Windows

Powershell setup scripts

Install modern PowerShell

Windows ships with `Windows PowerShell` which is stuck at v5.1, so install latest `PowerShell`

```
winget install --silent --id Microsoft.Powershell --source winget
```

Post-install script

Dead Windows:

```
# W10 22H2
# Take Cortana off the taskbar
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v ShowCortanaButton
/t REG_DWORD /d 0 /f
# Hide People button
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\People /v PeopleBand
/t REG_DWORD /d 0 /f
# Delete Windows Defender tray from startup
reg delete HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v SecurityHealth /f
# Disable Skype from startup
reg add "HKCU\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.SkypeApp_k
zf8qxf38zg5c\SkypeStartup" /v State /t REG_DWORD /d 0 /f
# Do not hide tray items when they get cluttered
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer /v EnableAutoTray /t REG_DWORD
/d 0 /f
```

Windows 11 21H2 and later:

```
# W11 21H2
# Disable Teams+Edge from autostartup
# TODO
# Disable Widgets icon from Taskbar
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v TaskbarDa /t
REG_DWORD /d 0 /f
# Disable Chat icon from Taskbar
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v TaskbarMn /t
REG_DWORD /d 0 /f
# Align Taskbar to the left
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v TaskbarAl /t
REG_DWORD /d 0 /f

# W11 21H2 + W10 22H2
# Enable Hyper-V on Pro or Edu
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All -NoRestart
# Ignore CPU freshness check and downgrade minimum TPM version from 2.0 to 1.2 for upgrades
reg add HKLM\SYSTEM\Setup\MoSetup /v AllowUpgradesWithUnsupportedTPMOrCPU /t REG_DWORD /d 1 /f
# Disable Automatic Install of Suggested Apps
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager /v
SilentInstalledAppsEnabled /t REG_DWORD /d 0 /f
# Disable App Suggestions in Start menu
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager /v
SystemPaneSuggestionsEnabled /t REG_DWORD /d 0 /f
# Disable popup "tips" about Windows
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager /v
SoftLandingEnabled /t REG_DWORD /d 0 /f
# Disable Windows Welcome Experience
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager /v
SubscribedContent-310093Enabled /t REG_DWORD /d 0 /f
# Disable xbox game DVR capture
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\GameDVR /v AppCaptureEnabled /t
REG_DWORD /d 0 /f
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\GameDVR /v HistoricalCaptureEnabled /t
REG_DWORD /d 0 /f
# Show file extensions
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v HideFileExt /t
```

```
REG_DWORD /d 0 /f
# Opening explorer opens in THIS PC rather than RECENT FILES
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v LaunchTo /t
REG_DWORD /d 1 /f
# Take Search off the taskbar
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Search /v SearchboxTaskbarMode /t
REG_DWORD /d 0 /f
# Hide Task View button
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v ShowTaskViewButton
/t REG_DWORD /d 0 /f
# Show hidden files
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Hidden /t
REG_DWORD /d 1 /f
# Show hidden system files
#reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v ShowSuperHidden
/t REG_DWORD /d 1 /f
# Disable lock screen window when using password, saving one extra click
reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization /v NoLockScreen /t REG_DWORD
/d 1 /f
# Enable Dark Mode for apps
reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize /v AppsUseLightTheme
/t REG_DWORD /d 0 /f
# Enable Dark Mode for system
reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize /v
SystemUsesLightTheme /t REG_DWORD /d 0 /f
# Disable new context menu, always show the old one
reg.exe add 'HKCU\Software\Classes\CLSID\{86ca1aa0-34aa-4e8b-a509-
50c905bae2a2}\InprocServer32' /f /ve
# To revert the above:
#reg.exe delete "HKCU\Software\Classes\CLSID\{86ca1aa0-34aa-4e8b-a509-50c905bae2a2}" /f
# Disable UAC prompts
reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t
REG_DWORD /d 0 /f
# TODO also disable the UAC service that fails to start and spams eventviewer
# Disable pagefile (? does not look like it disables at a glance)
#reg add 'HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management' /v
ClearPageFileAtShutdown /t REG_DWORD /d 1 /f
# Delete OneDrive from startup
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v OneDrive /f
```

```
# Delete all taskbar shorcuts to get rid of Edge, Store and more
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband /v Favorites /f
# Disable hibernation to get rid of hiberfile.sys
#powercfg.exe -h off
# Kill and restart explorer.exe to apply most changes right now
taskkill /f /im explorer.exe
explorer.exe
# https://chocolatey.org/install
Set-ExecutionPolicy Bypass -Scope Process -Force;
[System.Net.ServicePointManager]::SecurityProtocol =
[System.Net.ServicePointManager]::SecurityProtocol -bor 3072; iex ((New-Object
System.Net.WebClient).DownloadString('https://community.chocolatey.org/install.ps1'))
# Reopen powershell

# Minimal install
choco install -y 7zip-zstd everything googlechrome hashcheck notepadplusplus nomacs smplayer
ventoy windirstat vcredist-all
# Remove Chrome from DB, it has its own autoupdater
choco uninstall -n --skipautouninstaller googlechrome
# Further Bloat
choco install -y crystaldiskmark crystaldiskinfo hwinfo mumble keepassxc libreoffice-fresh
sharex telegram vscode qbittorrent
```

Activate Windows

First install vlmcsd and OpenVPN's tap driver for a 10.10.10.10 tunnel, as Windows will refuse to authenticate against a KMS server running on localhost

```
# Open Powershell as admin
choco install -y tapwindows
# https://github.com/Wind4/vlmcsd/releases/latest
# Download the vlmcsd binaries archive and extract binaries/binaries/Windows/intel/vlmcsd-
Windows-x64.exe to C:\install\vlmcsd.exe
New-Item -ItemType Directory -Force -Path C:\install
Invoke-WebRequest -Uri https://cloud.rys.rs/s/H3WeZ37ntKxGZ2s/download -OutFile
C:\install\vlmcsd.exe
# Install the service
C:\install\vlmcsd.exe -s -U /n -O .
```

```
netsh advfirewall firewall add rule name="vlmcsd" dir=in action=allow
program=C:\install\vlmcsd.exe enable=yes
# Start the service (it's enabled, reboot would also start it)
net start vlmcsd


# https://docs.microsoft.com/en-us/windows-server/get-started/kmsclientkeys
# https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-edition-
upgrades#upgrade-using-a-command-line-tool
# If you do not have Home(Core) installed, you can switch between different editions (not
Home)
# You can get a popup with available editions via 'slmgr /dlv all'.
# Get just the editions by copypasting the box and running 'grep Name boxtext.txt | sort |
uniq'
# Note: Windows 11 KMS keys seem to match W10 ones

# Switch edition to Edu
Cscript.exe c:\windows\system32\slmgr.vbs /ipk NW6C2-QMPVW-D7KKK-3GKT6-VCFB2

# W11 Edu
slmgr /ipk NW6C2-QMPVW-D7KKK-3GKT6-VCFB2
# Set KMS server to a LAN one
#slmgr /skms 192.168.1.40:1688
slmgr /skms 10.10.10.10:1688
# Force activation now
slmgr /ato
# You should get a box in a few seconds that the activation passed. You can see the license
info with
slmgr /dli
```

Activate Office

```
# Convert Retail to VL first if Office is Retail https://github.com/abbodi1406/C2R-R2V-
AIO/blob/master/C2R-R2V-AIO.cmd

# https://docs.microsoft.com/en-us/deployoffice/vlactivation/gvlks
cd 'C:\Program Files\Microsoft Office\Office16'
```

```
# Office 2019 Pro Plus
#cscript ospp.vbs /inpkey:NMMKJ-6RK4F-KMJVX-8D9MJ-6MWKP
# Office 2021 Pro Plus
cscript ospp.vbs /inpkey:FXYTK-NJJ8C-GB6DW-3DYQT-6F7TH
cscript ospp.vbs /sethst:10.10.10.10
cscript ospp.vbs /act
```

Force W10 to W11 upgrade

```
# Source for some of these: https://github.com/pbatard/rufus/wiki/FAQ#do-you-plan-to-remove-other-windows-11-installation-restrictions
# Can also be done by doing SHIFT+F10 from an unmodified booted W11 installer -> regedit and adding the LabConfig values

## Upgrade W10 to W11 with at least TPM 1.2
# Ignore CPU freshness check and downgrade minimum TPM version from 2.0 to 1.2 for upgrades
reg add HKLM\SYSTEM\Setup\MoSetup /v AllowUpgradesWithUnsupportedTPMOrCPU /t REG_DWORD /d 1 /f

## Clean install W11 with possibly no TPM, <4GB RAM and on BIOS/UEFI with no Secure Boot
# Bypass TPM check in booted image
reg add HKLM\SYSTEM\Setup\LabConfig /v BypassTPMCheck /t REG_DWORD /d 1 /f
# Bypass 4GB+ RAM check in booted image
reg add HKLM\SYSTEM\Setup\LabConfig /v BypassRAMCheck /t REG_DWORD /d 1 /f
# Bypass SecureBoot check (UEFI check pretty much) in booted image
reg add HKLM\SYSTEM\Setup\LabConfig /v BypassSecureBootCheck /t REG_DWORD /d 1 /f
# Bypass Storage Check... is this even required?
reg add HKLM\SYSTEM\Setup\LabConfig /v BypassStorageCheck /t REG_DWORD /d 1 /f
```

Download

You can download .ISO of Windows 10 or Windows 11 versions directly from Microsoft's servers. Note that you'll have to spoof the user agent if you're on Windows, as you'll get redirected to the Media creator tool otherwise.

The ISOs provided by MS contain all the editions (sans enterprise pretty much), but you might have to add.../sources/ei.cfg file to show them all.

~~You can download older versions of windows and different versions of W10 through this method~~

If you want Enterprise, one way to get it is to install Pro/Edu and then switch the license, as per the powershell example above.

Links to various Microsoft images

Reboot into UEFI

Open admin cmd.exe and run:

```
shutdown /r /fw /t 0
```

Windows 11 Installation

Boot from the flash drive. Remember to always select "Custom" where applicable. You can skip creating a Microsoft account by trying to login with a nonexistent email.

Windows usually gets all the drivers itself, but if something doesn't work as it should you might need to visit your motherboard or device manufacturer's website and download drivers/update firmware.

Windows usually downloads an outdated GPU driver so head over to AMD's or Nvidia's website depending on what GPU you have.

If you already have or had a Windows license, then your hardware ID combination(should be motherboard+CPU) is stored on Microsoft's servers and your license will be obtained automatically when you connect to the internet, provided you installed the same Windows version.

If you don't have a W11 license you can either:

1. Buy a license key from official source. **Buying from unofficial sources/grey markets is exactly as illegal as cracking it. You'd be literally giving your money away to thieves. The keys are from hacked MSDN accounts, credit card frauds etc.**
2. If you're in college or some sort of academic institute, they might have MSDN licenses, see if you can find a copy from their IT department.
3. Not activate Windows - you will not be able to use Personalization features and it'll nag you

4. Activate Windows with KMSpico. Defender will complain about it, allow it manually in Defender after installing it. Alternatively you can use vlmcsd if you want an open source, more hardcore solution.

Upgrade from Home edition

Use a generic key - W10 or W11 - to upgrade to the needed edition.

```
# W10/W11 Edu
changepk.exe /ProductKey YNMGQ-8RYV3-4PGQ3-C8XTP-7CFBY
```

This is not a valid key for activation, it only allows for the upgrade.

Setting up OpenSSH

Due to this, to connect to an admin user, one needs to use

```
C:\ProgramData\ssh\administrators_authorized_keys
```

instead of

```
~/.ssh/authorized_keys
```

```
$PSDefaultParameterValues['Out-File:Encoding'] = 'utf8'
echo 'ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPR3/QA/+Kq1txg/APGQcpa3UradYnaaxSomDQamFDpH' >
'C:\ProgramData\ssh\administrators_authorized_keys'
# Check that the resulting file is(file is not preinstalled):
#   Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
# And not this or anything else:
#   Unicode text, UTF-16, little-endian text, with CRLF line terminators
file 'C:\ProgramData\ssh\administrators_authorized_keys'
```

To use sshd, first install it via Optional Features as per the docs;

To start it, run services.msc and configure OpenSSH Server to start Automatic and also Start it.

Disable password authentication in the config and then restart the server to apply it. Optionally also disable forcing the key path for admins.

```
C:\ProgramData\ssh\sshd_config
```

If you can't connect to an admin account and you kept the forced key path, permissions are probably wrong, run the following to set them correctly

```
icacls C:\ProgramData\ssh\administrators_authorized_keys /remove "NT AUTHORITY\Authenticated Users"
icacls C:\ProgramData\ssh\administrators_authorized_keys /inheritance:r
get-acl C:\ProgramData\ssh\ssh_host_dsa_key | set-acl C:\ProgramData\ssh\administrators_authorized_keys
```

VM setup

Install spice-guest-tools on KVM with Spice for better experience.

Revision #51
Created 2021-06-29 11:05:19 UTC by C0rn3j
Updated 2024-12-22 15:54:25 UTC by C0rn3j