	Compress and email	45			
sp98820	Mehr GpgEX Optio	onen >	Add to "HPIADownload	ls.7z"			
sp101370	Send to	<u> </u>	Compress to "HPIADov	vnloads.	7z" and e	email	
sp104124	Send to	/	Add to "HPIADownload	ls.zip"			
sp111438	Cut		Compress to "HPIADov	vnloads.	zip" and	email	
sp112848	Сору		CRC SHA			>	
sp115295	Create shortcut		Filefolder		_		
sp135655	Delete		File folder				
sp138373	Rename		File folder				
sp140913			File folder				
sp141045	Properties		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 (202	230329 094525).html	29.03.2023 09:45	Firefox HTML Doc.		133 KB		

Add to Archive				×	
				^	As self-extracting archive with the
Archive: C:\HPIADownload			~		name of the laptop model
		40.00			
Archive <u>f</u> ormat:	7z ~	<u>U</u> pdate mode:	Add and replace files	~	
Compression level:	5 - Nomal 🗸 🗸	Path mode:	Relative pathnames	~	
Compression method:	* LZMA2 ~	Options	<u> </u>		
Dictionary size:	* 16 MB $\qquad \sim$	Create SFX arch			
Word size:	* 32 ~	Delete files after	r compression		
<u>S</u> olid Block size:	* 4 GB ~	Encryption			
Number of CPU threads:	* 8 ~ / 8	Enter password:			
Memory usage for Compressing 1248 MB / 12953 MB / 16191 Memory usage for Decompress	MB *80% ~	Reenter password:			
Split to <u>v</u> olumes, bytes:	-	_			
	~	Show Password			
Parameters:		Encryption method:		~	
		Encrypt file <u>n</u> am	es		
Ortions					
Options					
		ОК	Cancel Help		
Z hp elitebook 85	50_g5.exe Properties			×	Sign the finished archive (with
					timestamp)
Security	Details	Pr	evious Versions		
General	Compatibilit	y [Digital Signatures		
Signature list					
Name of sign.	Digest algorit Tir	nestamp			
Ontrex AG	U	October 2022			

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

Microsoft Update Catalog	K B5017308		Search	Go to https://catalog.update.microsoft.
	Welcome Welcome to the Micro feedback Visit our n us shall your hought the site, enter in your visit our FAQ for sea	<u>com/Home.aspx</u> and search for the KB article numbers in the top right		
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	For the monthly updates,
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	download the regular cumulative
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	update, not the dynamic one
2022-09 Vorschau zum kumulativen Update für .N Version 21H2 für x64 (KB5017858) 	For .NET only download the 4.8.1 package, not the 4.8			

<u>Windows Maliciou</u> <u>Removal Tool - v5.</u> (<u>KB890830)</u>		Update Rollups	10/11/2022	For the malicious software removal tool, sort by date, then
Windows Maliciou Removal Tool x64 - (KB890830)		Update Rollups	10/11/2022	pick the newest package for
<u>Windows Maliciou</u> <u>Removal Tool - v5.</u> (<u>KB890830)</u>		Update Rollups	10/11/2022	Windows 10 64 bit
.NET Desk	top Runtime 6.0.15			For .NET 6, go to
The .NET Deskto	op Runtime enables you to run existing Windows desktop es the .NET Runtime; you don't need to install it separ	ons. This	https://dotnet.microsoft.com/en- us/download/dotnet/6.0 and	
os	Installers	ries	download the newest "Desktop	
Windows	Arm64 x64 x86 winget instructions		Runtime" for x64	

Microsoft Defender

Antimalware solution	Definition version	On
Microsoft Defender Antivirus for Windows 11, Windows 10, Windows 8.1, and Windows Server	<u>32-bit 64-bit ARM</u>	https://www.microsoft.com/en- us/wdsi/defenderupdates Download the 64-bit Version for the antivirus definitions
Update for Microsoft Defender Antivirus antimalware platform Microsoft Defender Definition - KB4052623 (Version 4.18.2211.5) Antivirus Updates	12/8/2022	For the antimalware update, download the newest "Definition Updates" package
updateplatform.x86fre_85dfdcc7cc8df1062fc64ae81dbe0fc3b4 updateplatform.amd64fre_7f1e1eb218c67263a51f402fb080f1bb updateplatform.arm64fre_9383ac7ca8917dc66023c6ff68d3679c	<u>be311041b.exe</u>	Pick the one for "amd64fre"

BIOS

BIOS		
2 Select from My Products List	 My Products List H P ZBook Fury 16 G10 Mobile Workstation Microsoft Windows 10 version 21H2 (6 H P ZBook Fury 16 G9 Mobile Workstation Microsoft Windows 10 version 21H2 (6 H P LiteBook 850 G5 Notebook PC Microsoft Windows 10 version 21H2 (6 	4-bit) PC 4-bit)
3 Get SoftPaqs	Analyze	
bios	× 🖄 🖉	Filter for the word "bios"
Critical Select Components	to Download/Apply	Then check all the BIOS updates and click "Download"
Name	↓ Category	
HP BIOS and System Firmware (U96	V BIOS - System	n Firm
HP BIOS and System Firmware (V96)	BIOS - Syster	n Firm
HP BIOS Config Utility (BCU)	Software - Sy	vstem
HP Firmware Pack (Q78)	✓ BIOS	



Q Download SoftPaqs	Download SoftPaqs				
Operation					
Download SoftPag(s	s) only				
 Download and extra 					
Folder preview					
Download					
C:\HPIADownloads\s	pXXXXX.exe				
Unpack					
C:\HPIADownloads\s	pXXXXX				
		Start			
Select all				For Lenovo, select the model in	
System				Update Retriever, then search for	
	updates				
20LC [ThinkPad P52s]	20JH [ThinkPad Yoga 370]				
				Filter for "Bios"	
Туре:	Systems:				
Bios 🗸	Select.	. Se	earch		
Title	Update ID	Severity	Туре	Then download the BIOS update	
BIOS Update Utility - 10/11	n27uj32w	Recommended	Bios		
PC > DVD Drive (E:) CES_X64FREV_DE-DE_DV9 > configuration > biosupdates \checkmark ζ			Rename them with their		
Name	Date modified	Туре	Size	respective models, and copy	
//p hp_elitebook_850_g5_sp152771.exe	25.06.2024 19:04	Application	16'795 KB	them to the "biosupdates"	
Image: Weight and the second			directory under customization		
ゆりしていたいでは、「していた」のでは、「「「しん」」を見ていた。 のでは、「「「しん」」を見ていた。 「「しん」、「「しん」、「「しん」、「「しん」、「「しん」、「「しん」、「「しん」、「「しん」、「しん」、	25.03.2024 09:33 25.06.2024 16:43	Application Application	23'935 KB 12'910 KB		

Hardening

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

Microsoft security baselines

Choose the download you want		On https://www.microsoft.com/en-
File Name	Size	us/download/details.aspx?id=553
Windows 11 version 22H2 Security Baseline.zip	1.4 MB	<u>19</u> download LGPO.exe
LGPO.zip	520 KB	
Windows 10 version 21H1 Security Baseline.zip	1.2 MB	And the baselines for 21H2
Vindows 10 version 21H2 Security Baseline.zip	1.2 MB	
Windows 11 Security Baseline.zip	1.2 MB	

r PC → Windows (C:) → temp2 → GPOs			Extract the baseline zip file
Name	Änderungsdatum	Тур	
486589C2-0290-4764-8058-9825B56B4169}	04.10.2022 09:04	Dateiordner	
	04.10.2022 09:04	Dateiordner	
	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	
C:\temp2\GPOs> lgpo /parse /m ".\{23DEF82E-039F-40D5-BBCC-; computer.txt			Export the GPOs as text file using
C:\temp2\GPOs> lgpo /parse /m ".\{486589C2-0290-4764-8058- xt C:\temp2\GPOs> lgpo /parse /m ".\{7AD4F62E-9296-4FEA-9765-			the script.
<pre>citemp2/QPOS> lgp0 /parse /m(/AD4F02E-9296-4FEA-9705- dentialguard.txt C:ttemp2/QPOS> lgp0 /parse /m "\{8669E0C6-C1E3-4582-8797- C:ttemp2/QPOS> lgp0 /parse /m "</pre>			the <u>serpe</u> .
C:\temp2\GPOs> lgpo /parse /m ".\{8697C660-A878-4AF1-B37D-1			
C:\temp2\GPOs> lgpo /parse /m ".\{C94113F4-C027-4F5F-8210-4			
<pre>c.\temp2\GPOs> 1gpo /parse /m .\{D30447D-15A7-4287-A852-; c.\temp2\GPOs> 1gpo /parse /m ".\{D30447D-15A7-4287-A852-;</pre>			
mputer.txt		indefinite (registery) por /q / c	

Swiss Post recommendations

<pre>1 bg _ Set hardming rules free Sets Post" 1 bg _ Registry (set) 1 bg _ Registry (se</pre>	The security settings from the Swiss Post have been implemented as PowerShell commands inside the customization.ps1
--	---

CIS Benchmark

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

Custom settings

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

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

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



Non-implemented security settings

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

Setting	Reason
Disable Windows + R	It's a usability decrease without a clear security benefit
Static DNS server	We didn't want to set a public DNS server like 8.8.8.8 due to
	privacy issues, and the security risk from a DNS based MitM
	attack seemed low considering we're using transport
	encryption
Configure Windows Defender	Because the offline laptops don't have network connectivity,
SmartScreen: Block	this would cause queries to SmartScreen to not work, and
	authorized E-Voting applications to be blocked
Deny write access to removable	We need to save data to unencrypted USB drives during the e-
drives not protected by	voting process
BitLocker	
Block untrusted and unsigned	We need to be able to run executables from USB drives during
processes that run from USB	the e-voting process
Script execution policy: All	We need to be able to run unsigned scripts during the e-voting
Signed	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
 - o 16 MB MSR partition for disk metadata
 - o 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
 - o 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 <u>every application</u> 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 <u>supported model</u>. Make sure to <u>exclude the drivers</u> that have caused issues in the past.
- Download current BIOS update packages for every model, and update the script "checkbiosupdatestatus.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 <u>documentation</u>.
- 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.

Windows PowerShell PS C:> 15 E:\configuration\ -Recurse s Afflelist.csv -NoTypeInformation -Encodi PS C:\> _	select FullName, Length, LastWrit	eTime Export-Csv	C:\temp\thurgau	□ ×	<pre>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</pre>
customization.ps1	07/11/2022 11:33	Windows	PowerSh	21 KB	Archive the four PowerShell files
software.ps1	04/11/2022 09:08	Windows	PowerSh	18 KB	and the entire "customization"
a updates.ps1	19/10/2022 11:47	Windows	PowerSh	16 KB	
drivers.ps1	19/10/2022 11:47		PowerSh	17 KB	directory into a zip file
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	r i	_	
🎓 📴 C:\temp\thurgau\d	ocumentation\image-v1	.0-documenta	ation.7z\		and add:
Name	Size	Packed Size	Modified		 autounattend.xml
customization	588 014	208 804	2023-01-1	0 10:29	 filelist.csv
autounattend.xml	9 659	1 831	2022-10-2	4 17:21	• the image verification
kustomization.ps1	21 280		2023-01-1	0 11:01	_
drivers.ps1	17 158		2023-01-1	1 14:19	script
allelist.csv	3 732	1 154	2023-01-1		 image documentation
software.ps1	18 115		2023-01-1		Word file as a PDF
w updates.ps1	15 614		2022-10-1		
verify-image_v1.0.ps1	24 799	12 971	2022-10-1		
			2023-01-1		
🚾 Windows Image.pdf	1 388 348	1 242 970	2023-01-1	5 11:20	
🗆 🗋 image-v	0.5-documentati	ion.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 > V 🗸				Create a subdirectory for the
Name	Date modified	Туре	Size	current image version, and copy
biosupdates	28.03.2024 15:12	File folder		the documentation 7z, as well as
customization	28.03.2024 15:13	File folder		the directories: <i>customization</i> ,
software	28.03.2024 15:15	File folder		
🔽 image-v1.4-documentation.7z	28.03.2024 15:07	7z Archive	1′412 KB	software and biosupdates

Create the bootable ISO

 AnyBurn Options Help 			- 🗆	Start Anyburn, then choose "Edit
Please select a task:				Image"
Burn image file to disc Burn or append files/folders to disc				
Burn Audio CD from	n mp3/m4a/flac/ape/wav	Erase rewritable disc		
Copy dis	sc to image file	Copy disc to another dis	c	
Rip Audio CD t	o mp3/flac/ape/wav	Convert image file format		
Browse / E	xtract image file	Edit image file		
Edit image file	,			Open a bootable ISO file
Options Help				
Select an image file				
C:\temp\thurgau	\de-de_windows_10_ent	erprise_ltsc_2021_x64_dvd_71	796d33.iso	
Edit image file			- 0	Add the "autounattend.xml" and
Options Help	Options Help			the "configuration" directory
🔪 🕼 👘 Add 🌗 Remove 🗡 Properties 🖌 More 🕶				
CES_X64FREV_DE-DE_DV9 boot configuration efi sources b- support	Name / boot configuration efi sources support autorun.inf autorun.inf autorun.inf bootmgr bootmgr.efi tissetup.exe	Size Type 17921 KB File folder 2539337 KB File folder 21335 KB File folder 21736 KB File folder 313 KB File folder 11 KB Setup Information ml 10 KB XML Document 405 KB File 13 KB File File 73 KB Application	Modified 2021-10-06 2022-10-05 2021-10-06 2021-10-06 2021-10-06 2022-10-05 2021-10-06 2021-10-06 2021-10-06	
Edit image file Options Help			- 🗆 ×	Save under a different name
Destination image file:				
Select image file name:	C:\temp\thurgau\de-de_window	s_10_enterprise_ltsc_2021_x64_dvd_71796d	33_a.iso 🛅	
Select image file type: Standard ISO Images (.ISO)				
O Edit image file			- C	Wait until it's finished
Options Help				
Information:				
	essage			
U10:57:49 Destination image file: C:\temp\thurgau\de-de_windows_10_enterprise_ttsc_2021_x64_dvd_71 Scanning and optimizing files layout				
	tart writing image file			
 11:00:45 	reating image file finished successfully			

Upload the image

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

All Files > Kiteworks > Kanton Thurgau	And upload it to the Kiteworks share
Name ~	https://kiteworks.ontrex.ch/#/fol
🗌 💶 Upload	der/8666a49b-a3d7-4831-9d02- 45666f755d19
evotinglaptop_v0.5.iso	



User Guide

Extract the ISO to a USB Stick

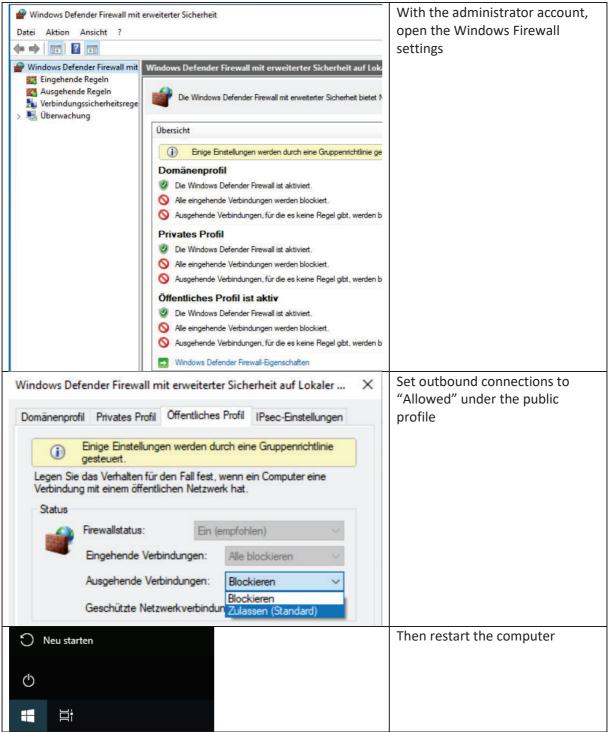
	Start Rufus and select the ISO file
Laufwerkseigenschaften	
Laufwerk	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
Startart	
Medium oder Abbilddatei (Bitte wählen Sie ein Abbild) 🗸 🔗 🛛 AUSWAHL	
✓ Rufus 3.20.1929 (Portable)	Use GPT, UEFI (without CSM) and
	Large FAT32 as options
Laufwerkseigenschaften	
Laufwerk	Do not modify the drive name, it
Mehrere Partitionen (E:) (G:) [64 GB]	has to stay on the default value
Startart	
evotinglaptop_v0.3.iso V V AUSWAHL	
Abbildeigenschaft	
Standard-Windows-Installation	
Partitionsschema GPT	
Erweiterte Laufwerkseigenschaften einblenden	
Formatierungseinstellungen	
Laufwerksbezeichnung	
CES_X64FREV_DE-DE_DV9	
Dateisystem Größe der Zuordnungseinheit	
Large FAT32 (Standard) V 32 Kilobyte (Standard) V	
<ul> <li>Erweiterte Formatierungsoptionen ausblenden</li> </ul>	
Schnellformatierung	
Erweiterte Bezeichnung und Symbole erstellen	
Auf defekte Blöcke prüfen 1 Durchgang ~	
Status	
FERTIG	
Verwende Abbild: evotinglaptop_v0.3.iso	
Windows User Experience	Do not let Rufus do any
Customize Windows installation?	adjustments to the Windows
Disable data collection (Skip privacy questions)	installation
Set a local account using the same name as this user's	
Set regional options using the same values as this user's	
OK Abbrechen	

### Apply the image to a computer

	er	I.
💰 Windows Setup		Boot the laptop from the USB stick by pressing either F9 for HP
Windows wird installiert		or F12 for Lenovo early in the boot process.
Status		
		The Windows Setup will then
		automatically start
Windows-Dateien werden kopiert	(0%)	
Dateien werden für die Installation v		
Features werden installiert		
Updates werden installiert		
Aktion wird abgeschlossen		
🔏 Windows Setup		After a while it'll reboot
Windows muss neu gestartet werden, um	i fortzufahren.	
Neustart in 7 Sekunden		
Administrator: C:\Windows\System32\Wi	indowsPowerShell\v1.0\powershell	and continue by installing
13.10.2022 - 15:50:26.42 - Insta	lling software	drivers, applications etc
	Pass	
	lesult 0	
13.10.2022 - 15:50:45.97 - Edg	,e	
Administrator: Windows PowerShell		When the computer is installing
13.10.2022 - 13:00:23.67	- Installing undates	updates, the USB stick can be
13.10.2022 - 13:00:23.80	NET 4.8	removed
13.10.2022 - 13:00:54.16	- Result 3010	
13.10.2022 - 13:00:54.17	- Windows Cumulati	ive
er PC > Windows (C:) > ProgramData >	5 ~	Log files about the setup are
	÷G	created in the directory
Name	Änderungsdatum	c:\programdata
A.E.T. Europe B.V	13.10.2022 15:51	
Microsoft	12 10 2022 15 54	
	13.10.2022 15:54	
Packages	13.10.2022 15:54	
Packages	13.10.2022 16:11	
regid.1991-06.com.microsoft	13.10.2022 16:11 13.10.2022 16:15	
regid.1991-06.com.microsoft	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14	
regid.1991-06.com.microsoft SoftwareDistribution ssh	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16	The hard drive will not be
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs Geräte und Laufwerke (2)	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16	The hard drive will not be immediately encrypted
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs Geräte und Laufwerke (2) Windows (C:)	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16 13.10.2022 16:16	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs V Geräte und Laufwerke (2)	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16 13.10.2022 16:16	
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs Geräte und Laufwerke (2) Windows (C:) 37.0 GB frei von 59.0 GB	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16 13.10.2022 16:16	
<ul> <li>regid.1991-06.com.microsoft</li> <li>SoftwareDistribution</li> <li>ssh</li> <li>USOPrivate</li> <li>USOShared</li> <li>drivers</li> <li>installs</li> <li>Geräte und Laufwerke (2)</li> <li>Windows (C:)</li> <li>37.0 GB frei von 59.0 GB</li> <li>Ceräte und Laufwerke (2)</li> </ul>	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16 13.10.2022 16:16	immediately encrypted
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs Ceräte und Laufwerke (2) Windows (C:) 37.0 GB frei von 59.0 GB	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16 13.10.2022 16:16	immediately encrypted After a few reboots however it'll be encrypted (if the laptop is
regid.1991-06.com.microsoft SoftwareDistribution ssh USOPrivate USOShared drivers installs Geräte und Laufwerke (2) Windows (C:) 37.0 GB frei von 59.0 GB Ceräte und Laufwerke (2)	13.10.2022 16:11 13.10.2022 16:15 07.12.2019 10:14 06.10.2021 15:28 07.12.2019 10:14 07.12.2019 10:14 13.10.2022 16:16 13.10.2022 16:16	immediately encrypted After a few reboots however it'll

### 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.



### 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.

	Downloads → IS	50			5 V			Download the German Windows
Nam	e	^			Date modified	Туре	Size	LTSC 2021 ISO from an official
_	e-de_windows_10			-	16.11.2021 20:25	Disc Image File	4'832'998 KB	Microsoft source, like the VLSC,
َوَّ S	W_DVD9_WIN_EN	T_LTSC_2021_6	54BIT_German_N	1LF_X22-84426.ISO	16.11.2021 20:25	Disc Image File	4'832'998 KB	the partner download portal or
								Visual Studio Downloads.
PS C:	\users\athman.bo	ukhaoua\Docum	ents\Kanton-Thu	urgau> .\verify-im	age.ps1 -Reference	ISO "C:\temp\thurga	u\de-de_windows_1	
Verif	erprise_ltsc_202: ying integrity o	f the referen		ageUSB d:_				Run the script with the parameter
Mour	ing reference IS( nted to drive F stem Volume Info							-ReferenceISO pointing to the
Resul	ts of the scan have ts of the scan have	ave been writ	ten to:			above ISO file, and -ImageUSB set		
0. (05			a feacture tune	encek.cov				to the USB drive that should be
								checked
				u <b>rgau≻ .\verify-im</b> ageUSB <b>d:</b> -Display		ISO "C:\temp\thurga	u\de-de_windows_1	Optionally, the parameter "-
Verif	ving integrity of ing reference IS	f the referen		igeoup ubispiny				
	nted to drive G torun.inf ok beca	ause original						DisplayPositiveResults" can be
	tounattend.xml ol							
D:\bo	otmgr ok because	original						used to show correctly checked
D:\bo D:\bo	otmgr ok because otmgr.efi ok beca tup.exe ok becau	original ause original se original						files in green
D:\bo D:\bo D:\se D:\se	otmgr ok because otmgr.efi ok beca tup.exe ok becau A	original ause original se original B	С	D	E	F G	Н	
D:\boo D:\boo D:\set D:\set	otmgr ok because otmgr.efi ok becaus tup.exe ok becaus A Info	original ause original se original B Reason	C Result	FileName	_	F G	Н	files in green
D: \boo D: \boo D: \set D: \set 1 2	otmgr ok because otmgr.efi ok because tup.exe ok becaus A Info 3378723CI	original ause original se original B Reason original	C Result ok	FileName D:\autorun	.inf	F G	H	files in green The script will output a detailed report in the "Documents"
D:\boo D:\boo D:\set D:\set	otmgr ok because otmgr.efi ok becaus tup.exe ok becaus A Info	original ause original <u>se original</u> B Reason original hash	C Result	FileName	.inf ttend.xml	F G	Н	files in green The script will output a detailed report in the "Documents" directory that shows check
D:\boo D:\boo D:\set 1 2 3	otmgr ok because otmgr.ef1 ok because up.exe ok becaus A Info 3378723CI E803F1314	original ause original B Reason original hash original	C Result ok ok	FileName D:\autorun D:\autouna	.inf ttend.xml	F G	Н	files in green The script will output a detailed report in the "Documents"
D:\bov D:\bov D:\set 1 2 3 4	A Info 3378723CI E803F1314 4EEAC11B	original ause original B Reason original hash original original	C Result ok ok ok	FileName D:\autorun D:\autouna D:\bootmg	.inf ttend.xml r r.efi	F G	H	files in green The script will output a detailed report in the "Documents" directory that shows check
D: \boo D: \boo D: \set D: \set D: \set D: \set D: \set D: \boo D: \set D: \boo D: \boo D: \set D: \boo D: \bo	A Info 3378723CI E803F131/ 4EEAC11B 96B7EE39/	original ause original B Reason original hash original original original	C Result ok ok ok ok ok	FileName D:\autorun D:\autorun D:\bootmgu D:\bootmgu D:\setup.ex	.inf ttend.xml r r.efi ke	F G		files in green The script will output a detailed report in the "Documents" directory that shows check
2:\boo 2:\boo 2:\see 1 2 3 4 5 6 7 8	A Info 3378723CI E803F131/ 4EEAC11B 9687EE39/ 30043368( A6FB0A49) 163271445	original ause original B Reason original hash original original original hash original	C Result ok ok ok ok ok failed ok	FileName D:\autorun D:\autouna D:\bootmg D:\bootmg D:\setup.ex D:\System \ D:\boot\bc	.inf ttend.xml r r.efi ke Volume Inform			files in green The script will output a detailed report in the "Documents" directory that shows check
D: \boo D: \boo D: \see 1 2 3 4 5 6 7 7 8 9	A Info 3378723CI E803F131/ 4EEAC11B 9687EE39/ 30043368( A6FB0A49) 163271445 CD2C00CE	eriginal aus eriginal e eriginal B Reason original hash original original hash original original original	C Result ok ok ok ok ok failed ok ok	FileName D:\autorun D:\autorun D:\bootmg D:\bootmg D:\setup.ex D:\System \ D:\boot\bo D:\boot\bo	.inf ttend.xml r r.efi ke Volume Inford d oot.sdi			files in green The script will output a detailed report in the "Documents" directory that shows check
D: \box D: \box D: \see 1 2 3 4 5 6 7 8 9 10	A Info 3378723Cl E803F131/ 4EEAC11B 96B7EE39/ 30043368( A6FB0A49) 163271445 CD2C00CE 2F9C2428;	original se original Be original Acason original hash original original original original original original original	C Result ok ok ok ok ok failed ok ok ok ok	FileName D:\autorun D:\autorun D:\bootmg; D:\bootmg; D:\setup.ex D:\System \ D:\boot\bo D:\boot\bo D:\boot\bo	inf ttend.xml r r.efi ke Volume Infor d ot.sdi otfix.bin			files in green The script will output a detailed report in the "Documents" directory that shows check
1 2: \box 0: \box 0: \sec 1 2 3 4 5 6 6 7 8 8 9 100 11	A Info 3378723CI E803F131/ 4EEAC11B 96B7EE39/ 30043368( A6FB0A49) 163271445 CD2C00CE 2F9C24282 55A47316/	original se original Be original Acason original hash original original original original original original original original	C Result ok ok ok ok ok failed ok ok ok ok ok	FileName D:\autorun D:\autorun D:\bootmg D:\bootmg D:\setup.ex D:\System \ D:\boot\bo D:\boot\bo D:\boot\bo D:\boot\bo	inf ttend.xml r r.efi te Volume Infor d ot.sdi otfix.bin otsect.exe			files in green The script will output a detailed report in the "Documents" directory that shows check
1 2 3 4 5 6 7 8 9 10 11 12	A Info 3378723Cl E803F131/ 4EEAC11B 96B7EE39/ 30043368( A6FB0A49) 163271445 CD2C00CE 2F9C2428;	original se original B Reason original hash original original original original original original original original original original	C Result ok ok ok ok ok failed ok ok ok ok	FileName D:\autorun D:\autorun D:\bootmg D:\bootmg D:\setup.ex D:\System \ D:\boot\bo D:\boot\bo D:\boot\bo D:\boot\bo	inf ttend.xml r r.efi ke Volume Inford d ot.sdi otfix.bin otsect.exe fsboot.com			files in green The script will output a detailed report in the "Documents" directory that shows check

### 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 wellknown 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-withgroup-policy

https://learn.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setupclasses-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/