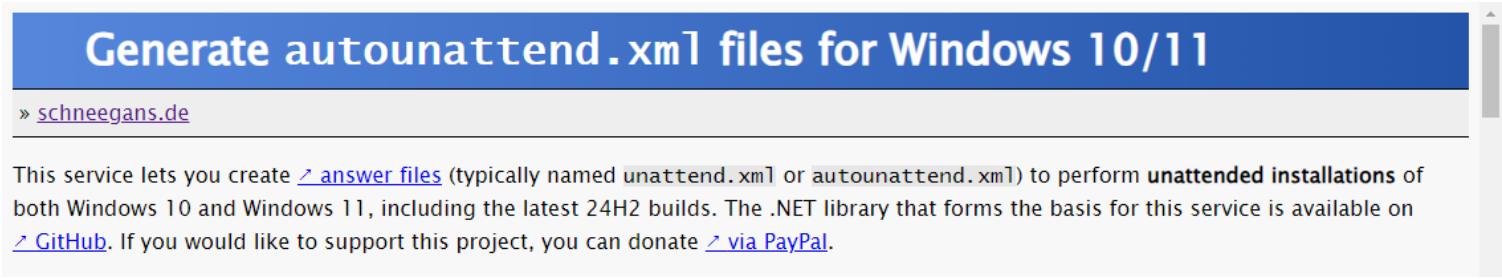
Generate autounattend installation for Windows 10/11

Creating an unattended installation file for Windows 10/11 using the service at schneegans.de involves several steps.

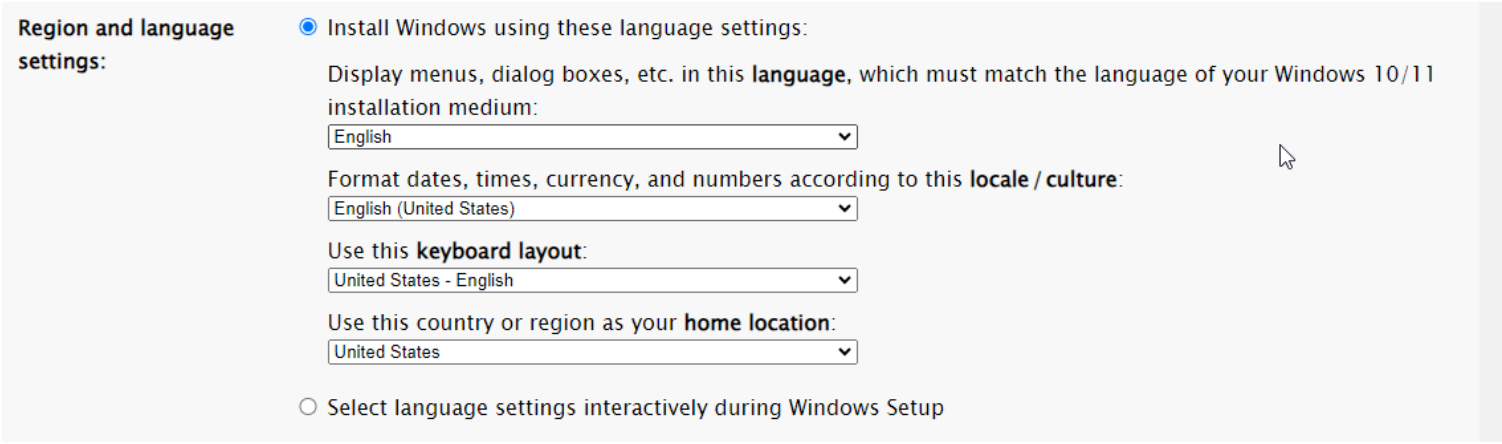
Step 1: Open the Website

Go to https://schneegans.de/windows/unattend-generator/



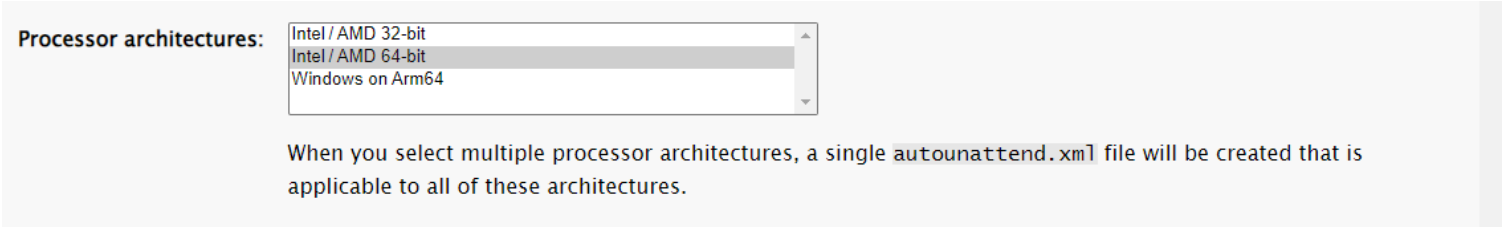
Step 2: Configure Region and Language Settings

Display Language: Select the language you want Windows to use for menus and dialog boxes.
Locale: Choose the locale for formatting dates, times, and currency.
Keyboard Layout: Select the desired keyboard layout.
Home Location: Choose the country or region.



Step 3: Select Processor Architecture

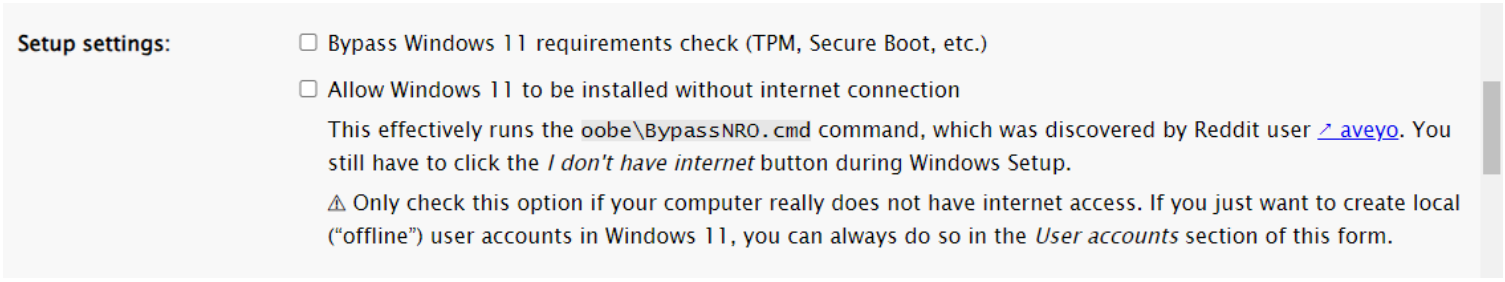
Choose the processor architecture(s) you need (e.g., Intel/AMD 64-bit).



Step 4: Setup Settings

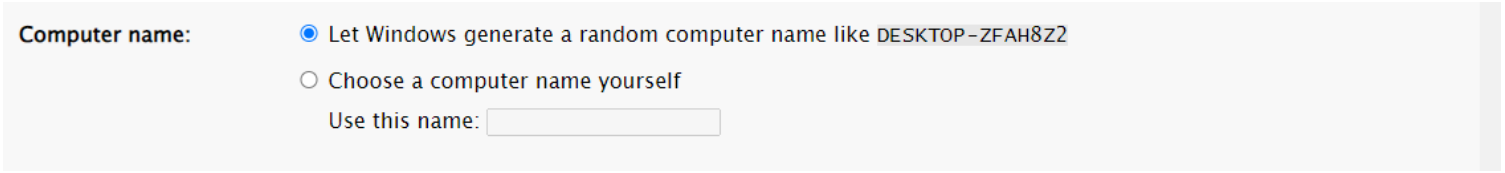
Bypass Windows 11 Requirements Check: Check this box if you need to bypass TPM and Secure Boot requirements.

Allow Windows 11 Installation Without Internet: Check this if your computer won't have internet access during setup.



Step 5: Configure Computer Name

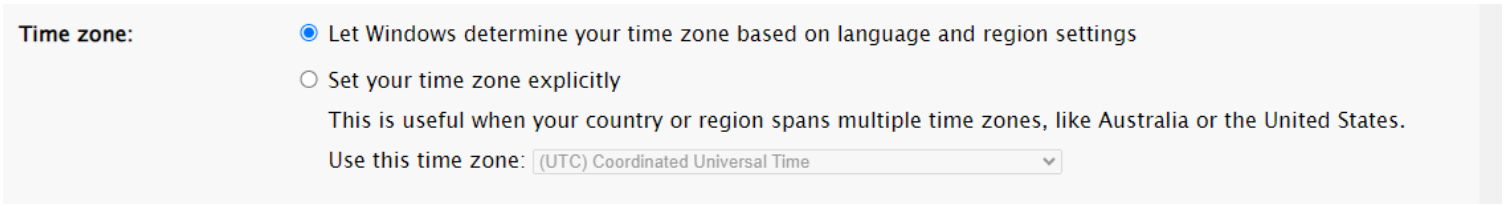
Choose whether to let Windows generate a random computer name or specify a custom name.



Step 6: Set Time Zone

Decide whether to let Windows determine the time zone or set it explicitly.

If explicit, choose the time zone from the dropdown.



Step 7: Partitioning and Formatting

Partition the disk interactively during Windows Setup: This option allows you to partition the disk manually during the Windows setup process.

Let Windows Setup wipe, partition and format your hard drive: *Choose this option to automate the process using predefined settings.*

Partition Layout:

GPT (GUID Partition Table): Select this if you are using a UEFI-based system. Set the size of the EFI System Partition (ESP) to 300 MB.

MBR (Master Boot Record): Select this if you are using a legacy BIOS system.

Windows RE (Recovery Environment) Installation:

Install on recovery partition: Create a separate partition for Windows RE with a size of 1000 MB.

Install on Windows partition: Install Windows RE in the C:\Recovery folder without creating a separate recovery partition.

Remove Windows RE: Delete the C:\Recovery folder, freeing up about 600 MB of disk space.

Custom Diskpart Script:

Use a custom script to configure your disk(s). Example:

```
SELECT DISK=0
CLEAN
CONVERT GPT
CREATE PARTITION EFI SIZE=300
FORMAT QUICK FS=FAT32 LABEL="System"
CREATE PARTITION MSR SIZE=16
CREATE PARTITION PRIMARY
SHRINK MINIMUM=1000
FORMAT QUICK FS=NTFS LABEL="Windows"
CREATE PARTITION PRIMARY
FORMAT QUICK FS=NTFS LABEL="Recovery"
SET ID="de94bba4-06d1-4d40-a16a-bfd50179d6ac"
GPT ATTRIBUTES=0x8000000000000001
```

Avoid drive letter assignments (e.g., ASSIGN LETTER=R) as these will not persist.

Choose Partition to Install Windows:

Install Windows to the first available partition that has enough space and does not already contain an installation of Windows.

Install to another partition:

Specify the disk and partition:

Disk (0-based): 0

Partition (1-based): 3

Partitioning and formatting:

- (•) Partition the disk interactively during Windows Setup
- ( ) Let Windows Setup wipe, partition and format your hard drive (more specifically, disk 0) using these settings:

Choose partition layout

- (•) GPT

  The ↗ GPT partition layout must be used for UEFI systems. Set the size of the EFI System Partition (ESP) to 300 MB.
- ( ) MBR

  MBR The ↗ MBR-based partition layout must be used for legacy BIOS systems.

Choose how to install Windows RE

- (•) Install on recovery partition

  Create a separate partition with a size of 1000 MB and install Windows RE to it.
- ( ) Install on Windows partition

  This will install Windows RE in `C:\Recovery`. No recovery partition will be created.
- ( ) Remove Windows RE

  This will delete the `C:\Recovery` folder and thus free about 600 MB of disk space. No recovery partition will be created.

Windows 24H2 BETA seems to ignore this setting and will always create a recovery partition with a minimum size of 600 MB.

- ( ) Use a custom `diskpart` script to configure your disk(s):

```
SELECT DISK=0
CLEAN
CONVERT GPT
CREATE PARTITION EFI SIZE=300
FORMAT QUICK FS=FAT32 LABEL="System"
CREATE PARTITION MSR SIZE=16
CREATE PARTITION PRIMARY
SHRINK MINIMUM=1000
FORMAT QUICK FS=NTFS LABEL="Windows"
CREATE PARTITION PRIMARY
FORMAT QUICK FS=NTFS LABEL="Recovery"
SET ID="de94bba4-06d1-4d40-a16a-bfd50179d6ac"
GPT ATTRIBUTES=0x8000000000000001
```

⚠ Avoid drive letter assignments (e.g. `ASSIGN LETTER=R`) in your script as these will not persist.

Choose partition to install Windows to after script has run

- (•) Install Windows to the first available partition that has enough space and does not already contain an installation of Windows
- ( ) Install to another partition:

  Disk (0-based): 0

  Partition (1-based): 3

Step 8: Choose Windows Edition

Select whether to use a generic product key or enter your own.
Choose the edition of Windows you want to install.

Windows edition:

- (•) Use a **generic product key**

  Such a key can be used to install Windows, but will not activate it. You can change the product key later.

  Install this edition of Windows: Pro
- ( ) Enter your **own product key** during Windows Setup

  You can also enter your key in the `autounattend.xml` file. To do this, find the `<Key>00000-00000-00000-00000-00000</Key>` element and replace the text with your key. Also use this if you plan to install an **Enterprise** edition of Windows.

Step 9: Create User Accounts

Account Creation:

Account Name: The username for the local account.

Password: The password for the local account.

Group: The group membership for the account (e.g., Administrators, Users).

First Logon:

Logon to the first administrator account created above: *Windows will automatically log in to the first administrator account created during the setup.*

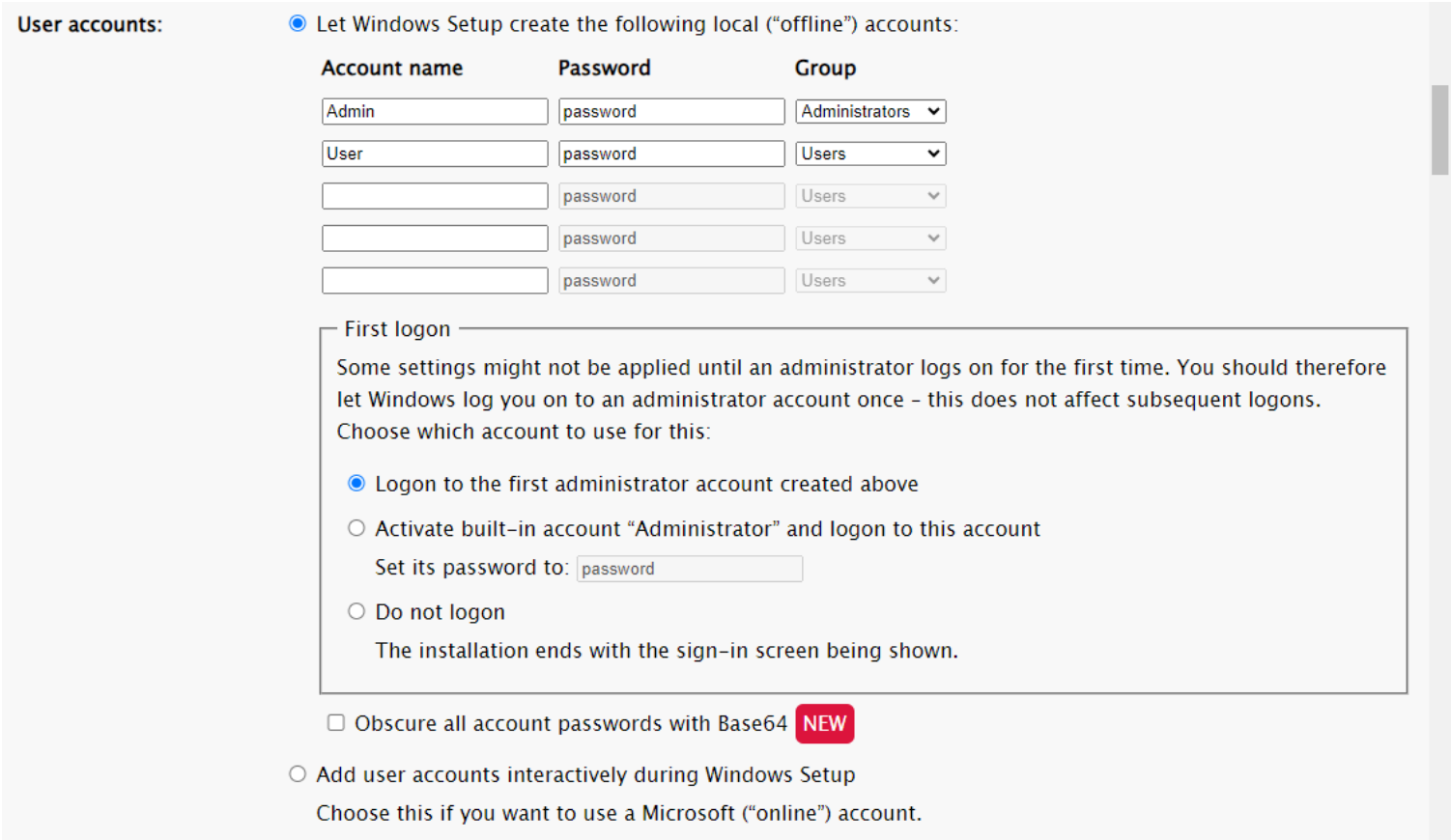
Activate built-in account "Administrator" and logon to this account: Enables and sets a password for the built-in Administrator account.

Do not logon: The installation will end at the sign-in screen.

Password Options:

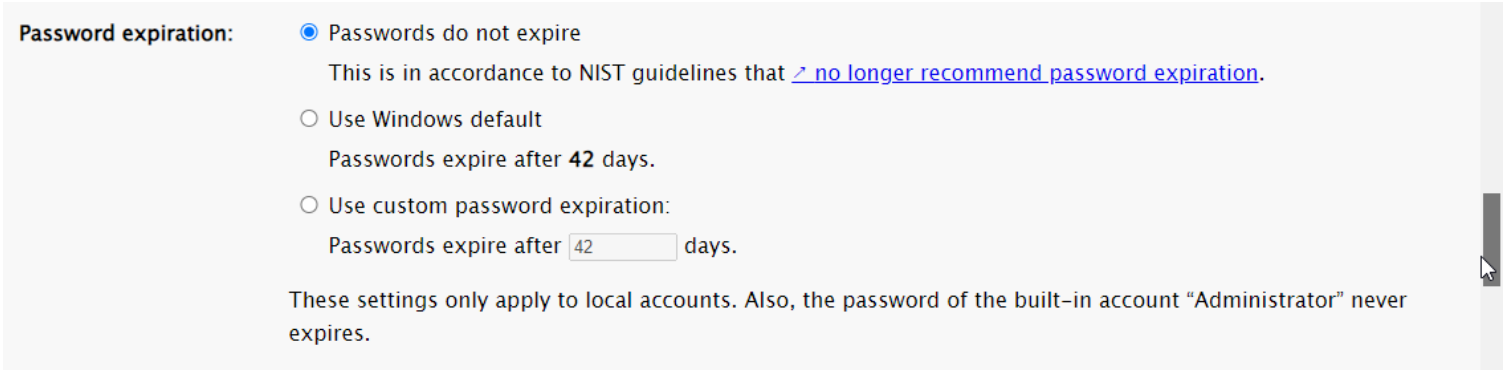
Obscure all account passwords with Base64: Passwords will be encoded in Base64 for added security.

Add user accounts interactively during Windows Setup: Allows adding accounts interactively if you plan to use Microsoft (online) accounts.



Step 10: Set Password and Account Policies

Configure password expiration settings.

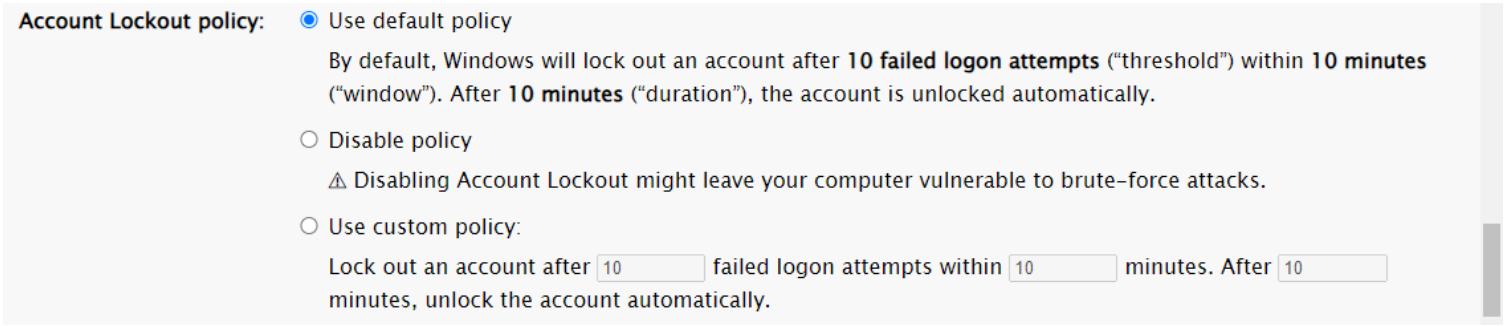


Step 11: Account Policies

Use Default Policy: Windows locks out an account after 10 failed logon attempts within 10 minutes. The account is automatically unlocked after 10 minutes.

Disable Policy: Disabling the Account Lockout policy can leave the computer vulnerable to brute-force attacks.

Use Custom Policy: Specify the number of failed logon attempts, the time window within which these attempts are counted, and the duration after which the account is automatically unlocked.



Step 12: Optimization Settings

Disable Windows Defender: Disables specific Windows Defender services during the Windows Setup process to streamline system performance.

Disable System Protection/System Restore: Prevents Windows from creating restore points on drive C:, conserving disk space.

Enable long paths: Enables programs like PowerShell and 7-Zip to utilize extended file paths up to 32,767 characters without additional prefixes.

Enable Remote Desktop services (RDP): Activates Remote Desktop Protocol services for remote system access.

Harden ACLs: *Removes write permissions for the Authenticated Users group on C:, preventing unauthorized creation of system folders.*

Allow execution of PowerShell script files: Sets PowerShell execution policies to 'RemoteSigned', permitting the execution of unsigned .ps1 script files.

Do not update Last Access Time stamp: Improves file system performance by disabling the update of last access timestamps using fsutil.exe.

Do not reboot with users signed in: Prevents Windows Update from automatically restarting the system while a user is signed in.

Turn off system sounds: *Changes the system sound scheme to 'No sounds', disabling all system sound notifications.*

Disable app suggestions: Modifies registry settings to prevent automatic downloading and installation of suggested applications.

Disable widgets: Hides the news and weather widget in the Windows 11 interface.

Prevent device encryption: Disables automatic activation of BitLocker encryption by Windows 11.

Audit process creation events: Logs each new process creation event in the Security log, aiding in system troubleshooting.

Optimizations:

- [ ] Disable Windows Defender

  This disables certain services (`Sense`, `WdBoot`, `WdFilter`, `WdNisDrv`, `WdNisSvc`, `WinDefend`) during Windows Setup. This method was adapted from an article by ↗ Rudy Mens.

  - [ ] Disable Windows Defender services early **BETA**

    Windows 11 24H2 does not permit to disable these services in the later stages of Setup. With this setting, they are disabled as early as possible, during the Windows PE stage.

- [ ] Disable System Protection / System Restore

  Windows will not create restore points for drive `C:` and thus use less disk space.

- [ ] Enable long paths

  This sets the ↗ LongPathsEnabled registry value, which enables several programs (including PowerShell, 7-Zip and TreeSize) to use long paths with up to 32,767 characters without resorting to the `\\?\` prefix.

- [ ] Enable Remote Desktop services (RDP)

- [ ] Harden ACLs

  This removes write permissions on `C:\` for the *Authenticated Users* group. In particular, this prevents unprivileged users from creating bogus folders such as `C:\Windows`.

- [ ] Allow execution of PowerShell script files

  This runs the command `Set-ExecutionPolicy -ExecutionPolicy 'RemoteSigned'`, which allows the execution of unsigned `.ps1` files.

- [ ] Do not update Last Access Time stamp

  This runs the command `fsutil.exe behavior set disableLastAccess 1`, which can improve file system performance.

- [ ] Do not reboot with users signed in

  This prevents Windows Update from ↗ rebooting when a user is signed in.

- [ ] Turn off system sounds

  This changes the sound scheme from *Windows Default* to *No sounds* for all users.

- [ ] Disable app suggestions

  This sets ↗ several registry values that prevent the silent download and installation of ↗ suggested apps.

- [ ] Disable widgets

  This hides the news and weather widget in the lower-left corner in Windows 11.

- [ ] Prevent device encryption

  Windows 11 would otherwise enable ↗ BitLocker encryption automatically.

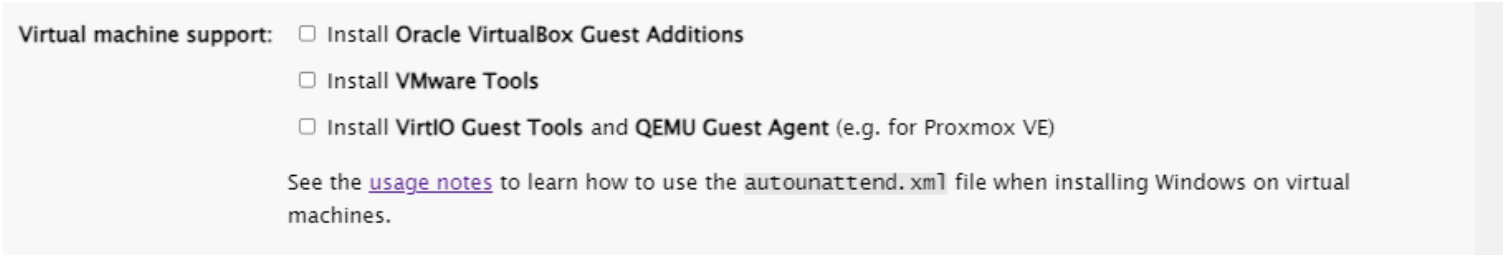
- [ ] Audit process creation events

  Each time a new process is created, Windows writes an event to the *Security* log. This is a powerful tool for troubleshooting.

  - [ ] Include command line in log events

Step 13: Virtual Machine Support

Choose whether to install VirtualBox Guest Additions, VMware Tools, or VirtIO Guest Tools. these instructions outline steps to enhance the functionality and integration of virtual machines on different virtualization platforms



Step 14: Wi-Fi Setup

Configure Wi-Fi settings or choose to skip Wi-Fi configuration.

Setup Options:

Interactive Wi-Fi Configuration during Windows Setup: Allows users to select and configure a Wi-Fi network directly during the Windows installation process.

Skip Wi-Fi Configuration: Recommended if a wired internet connection is available and preferred over Wi-Fi during initial setup.

Manual Wi-Fi Configuration using Provided Settings:

Enter the following details: Network name (SSID): Enter the name of your Wi-Fi network.

Connect even if not broadcasting: Check this if your Wi-Fi network doesn't broadcast its SSID.

Authentication: Choose the authentication method (Open, WPA2, WPA3).

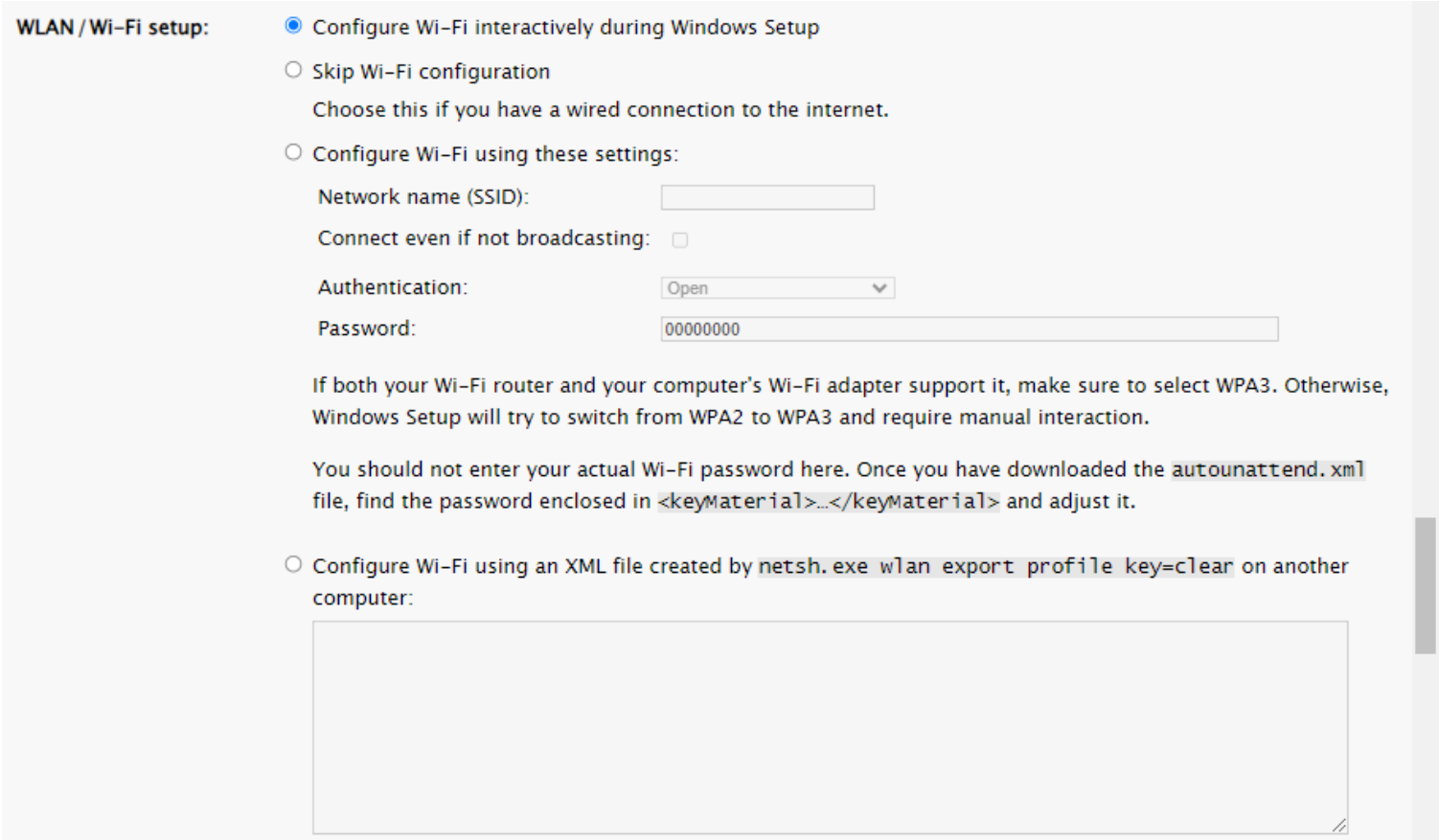
Password: Do not enter your actual Wi-Fi password here. Adjust it securely after obtaining the autounattend.xml file.

Advanced Configuration Options:

XML File Configuration using netsh.exe wlan export profile key=clear: Use an XML file exported from another computer to pre-configure Wi-Fi settings. Ensure security by adjusting the password enclosed in <keyMaterial>...</keyMaterial> post-download.

Important Notes: Avoid entering actual Wi-Fi passwords directly into setup files for security reasons.

Ensure compatibility between your Wi-Fi router and computer's Wi-Fi adapter regarding WPA3 support to prevent setup interruptions.

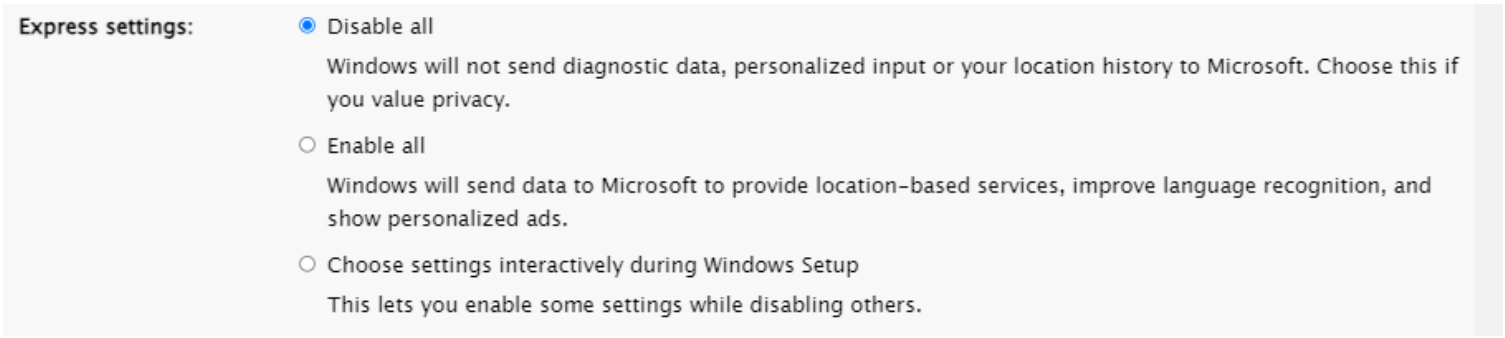


Step 15: Express Settings

Disable all: Windows will not send diagnostic data, personalized input, or location history to Microsoft. Choose this option if you prioritize privacy and do not want any data sent to Microsoft.

Enable all: Windows will send data to Microsoft to Provide location-based services, Improve language recognition, Show personalized ads. Choose this option if you want to utilize these features and are comfortable with data being sent to Microsoft.

Choose settings interactively during Windows Setup: Allows users to selectively enable or disable specific settings, Diagnostic data.



Step 16: Remove Bloatware

Windows includes several pre-installed apps that some users may not find necessary or useful. During Windows Setup, you can choose to remove these apps to streamline your system and free up space.

Apps Available for Removal:

3D Viewer	*Copilot*	Internet Explorer	Notepad (classic)	Outlook for Windows	PowerShell ISE	Sticky Notes	Windows Media Player (classic)
Bing Search	Cortana	Mail and Calendar	Notepad (modern)	Paint	Quick Assist	Teams	Windows Media Player (modern)
Calculator	Dev Home	Maps	Office 365	Paint 3D	*Skype*	Tips	Windows Terminal
Camera	*Family*	Math Input Panel	OneDrive	*People*	Snipping Tool	To Do	WordPad
Clipchamp	Feedback Hub	*Movies & TV*	OneNote	*Photos*	*Solitaire Collection*	Voice Recorder	*Xbox Apps*
Clock	Get Help	*News*	OpenSSH Client	Power Automate	Steps Recorder	Weather	Your Phone

Recommended Use: This feature works best with original Windows 10 and 11 .iso images downloaded directly from Microsoft.

Removing selected apps will delete all associated shortcuts, tiles, and pinned icons from the Start menu. This prevents accidental reinstallation of removed apps.

Remove bloatware: Windows comes with several apps that many users do not want or do not need. Check all the apps you want removed during Windows Setup:

Select all | Deselect all

- ☐ 3D Viewer
- ☐ Bing Search
- ☐ Calculator
- ☐ Camera
- ☐ Clipchamp
- ☐ Clock
- ☐ Copilot
- ☐ Cortana
- ☐ Dev Home
- ☐ Family
- ☐ Feedback Hub
- ☐ Get Help
- ☐ Internet Explorer
- ☐ Mail and Calendar
- ☐ Maps
- ☐ Math Input Panel
- ☐ Movies & TV
- ☐ News
- ☐ Notepad (classic)
- ☐ Notepad (modern)
- ☐ Office 365
- ☐ OneDrive
- ☐ OneNote
- ☐ OpenSSH Client
- ☐ Outlook for Windows
- ☐ Paint
- ☐ Paint 3D
- ☐ People
- ☐ Photos
- ☐ Power Automate
- ☐ PowerShell ISE
- ☐ Quick Assist
- ☐ Skype
- ☐ Snipping Tool
- ☐ Solitaire Collection
- ☐ Steps Recorder
- ☐ Sticky Notes
- ☐ Teams
- ☐ Tips
- ☐ To Do
- ☐ Voice Recorder
- ☐ Weather
- ☐ Windows Media Player (classic)
- ☐ Windows Media Player (modern)
- ☐ Windows Terminal
- ☐ WordPad
- ☐ Xbox Apps
- ☐ Your Phone

⚠ Bloatware removal works best with the original Windows ↗ 10 and ↗ 11 .iso images downloaded from Microsoft. I did not perform any tests with custom images.

⚠ If you select one or more apps to remove, *all* shortcuts, tiles and pinned icons in the start menu will be deleted, utilizing a technique ↗ demonstrated by Michael Niehaus. This is to prevent a user from accidentally reinstalling an app that has just been removed. The method to completely remove OneDrive was described by ↗ Stefan Kanthak, with whom I also collaborated to ↗ identify the registry keys that block the installation of *Dev Home* and *Outlook for Windows* on Windows 11 23H2.

Step 17: Run Custom Scripts

Windows Setup allows you to run custom scripts at various stages to automate tasks and configure system settings. This guide explains how to set up and use these scripts effectively.

1. Scripts to Run in the System Context (Before User Accounts are Created)

These scripts are executed before any user accounts are created, applying changes to the entire system.

- File Types: .cmd, .ps1, .reg, .vbs
- Purpose: Use these scripts to configure system-wide settings, such as disabling hibernation, modifying Windows Defender settings, or changing registry values for system features.

2. Scripts to Modify the Default User’s Registry Hive

These scripts affect the default user registry hive, influencing all new user accounts created after the setup:

- File Types: .reg, .cmd, .ps1
- Purpose: Configure default settings for new user accounts, such as hiding taskbar buttons or setting default application behaviors.

3. Scripts to Run When the First User Logs On

These scripts run when a user logs on for the first time, applying settings to their user profile:

- File Types: .cmd, .ps1, .reg, .vbs
- Purpose: Customize the user's environment, set default application settings, or display welcome messages.

4. Scripts to Run Whenever a User Logs On for the First Time

These scripts execute every time a user logs on for the first time, ensuring initial configurations are applied:

- File Types: .cmd, .ps1, .reg, .vbs
- Purpose: Apply user-specific configurations such as setting home locations, screen saver settings, or directory command options.

Run custom scripts:

Scripts to run in the system context, before user accounts are created

1. Run

```
powercfg.exe /HIBERNATE OFF
```

as a .cmd file.

2. Run

```
Set-MpPreference -DisableRealtimeMonitoring $true;
```

as a .ps1 file.

3. Run

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Remote Assistance]
"fAllowToGetHelp"=dword:00000000
```

as a .reg file.

4. Run

```
WScript.Echo "Hello!"
```

as a .vbs file.

Scripts to modify the default user's registry hive

This will automatically mount the `C:\Users\Default\NTUSER.DAT` hive, run your scripts and unmount the hive again. Your scripts will be run *before* user accounts are created – hence, they will affect all user accounts, including the built-in account "Administrator". You must access the keys in this hive as follows:

.reg `[HKEY_USERS\DefaultUser\…`

.cmd `HKU\DefaultUser\…`

.ps1 `Registry::HKU\DefaultUser\…`

1. Run

```
Windows Registry Editor Version 5.00

[HKEY_USERS\DefaultUser\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"ShowTaskViewButton"=dword:00000000
```

as a .reg file.

2. Run

```
reg.exe add "HKU\DefaultUser\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v "ShowTaskViewButton
```

as a .cmd file.

3. Run

```
Set-ItemProperty -LiteralPath "Registry::HKU\DefaultUser\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Adva
```

as a .ps1 file.

Scripts to run when the first user logs on

1. Run

```
setx.exe DIRCMD "/A /O:GN /C /N"
```

as a .cmd file.

2. Run

```
Set-WinHomeLocation -GeoId 94;
```

as a .ps1 file.

3. Run

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Control Panel\Desktop]
"ScreenSaverIsSecure"="1"
```

as a .reg file.

4. Run

```
WScript.Echo "Hello!"
```

as a .vbs file.

Scripts to run whenever a user logs on for the first time

1. Run

```
setx.exe DIRCMD "/A /O:GN /C /N"
```

as a .cmd file.

2. Run

```
Set-WinHomeLocation -GeoId 94;
```

as a .ps1 file.

3. Run

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Control Panel\Desktop]
"ScreenSaverIsSecure"="1"
```

as a .reg file.

4. Run

```
WScript.Echo "Hello!"
```

as a .vbs file.

Your scripts will be run as follows:

.cmd `cmd.exe /c "C:\Windows\Setup\Scripts\unattend-01.cmd >>"C:\Windows\Setup\Scripts\unattend-01.log" 2>&1"`

.ps1 `cmd.exe /c "powershell.exe -NoProfile -Command "Get-Content -LiteralPath 'C:\Windows\Setup\Scripts\unattend-02.ps1' -Raw | Invoke-Expression;" >>"C:\Windows\Setup\Scripts\unattend-02.log" 2>&1"`

.reg `cmd.exe /c "reg.exe import "C:\Windows\Setup\Scripts\unattend-03.reg" >>"C:\Windows\Setup\Scripts\unattend-03.log" 2>&1"`

.vbs `cmd.exe /c "cscript.exe //E:vbscript "C:\Windows\Setup\Scripts\unattend-04.vbs" >>"C:\Windows\Setup\Scripts\unattend-04.log" 2>&1"`

.js `cmd.exe /c "cscript.exe //E:jscript "C:\Windows\Setup\Scripts\unattend-05.js" >>"C:\Windows\Setup\Scripts\unattend-05.log" 2>&1"`

Step 18: Configure WDAC Policy

Windows Defender Application Control (WDAC) allows administrators to control which applications and drivers can run on their systems, enhancing security by preventing unauthorized or malicious software from executing.

Do Not Configure WDAC Policy: This option leaves WDAC disabled, and no application control policies are applied. Choose this if you do not wish to enforce any application restrictions.

Configure a Basic WDAC Policy Using These Settings:

Description: This option enables a predefined WDAC policy with the following rules:

Allowed Applications: Applications located in C:\Windows, C:\Program Files, and C:\Program Files (x86) directories are allowed to run.

Blocked Applications: Applications stored in other directories, especially known user-writable folders such as C:\Windows\Temp or C:\Windows\Debug\WIA, are blocked from running.

Disabling the Policy: To disable this WDAC policy later, delete the file located at C:\Windows\System32\CodeIntegrity\CiPolicies\Active\{d26bff32-33a2-48a3-b037-10357ee48427}.cip and reboot the system.

Enforcement Options:

Auditing Mode: This mode logs drivers and applications that would have been blocked by the policy without actually blocking them. It is useful for testing and refining policies before enforcing them.

Auditing Mode on Boot Failure: If a policy would prevent Windows from booting by blocking a critical system driver, this mode switches to audit mode during boot failures. Otherwise, it uses enforcement mode.

Enforcement Mode: This mode strictly enforces the WDAC policy, blocking drivers and applications unless they are explicitly allowed by the policy.

Script Enforcement Options:

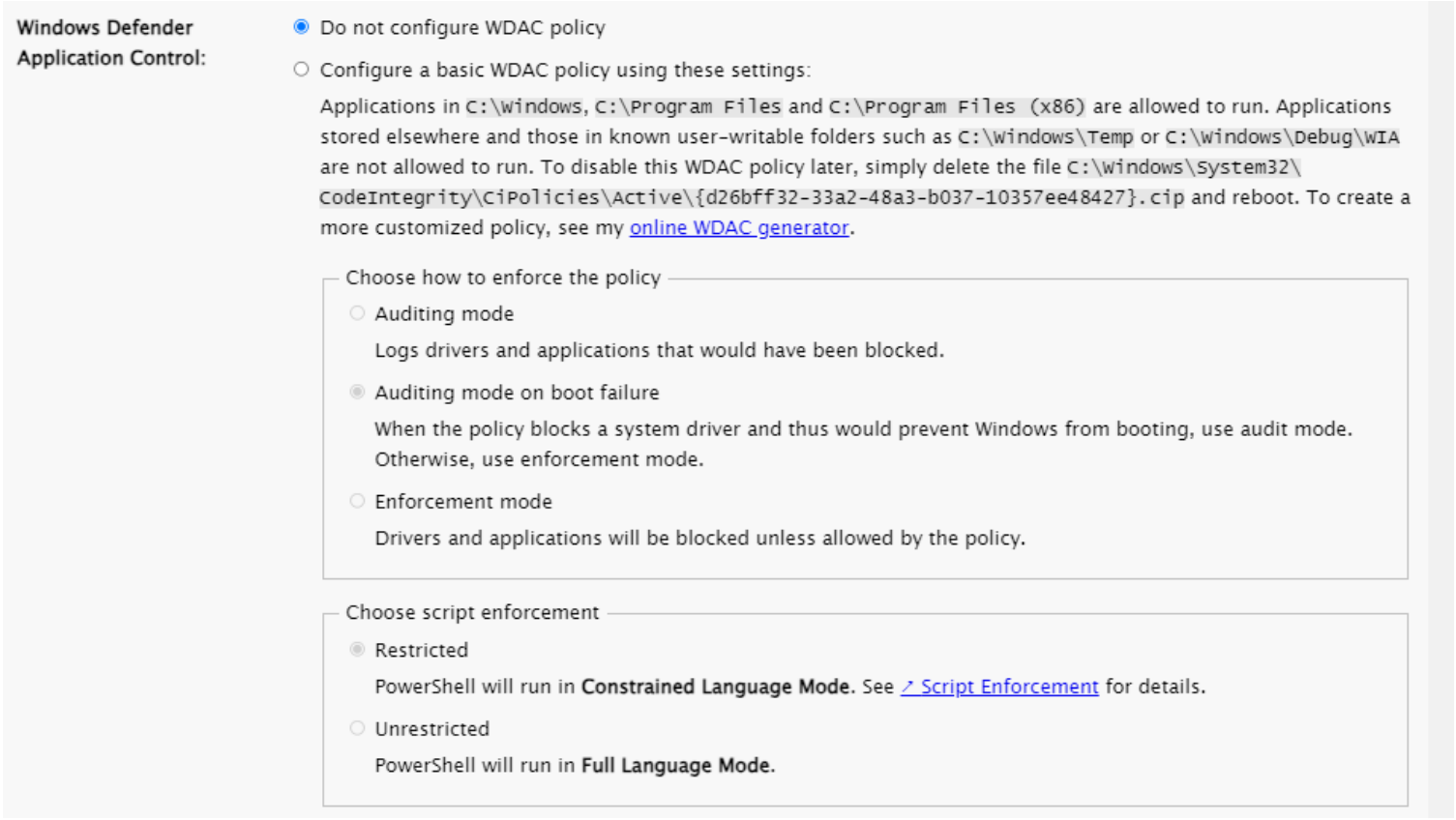
Restricted: PowerShell will run in Constrained Language Mode, restricting the execution of certain types of scripts and commands to increase security. See the Script Enforcement section for more details.

Unrestricted: PowerShell will run in Full Language Mode, allowing all types of scripts and commands to execute without restriction.

Additional Information:

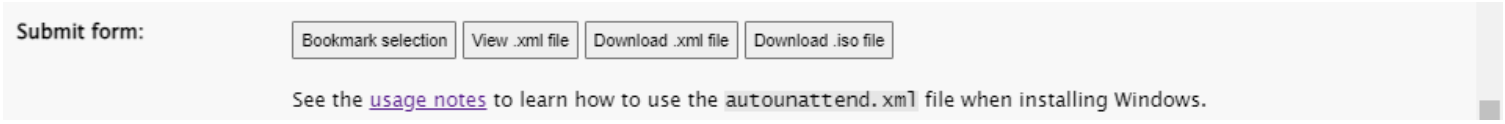
Custom Policies: For more advanced and customized policies, refer to the online WDAC policy generator tool.

Log Locations: The logs generated in auditing mode can be found in the Windows Event Viewer under Application and Services Logs -> Microsoft -> Windows -> CodeIntegrity -> Operational.



Step 19: Generate the autounattend.xml File

After configuring all settings, click the button to generate the autounattend.xml file.
Download the generated file.



Step 20: Use the autounattend.xml File

Place the autounattend.xml file on the root of your installation media (USB drive).
Boot from the installation media to start the unattended Windows setup.
By following these steps, you can create a custom unattended installation file for Windows 10 or Windows 11, tailored to your specific requirements.