Advantech Power Suite
User Manual

V2.1.0

Advantech Power Suite User Manual

1. Foreword

In Windows 10/11 IoT Enterprise LTSC, Microsoft provides many useful and helpful features for users, however, it's not intuitive to use these features. Therefore, Advantech developed Power Suite application, enabling users to access these features more quickly and easily.

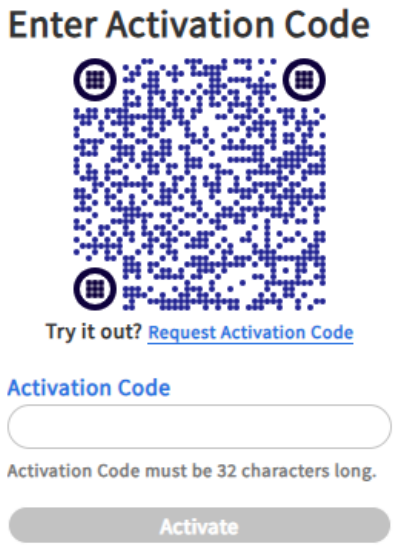
ADV Image Manager: In Windows, Microsoft offers a Backup and Restore function, but it requires multiple steps to complete the process. ADV Image Manager simplifies this by providing an easy way to back up and recover the computer system.

2. Requirements

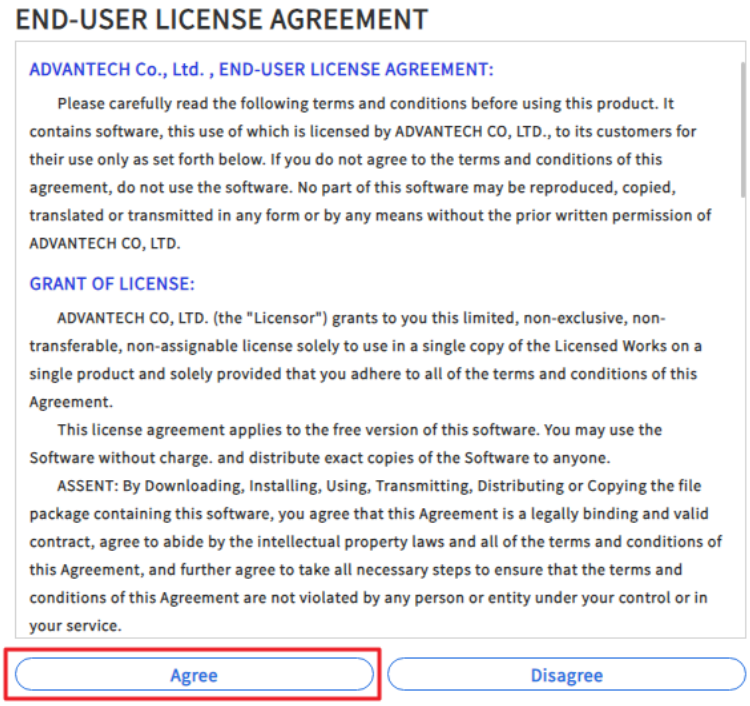
I. Windows 10/11 IoT Enterprise LTSC

II. The user account must have administrator privileges

III. If the device is not provided by Advantech, please fill-in information to get an activation code.



IV. The user must clicks "**Agree**" button to the END-USER License Agreement (EULA) when launching Advantech power suite application for the first time.



3. Limitations

After Sysprep, the setup of below items would be removed:

OS Enhancement Utility

- Notification Settings
- Hide Action Center
- Windows Settings: Hibernate
- Device Control
- Kiosk Mode

Lockdown Utility

- Automatic Logon
- Advanced Boot Option: Login Screen
- Ctrl + Alt + Del Screen Option: Lock/Sign Out/Change a Password/Task Manager

The following feature is only supported on Windows on ARM (WoA) devices:

OS Enhancement Utility

- Firmware Update

The following features are unsupported and have been blocked on Windows on ARM (WoA) devices:

OS Enhancement Utility

- System Settings: Touch, including Enable Touch and Enable Touch Gestures
- System Settings: Hibernate
- Windows Settings: Automatic Windows Update
- Kiosk Mode: Assigned Access (UWP)
- Energy: current BIOS power-saving settings

Lockdown Utility

- Unified Write Filter: HORM

Security Diagnosis

- The Security Diagnosis utility is unsupported and is removed on WoA devices

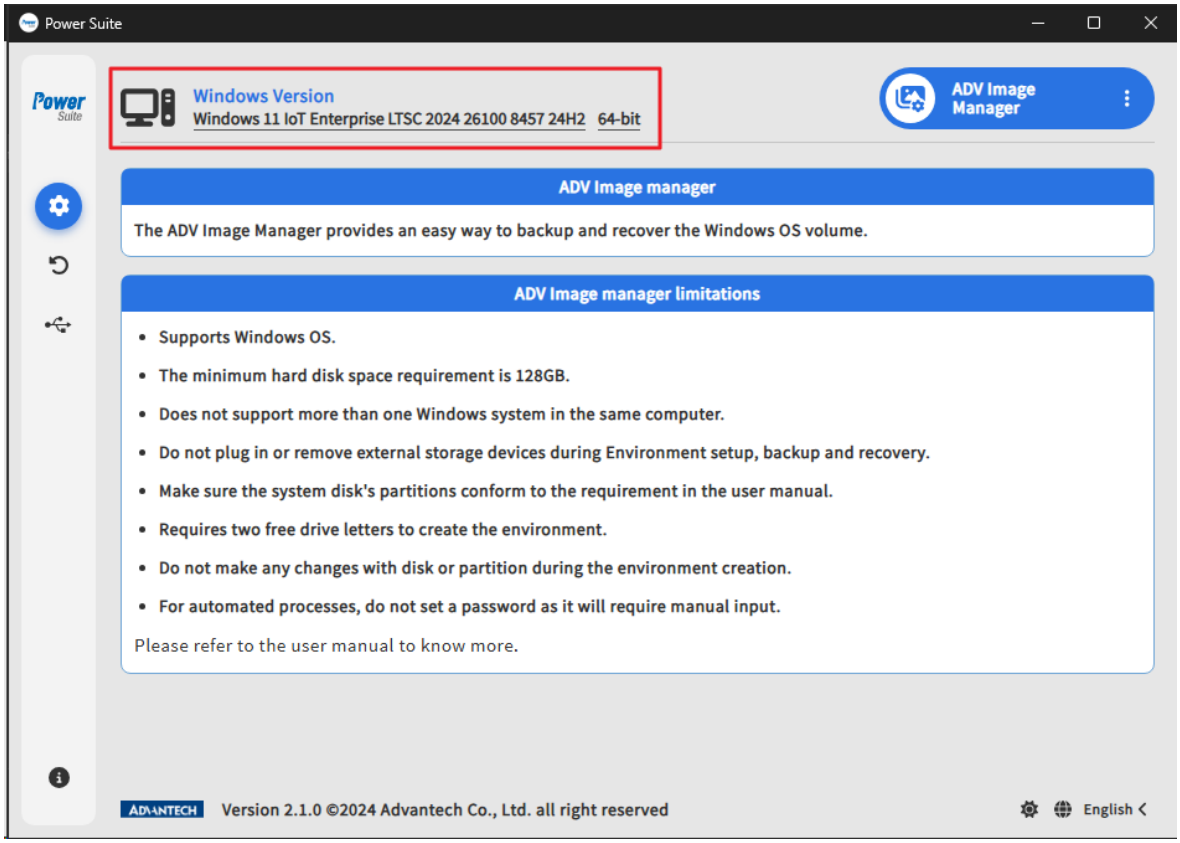
For ADV Image Manager:

I. Only supported on UEFI systems.
II. Supported on Windows 10 IoT Enterprise LTSC 2019, Windows 10 IoT Enterprise LTSC 2021, and Windows 11 IoT Enterprise LTSC 2024.
III. Only the C: partition will be backed up.
IV. Items in the Recycle Bin will not be included in the backup.
V. Multiple Windows systems on the same computer are not supported.
VI. Do not plug in or remove external storage devices during environment setup, backup, or recovery.
VII. Do not make any changes to disks or partitions during environment creation.
VIII. Please do not format C:, as it contains necessary driver files required for ADV Image Manager to start recovery.
IX. The number of partitions on the computer should not exceed 23.
X. The drive label “ADV Backup” must be reserved exclusively for ADV Image Manager.
XI. Two free drive letters are required to create the environment.
XII. The filter of the Unified Write Filter (UWF) feature must be disabled.
XIII. The defragmentation service (also known as “Optimize Drives” service) will be initiated during environment creation.
XIV. Ensure that the partitions on the system disk meet the requirements specified in Section 6.1 and that there is no unallocated space on the system disk.
XV. The Intel® Graphics Command Center may display an error after recovery.

4. General Functions

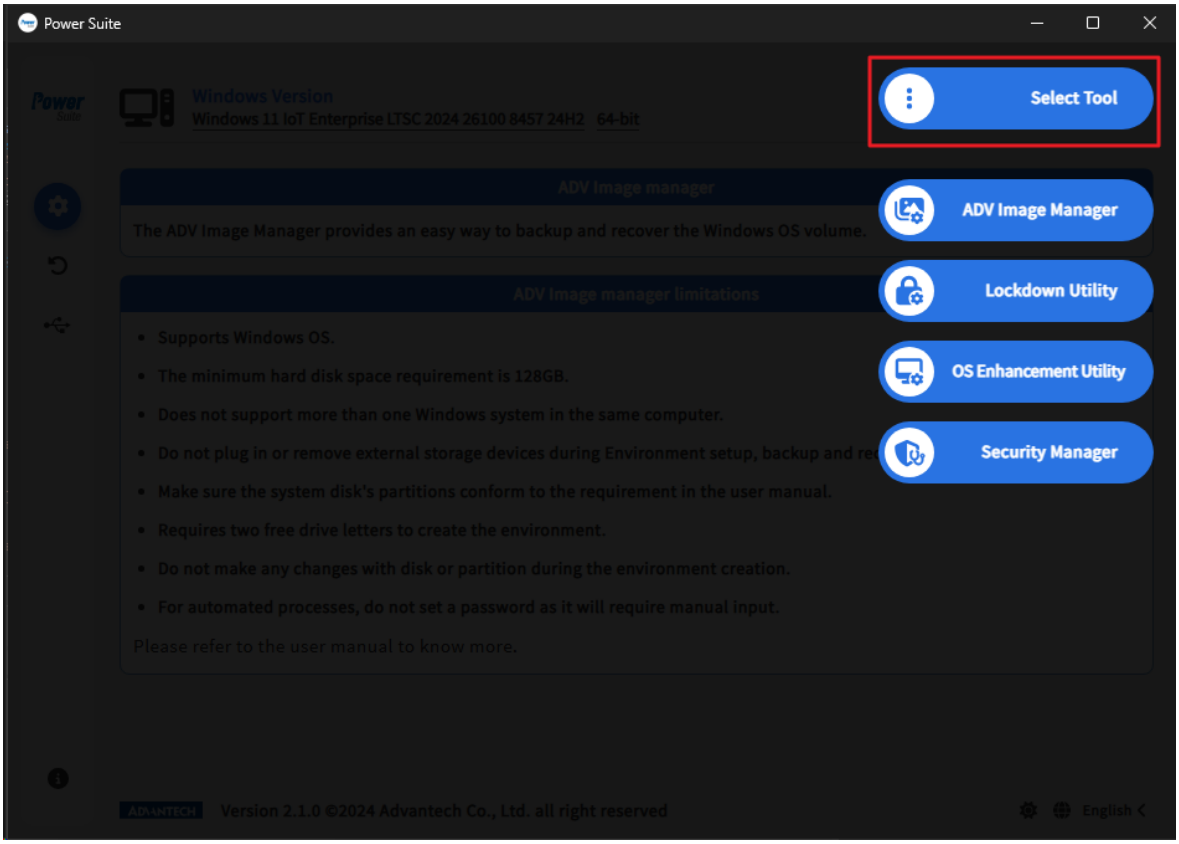
4.1 Windows Version

It shows Windows version, build numbers and architecture. Advantech Power Suite only supports OS build version newer than 17763.



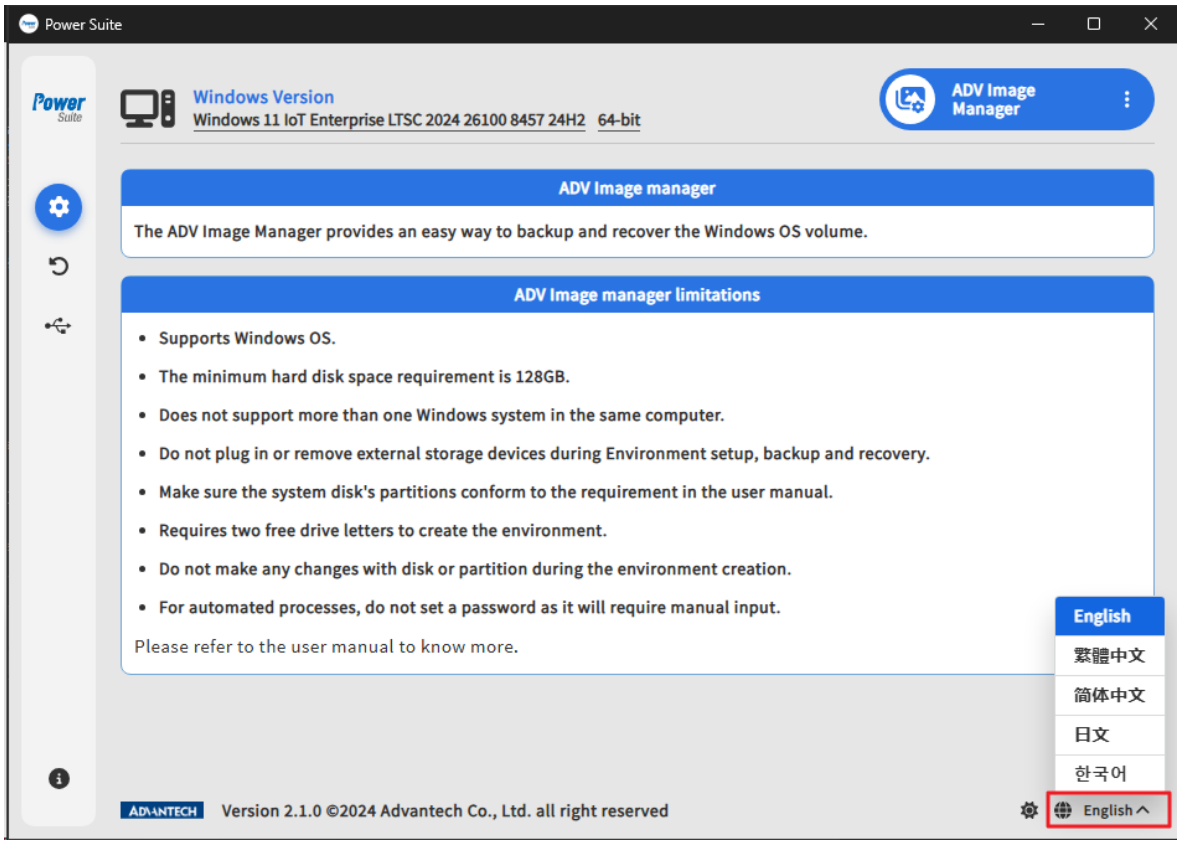
4.2 Select Tool/Utility

Four tools are available: ADV Image Manager, Lockdown Utility, OS Enhancement Utility, and Security Diagnosis.



4.3 Change Language

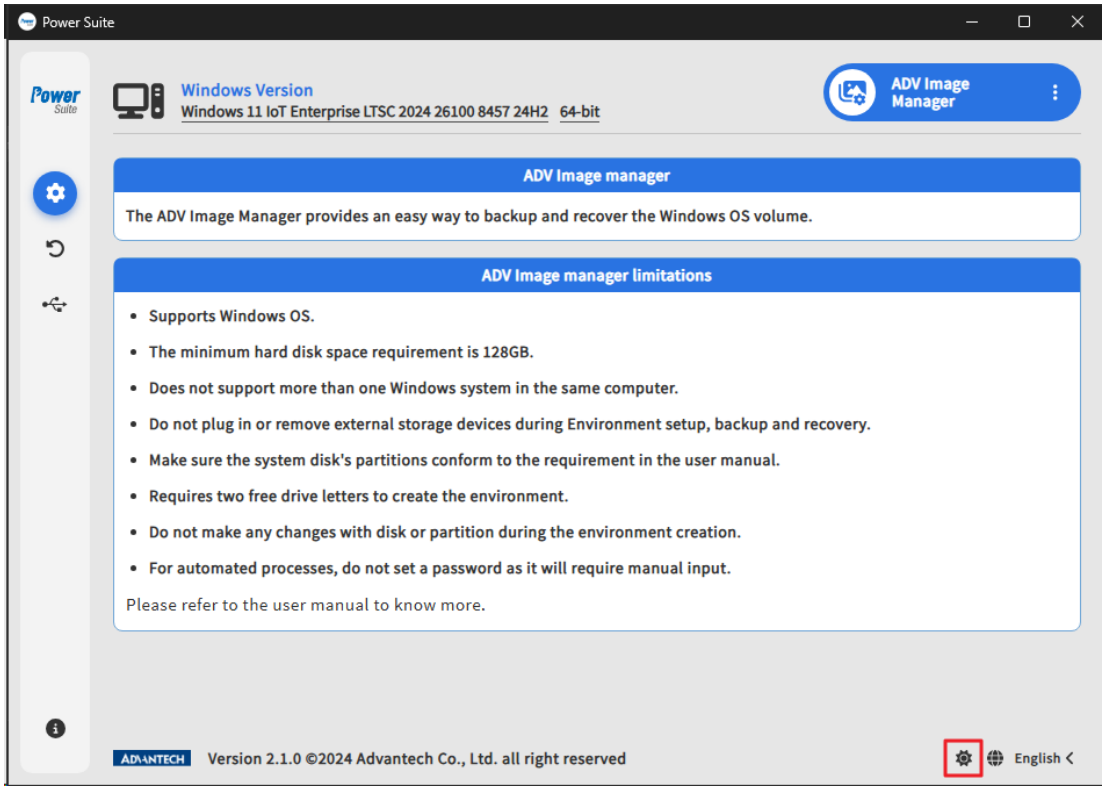
Change user interfaces of Advantech Power Suite based on the language selected by the user.

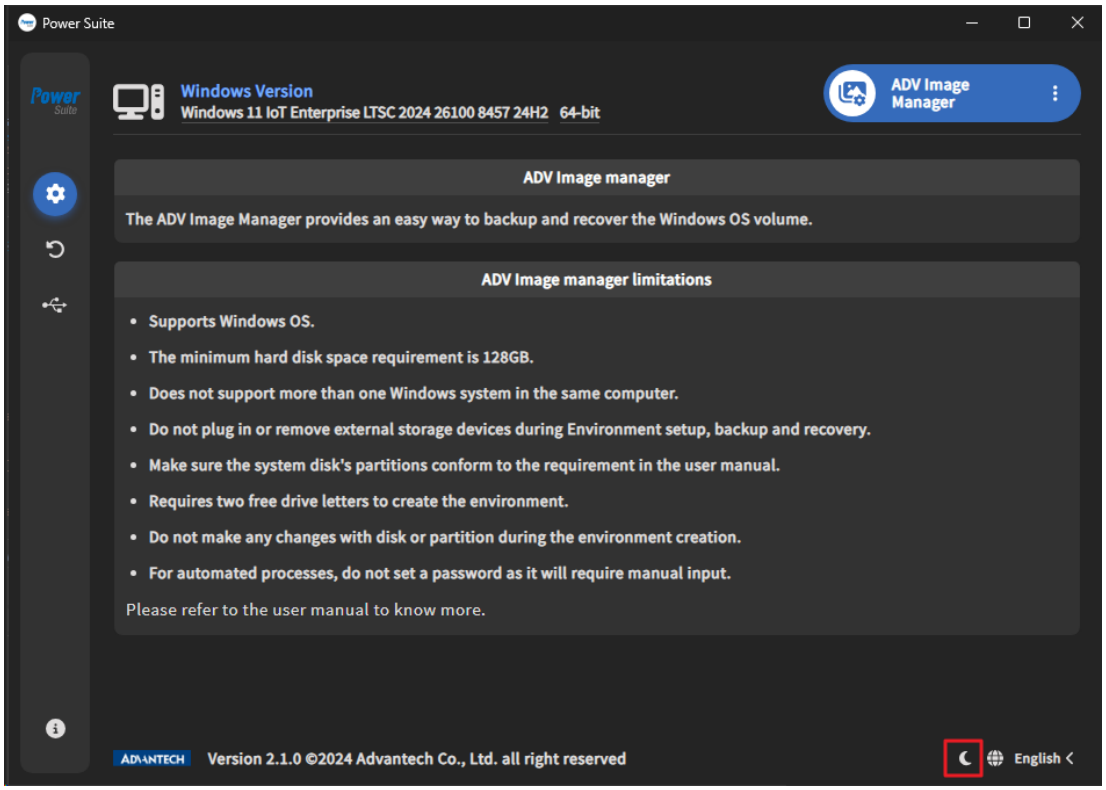


Note: Currently available in English, Traditional Chinese, Simplified Chinese, Japanese, and Korean.

4.4 Switch Dark/Light Modes

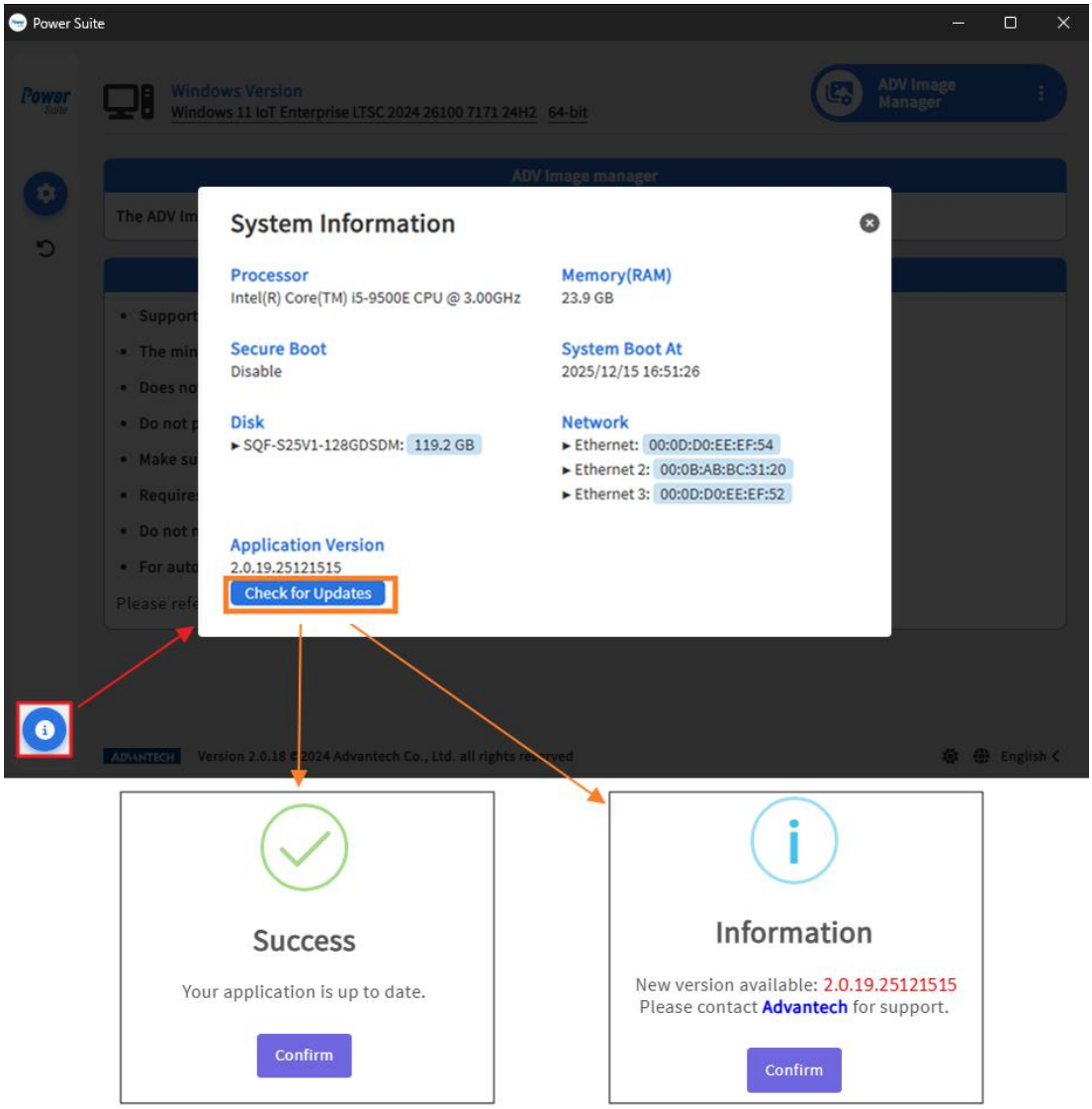
Users can switch between light (⚙) and dark (🌙) mode based on their preferences.





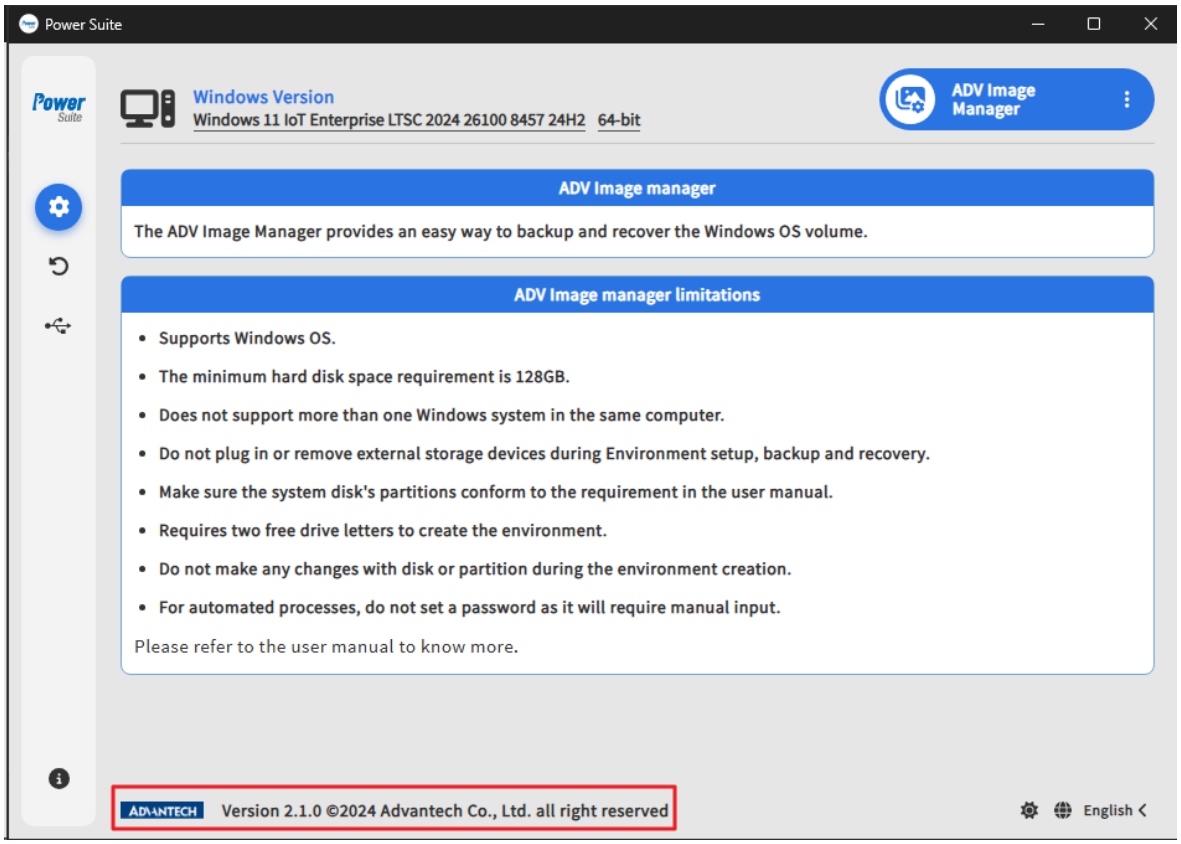
4.5 System Information

Display current system information and the application version. The user can click “Check for Updates” to see if a newer version is available.



4.6 Copyright Notice

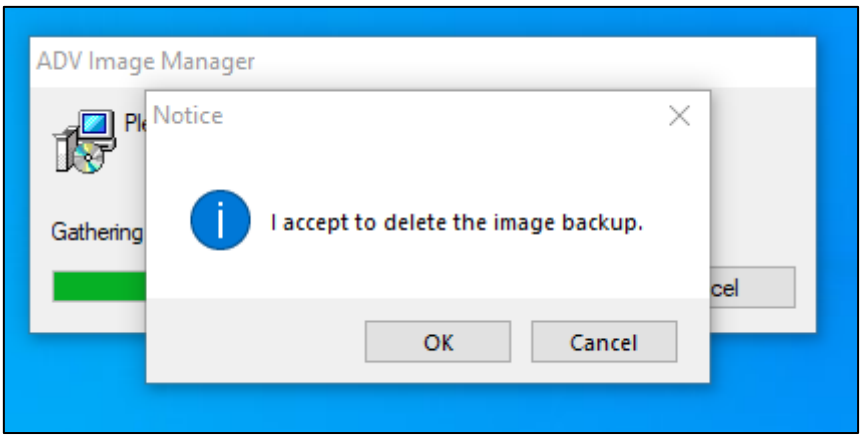
Copyright notice and software version of Advantech Power Suite.



4.7 Uninstall Advantech Power Suite

During the uninstallation of Advantech Power Suite, the “ADV Backup” partition will be deleted and the image backup will also be deleted.

Make sure you want to delete the image backup, then press “**OK**”. If not, please press “**Cancel**”. Uninstall will be canceled and nothing will be changed if “**Cancel**” is pressed.



5. Tools / Utilities

5.1 ADV Image Manager

5.1.1 Information

ADV Image Manager is a tool used to back up and recover computer systems. ADV Image Manager can perform backup and recovery from the desktop application. Additionally, when the computer fails to enter the Windows system, ADV Image Manager can be started from the EFI Shell to recover the system.

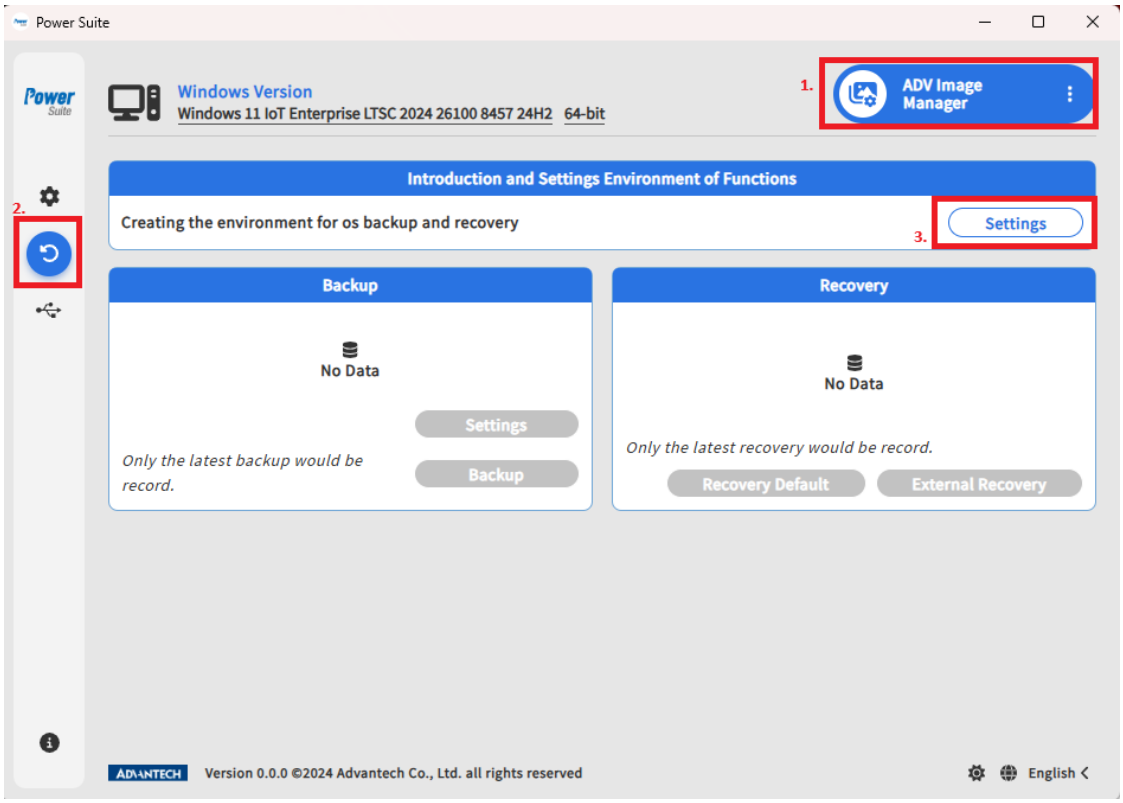
- **What does the Environment setup section do?**
  When the environment setup starts, ADV Image Manager will replace the built-in Windows RE (WinRE) with a new WinRE. Meanwhile, ADV Image Manager will create the “ADV Backup” partition on the system disk to store the backup image.

- **What does the Backup section do?**
  When the backup starts, the system will restart and boot into WinRE. In WinRE, ADV Image Manager will back up the C:\ partition. Please don’t close the command prompt and keep the system focused on the command prompt to run the backup. When the backup is finished, the system will automatically restart and boot into Windows. In Windows, open the ADV Image Manager application to check the backup result.

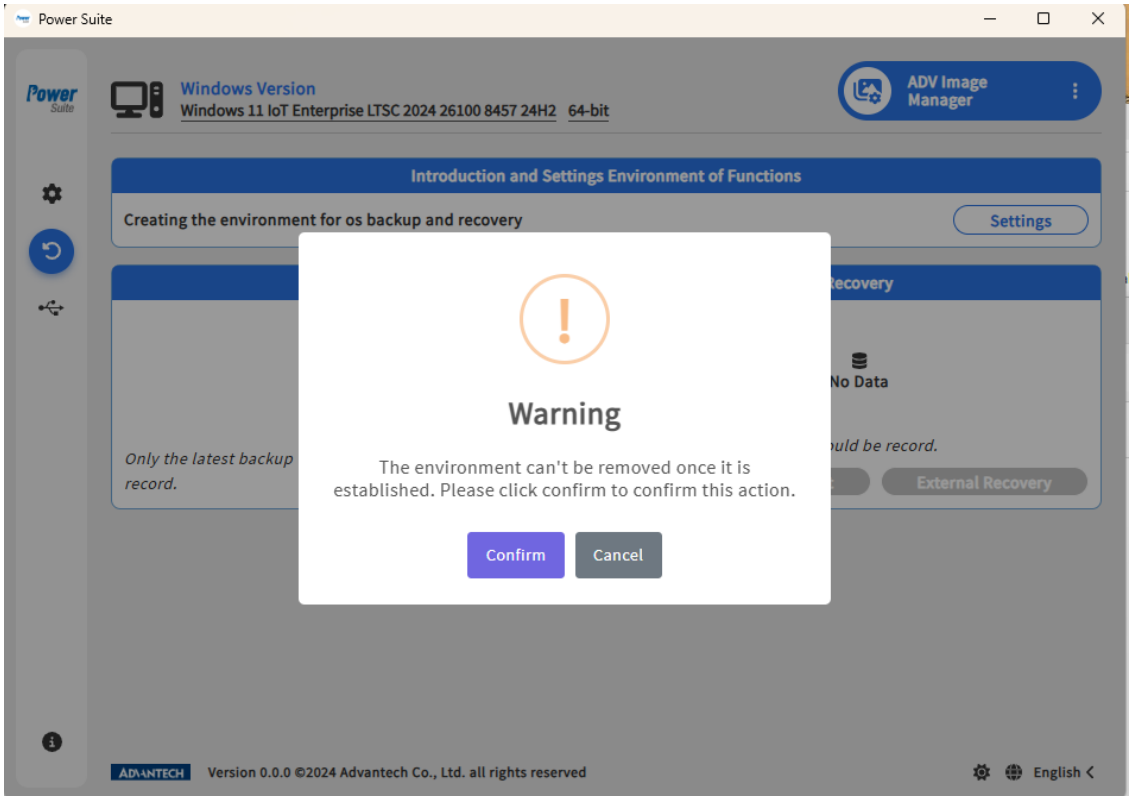
- **What does the Recovery section do?**
  When the recovery starts, the system will restart and boot into WinRE. In the WinRE, ADV Image Manager will recover the C:\ partition and the system partition. Please don’t close the command prompt and keep the system focused on the command prompt to run the recovery. When the recovery is finished, the system will automatically restart and boot into Windows. In Windows, open the ADV Image Manager application to check the recovery result.

5.1.2 Start to set up the environment

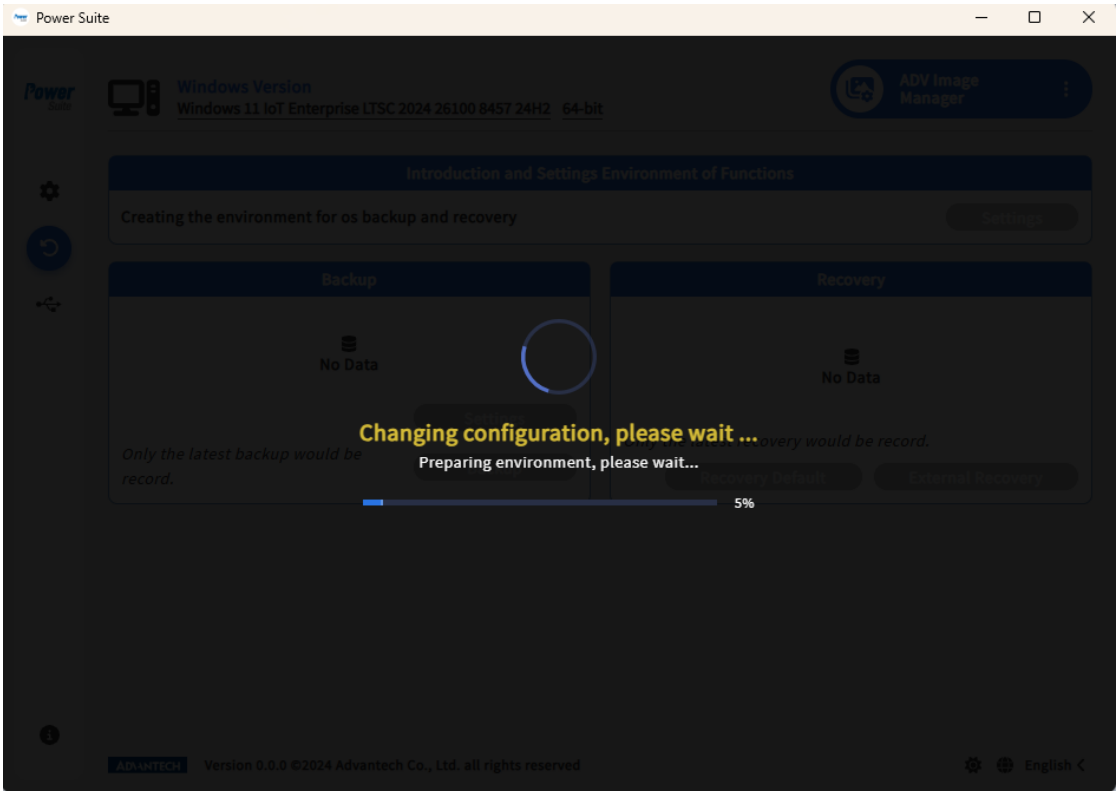
Select the "**ADV Image Manager**" tab, then select the "**Backup & Recovery**" page, and then press "**Settings**" button.



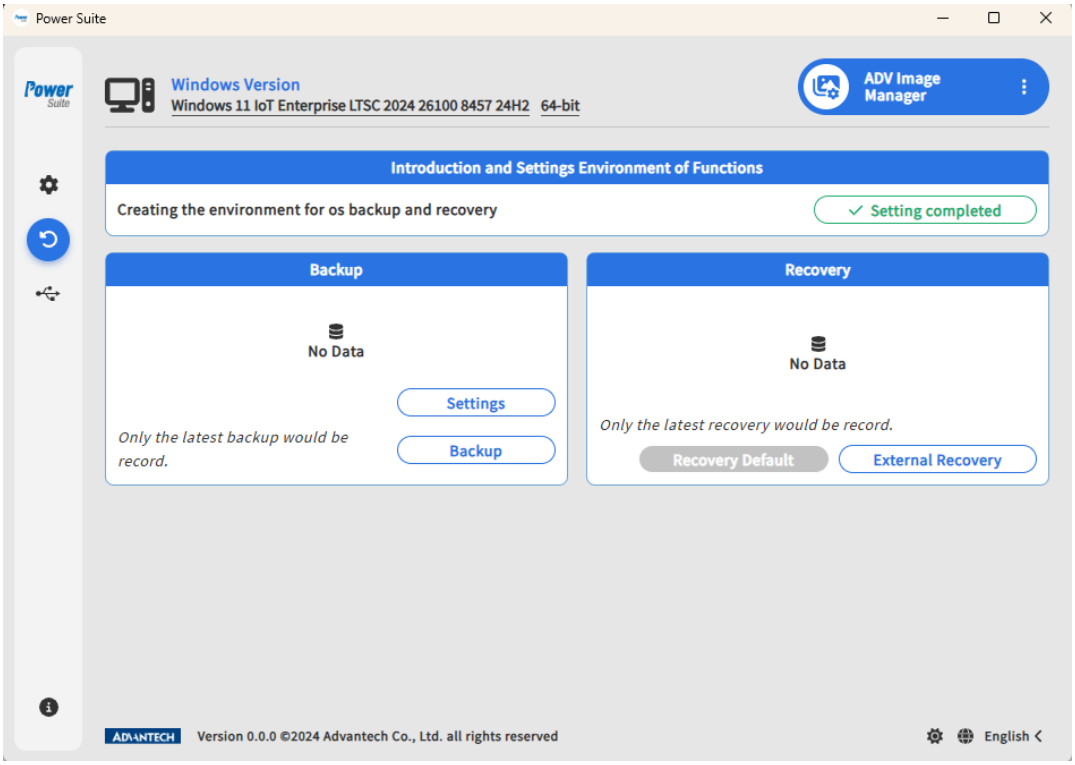
The computer's built-in WinRE will be replaced after the ADV Image Manager environment is created. This is an irreversible change even if the ADV Image Manager is uninstalled. Press "**Confirm**" to continue creating the environment.



It takes a while to create the environment, please wait.

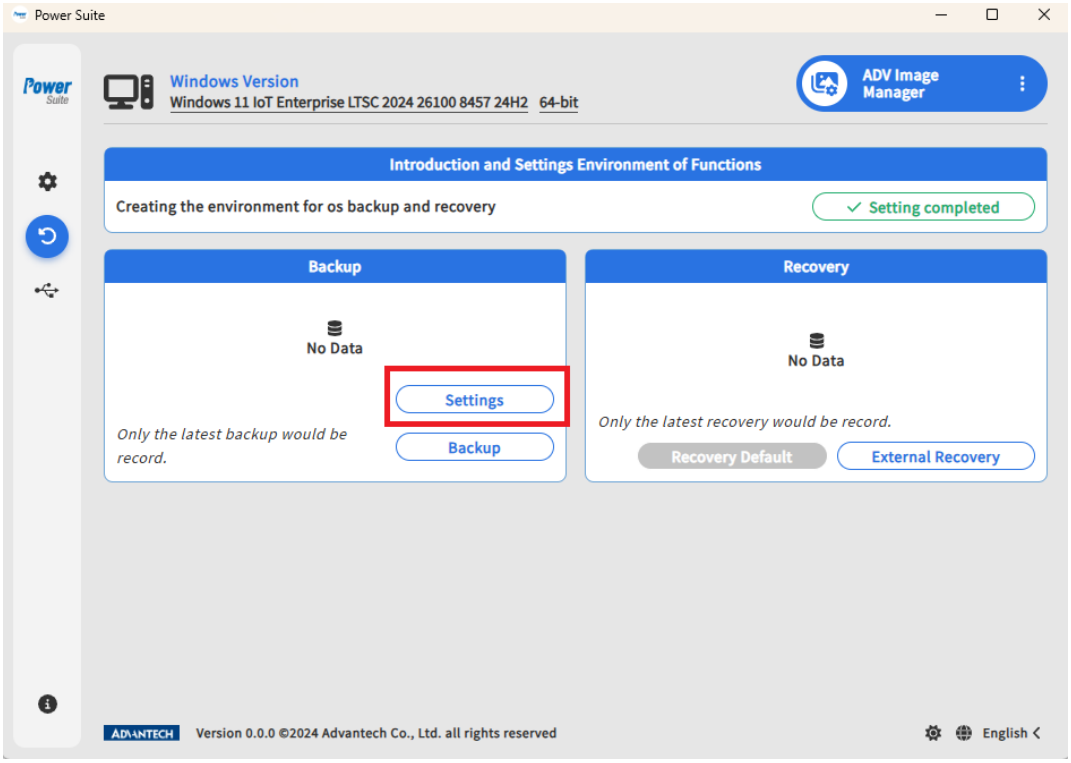


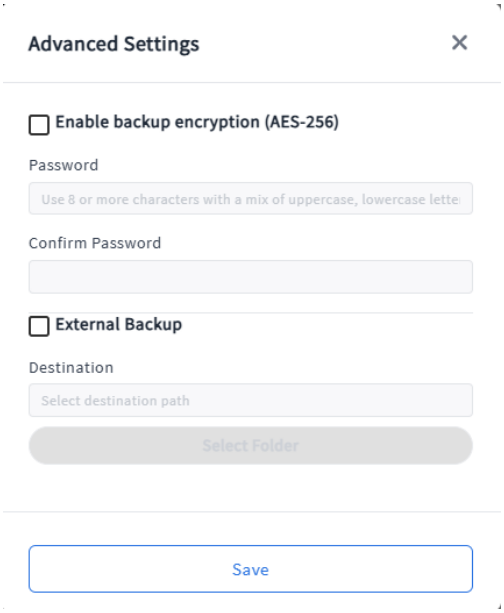
When the environment is created successfully, ADV Image Manager will display as shown below.



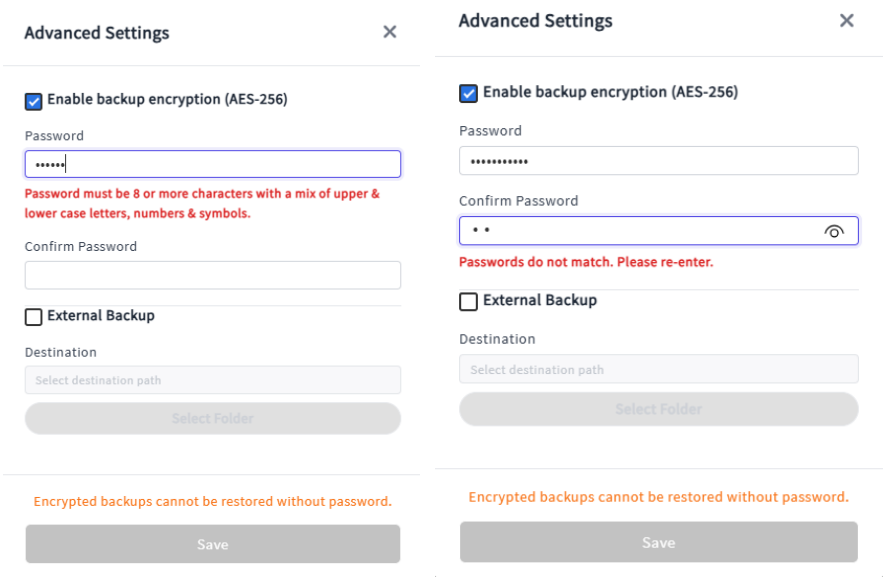
5.1.3 Create Image Encrypted Backup

Click the "**Settings**" button, then show **"Advanced Setting"** Dialog.





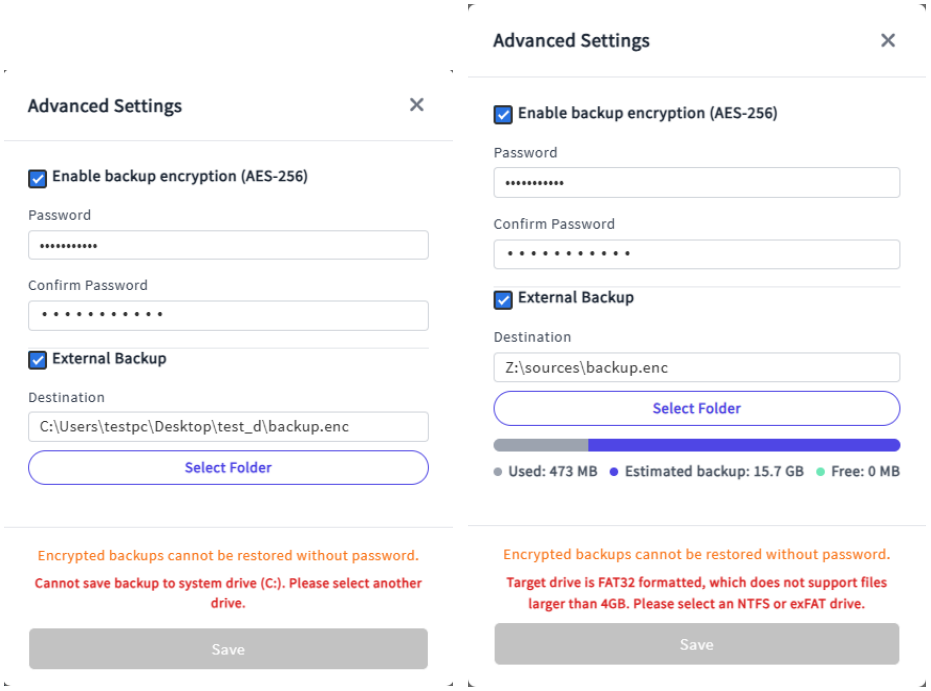
If you want to enable the encryption function, you must enter your password twice (Use 8 or more characters with a mix of uppercase, lowercase letters, numbers & symbols). If the password is not complex enough or the two passwords are different, a warning will be displayed.

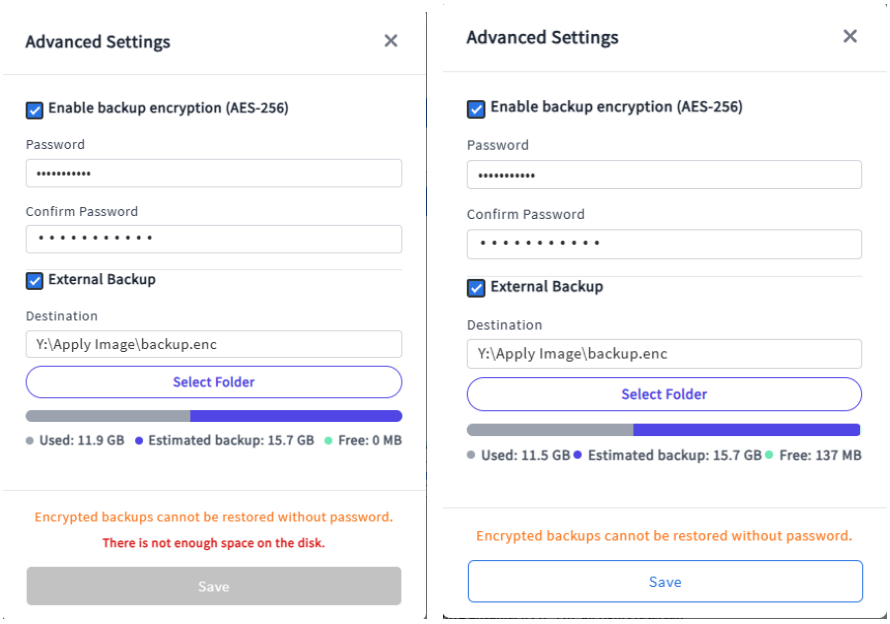


If you want to enable the external backup function, check the checkbox and select an external backup path. The following rules must be followed:

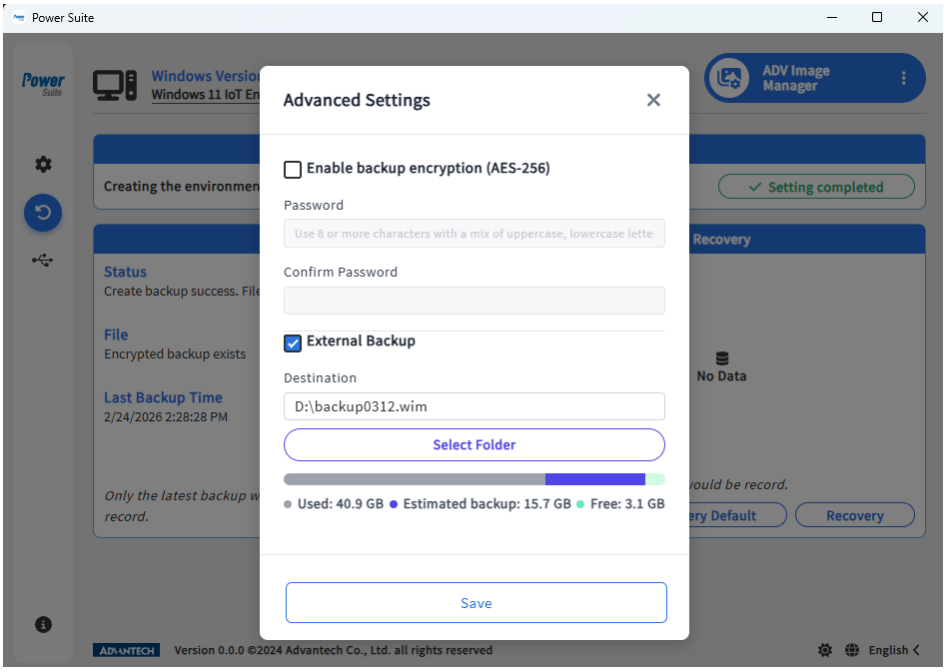
- The C drive cannot be selected.
- The storage space must be sufficient.
- FAT32 file systems are not supported.

If an invalid location is selected, the corresponding error message will be displayed on the screen.

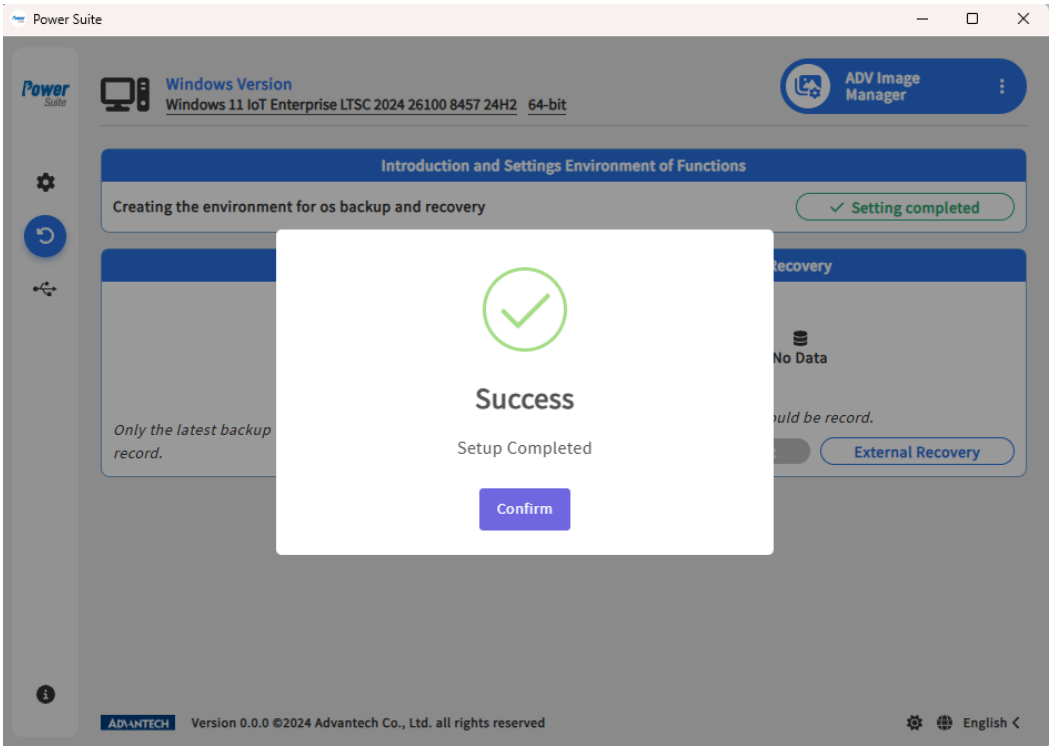




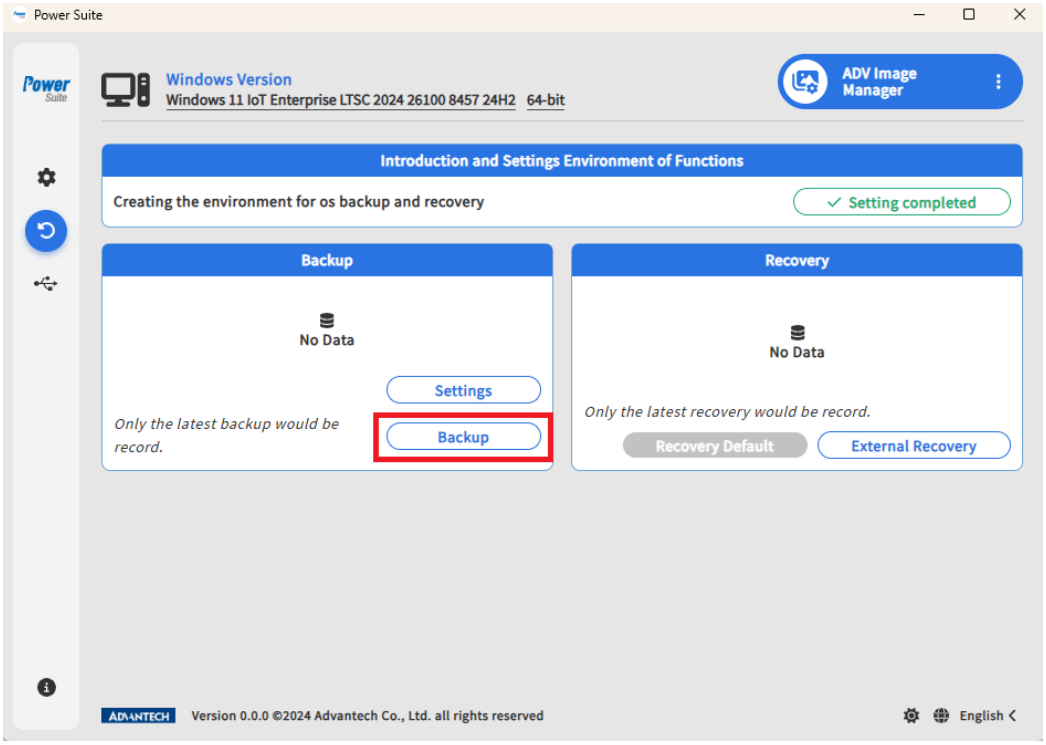
When all checks pass and no warning messages (red text) are displayed, you can click Save to proceed.

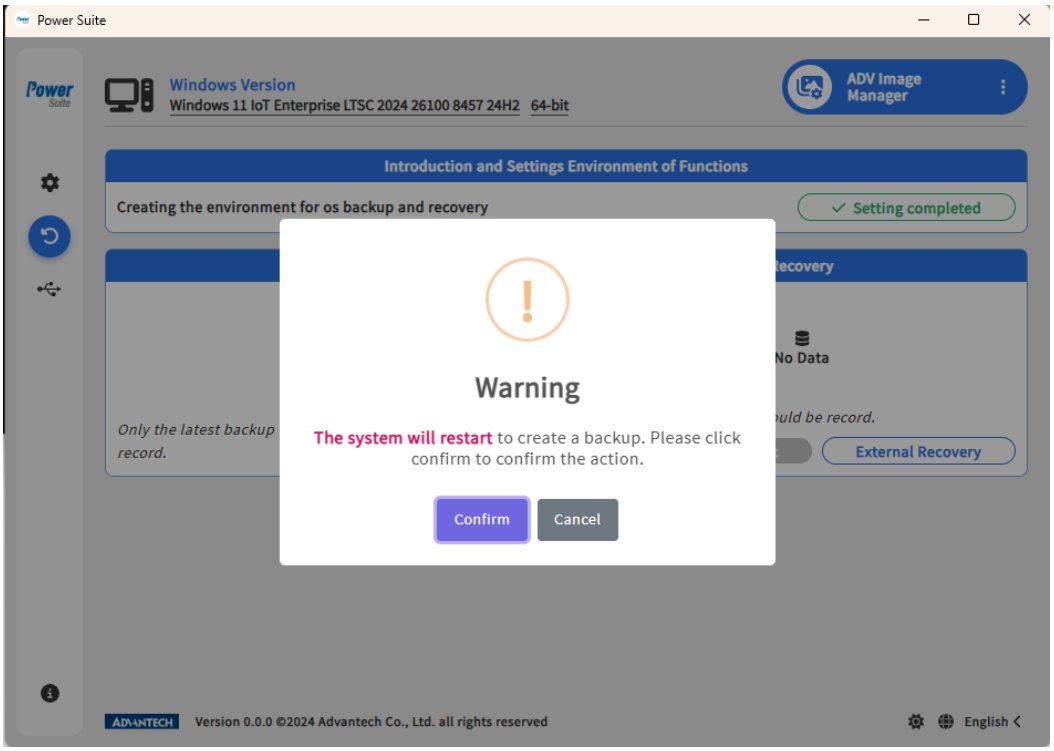


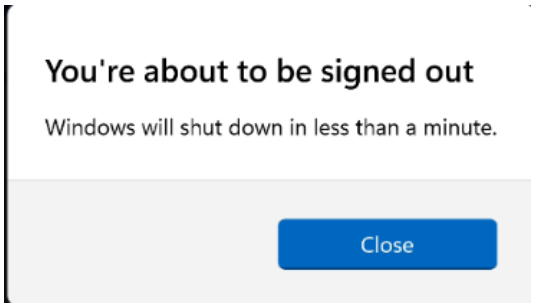
After Confirm your password even the external backup path.



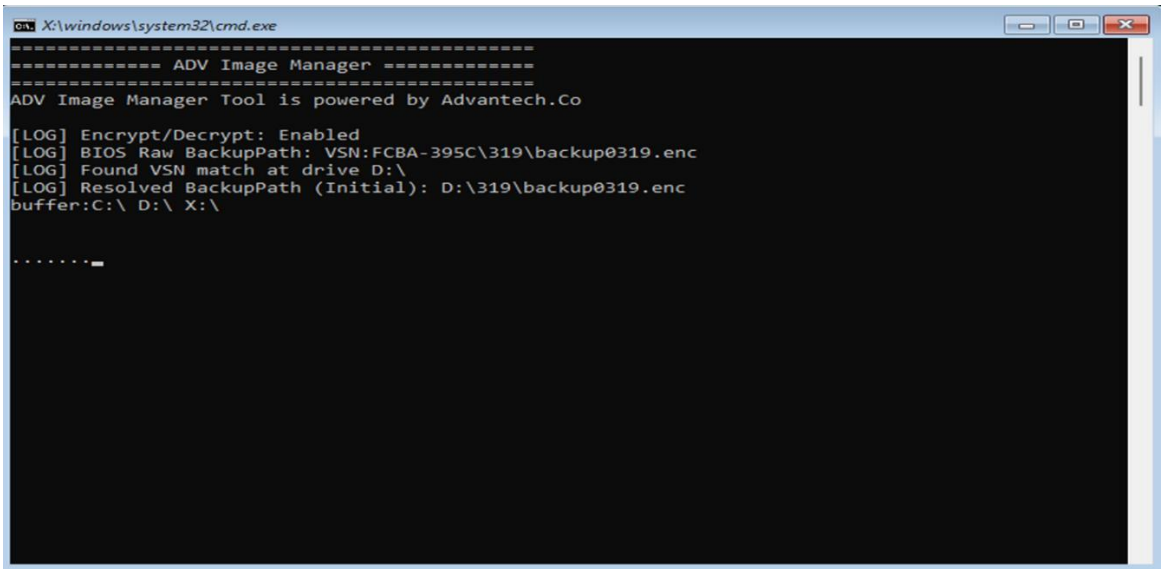
Click the “**Backup**” button, then press “**Confirm**”. The system will restart to WinRE and start the backup. Please don’t close ADV Image Manager after the backup starts.

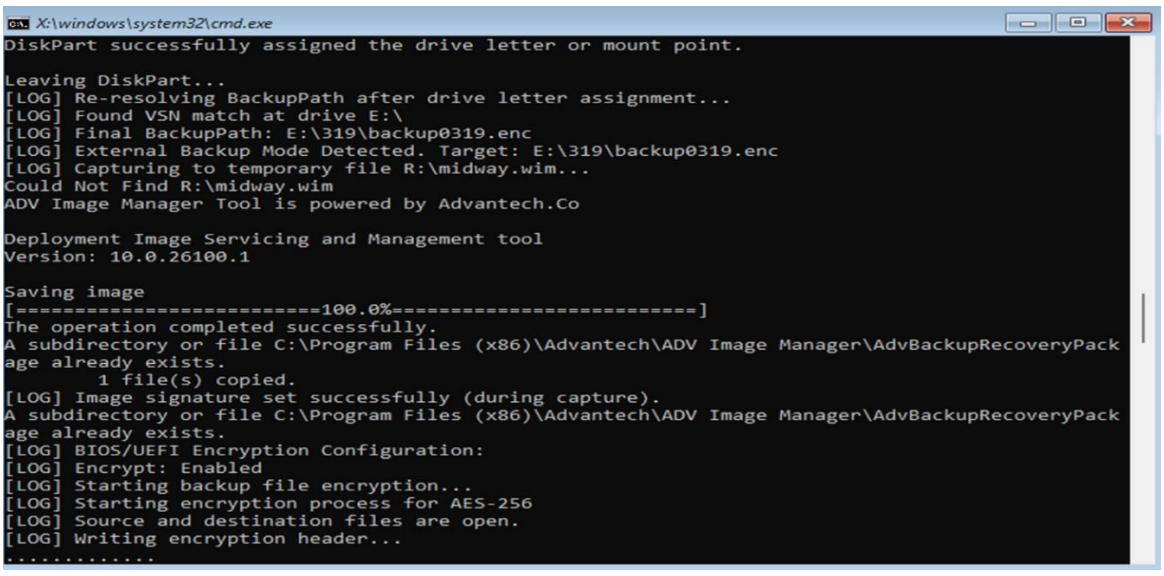

Power Suite
Windows Version
Windows 11 IoT Enterprise LTSC 2024 26100 8457 24H2 64-bit
ADV Image Manager
Introduction and Settings Environment of Functions
Creating the environment for os backup and recovery
Setting completed
Backup
No Data
Settings
Only the latest backup would be record.
Backup
Recovery
No Data
Only the latest recovery would be record.
Recovery Default
External Recovery
Version 0.0.0 ©2024 Advantech Co., Ltd. all rights reserved
English

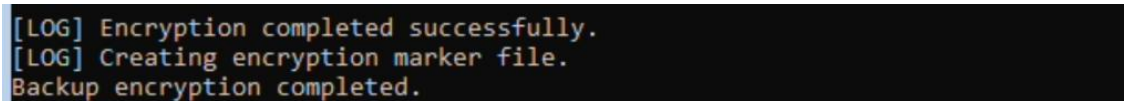

Power Suite
Windows Version
Windows 11 IoT Enterprise LTSC 2024 26100 8457 24H2 64-bit
ADV Image Manager
Introduction and Settings Environment of Functions
Creating the environment for os backup and recovery
Setting completed
Warning
The system will restart to create a backup. Please click confirm to confirm the action.
Confirm
Cancel
External Recovery
Version 0.0.0 ©2024 Advantech Co., Ltd. all rights reserved
English



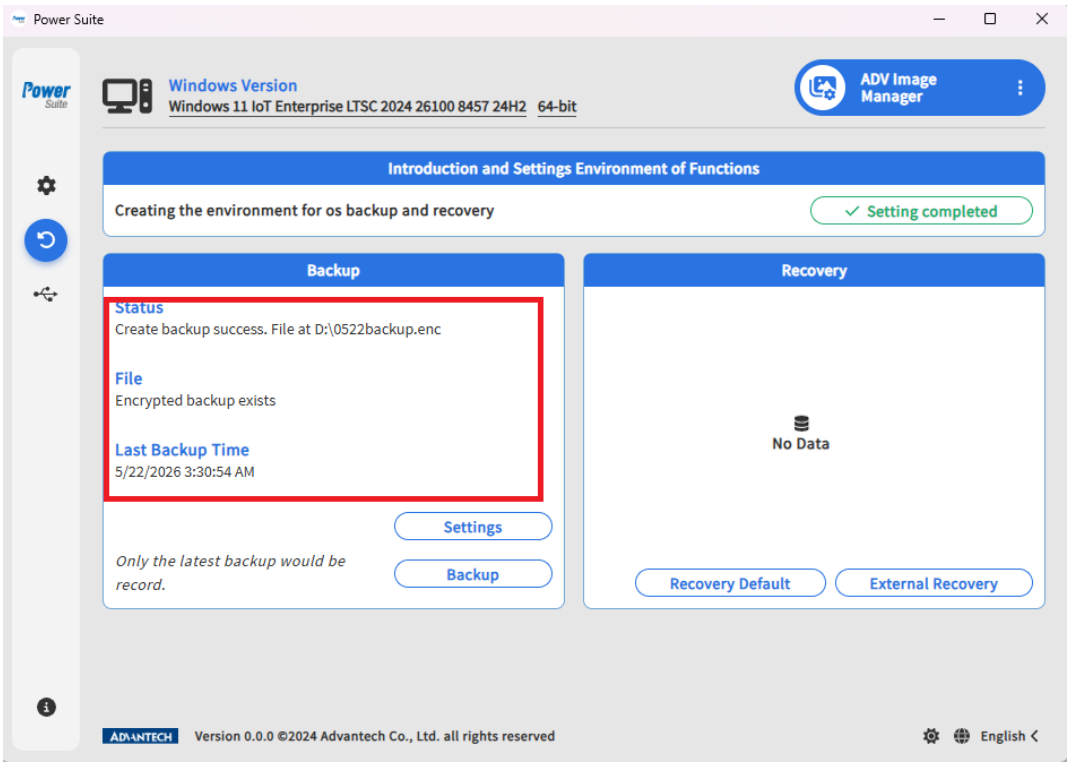
In WinRE, please don’t close the command prompt and keep the system focused on the command prompt to run the backup. If the system is not focused on the command prompt, please press “Enter” in the command prompt to regain focus.







When the backup is finished, the system will automatically restart and boot into Windows. In Windows, open the ADV Image Manager application to check the backup result. If the last successful backup was saved to an external location, the Status field will additionally display the external path where the backup was stored.

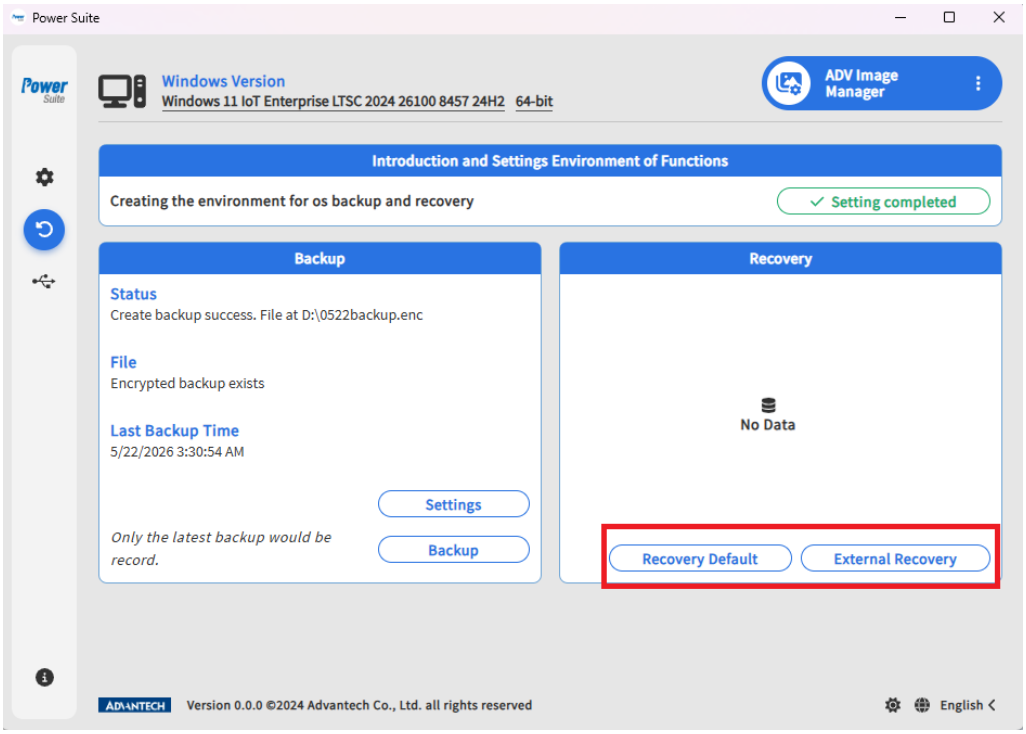


5.1.4 Recovery

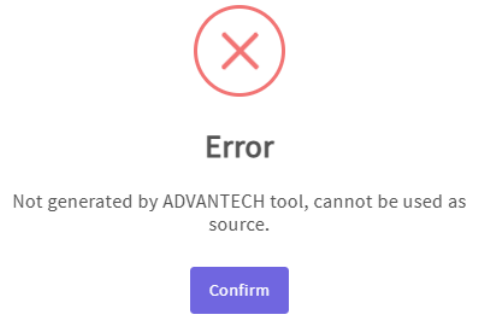
➢ **Recover Image from tool**

There are two recovery methods available.

- **Recovery Default**: Use this option to restore the system from the backup file stored internally in the system. This option is available only when a valid backup file exists in the system.
- **Recovery**: Use this option to restore the system from an external backup file. When an external file is selected, ADV Image Manager will verify the file to ensure it is valid and can be used for recovery.

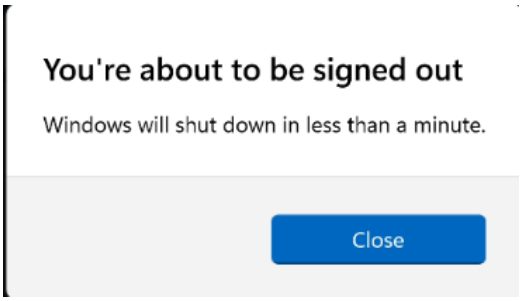


If the verification fails, the following message will be displayed.



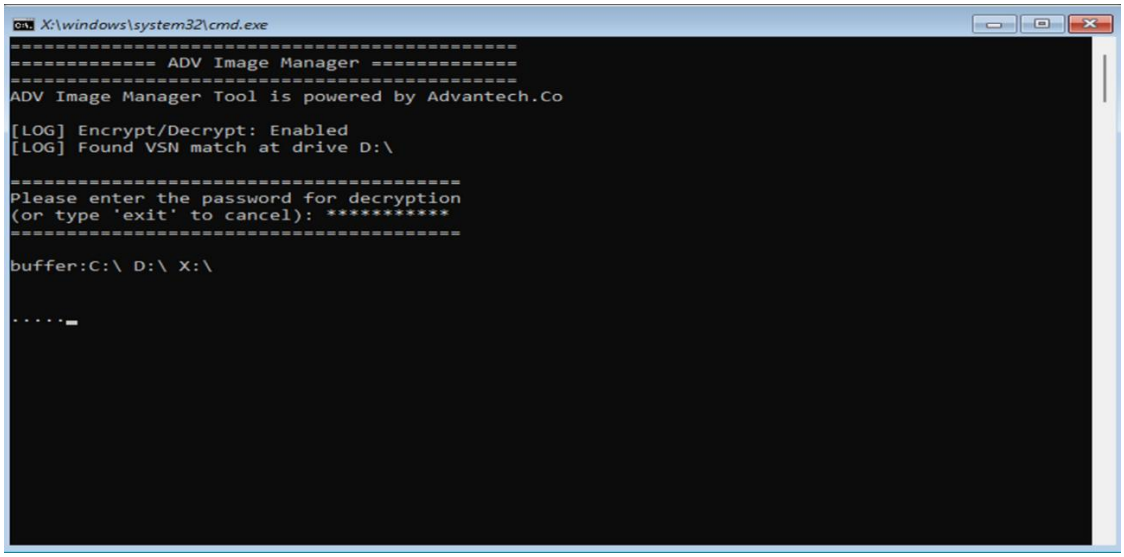
Click the Recovery button, then press Confirm. The system will restart to WinRE and start the recovery process. The backup file will be restored to C:, and all changes made after the backup file was created will be lost. Please do not close ADV Image Manager after the recovery process starts.

Now, you're ready to reboot.

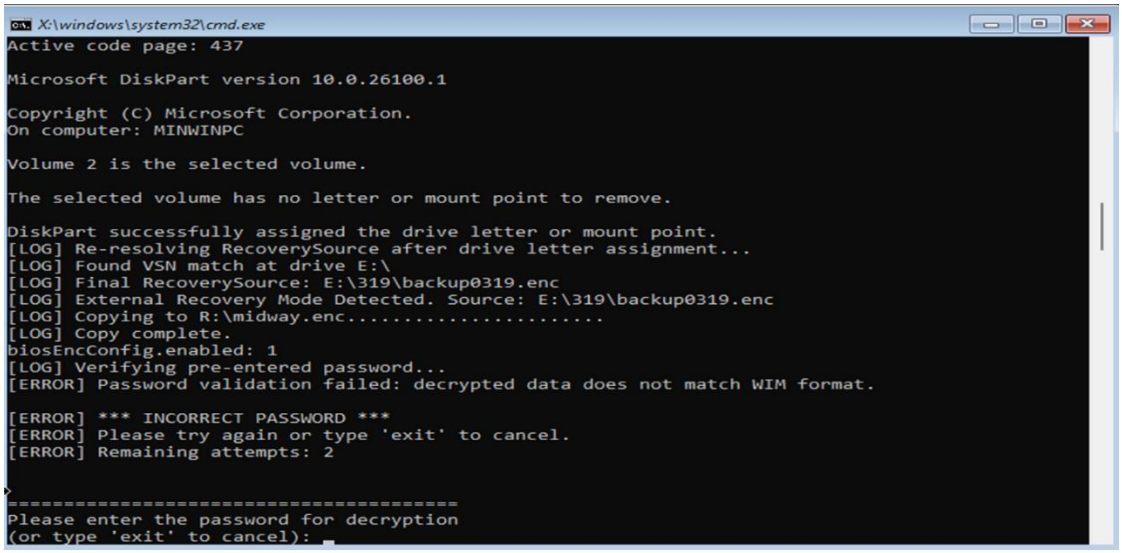


Please don't close the command prompt and keep the system focused on the command prompt to run the recovery. If the system is not focused on the command prompt, please press "Enter" in the command prompt to regain focus.

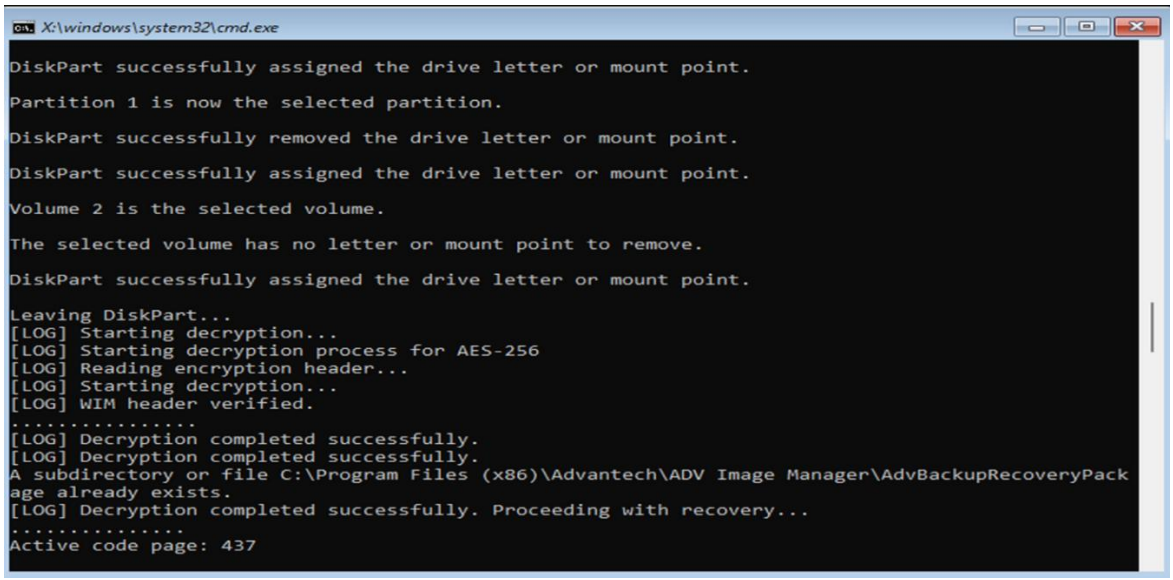
If you are restoring from an encrypted backup file(*.enc), please enter the password first. Otherwise, no password is required.

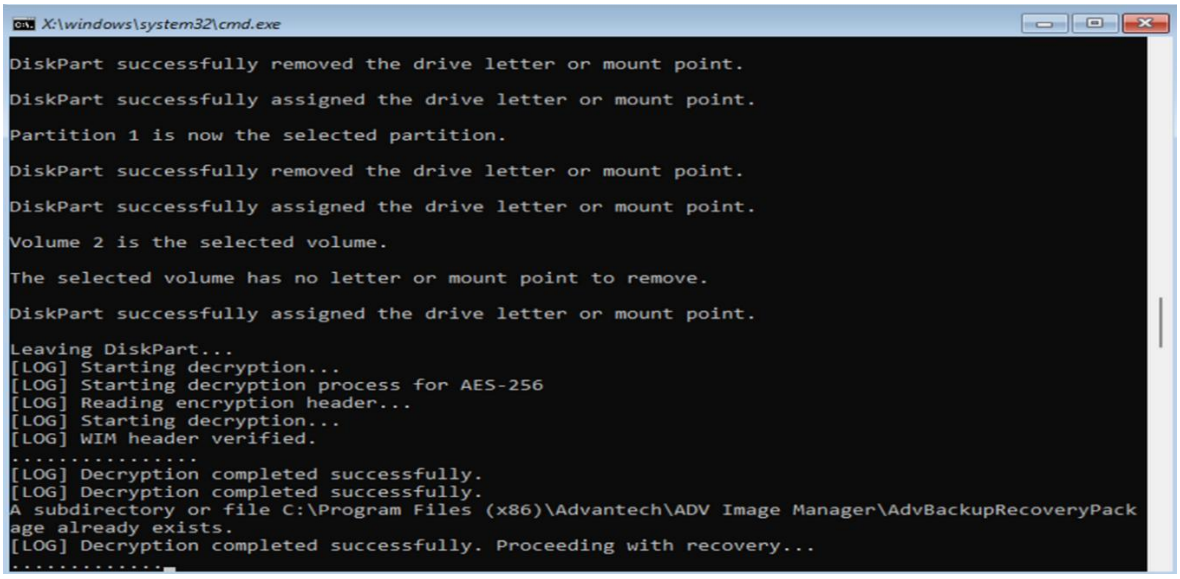


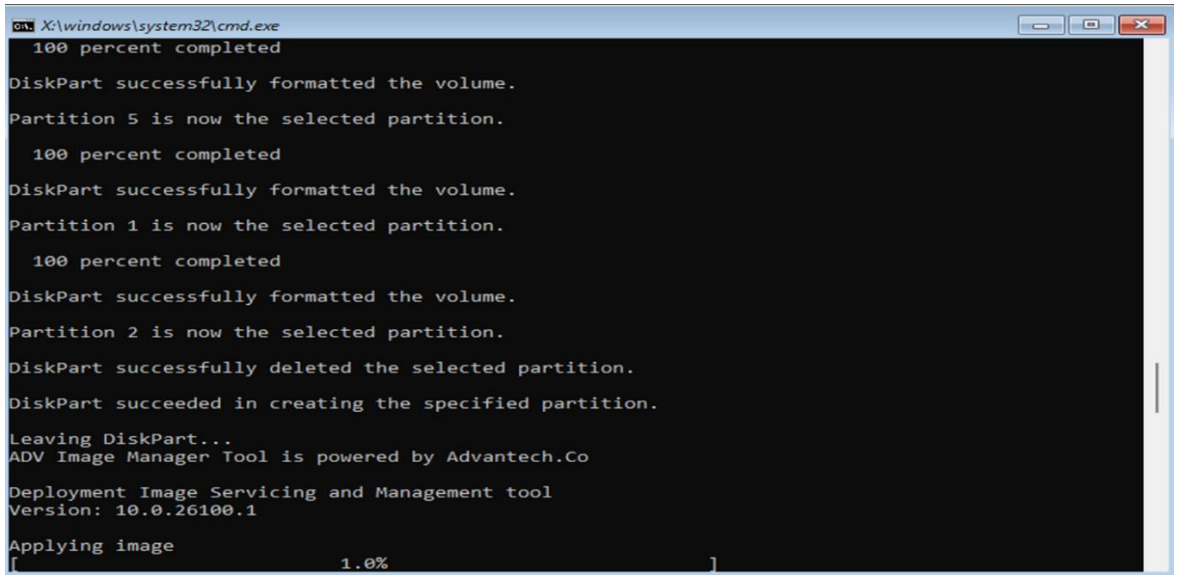
You have three chances to enter the correct password.



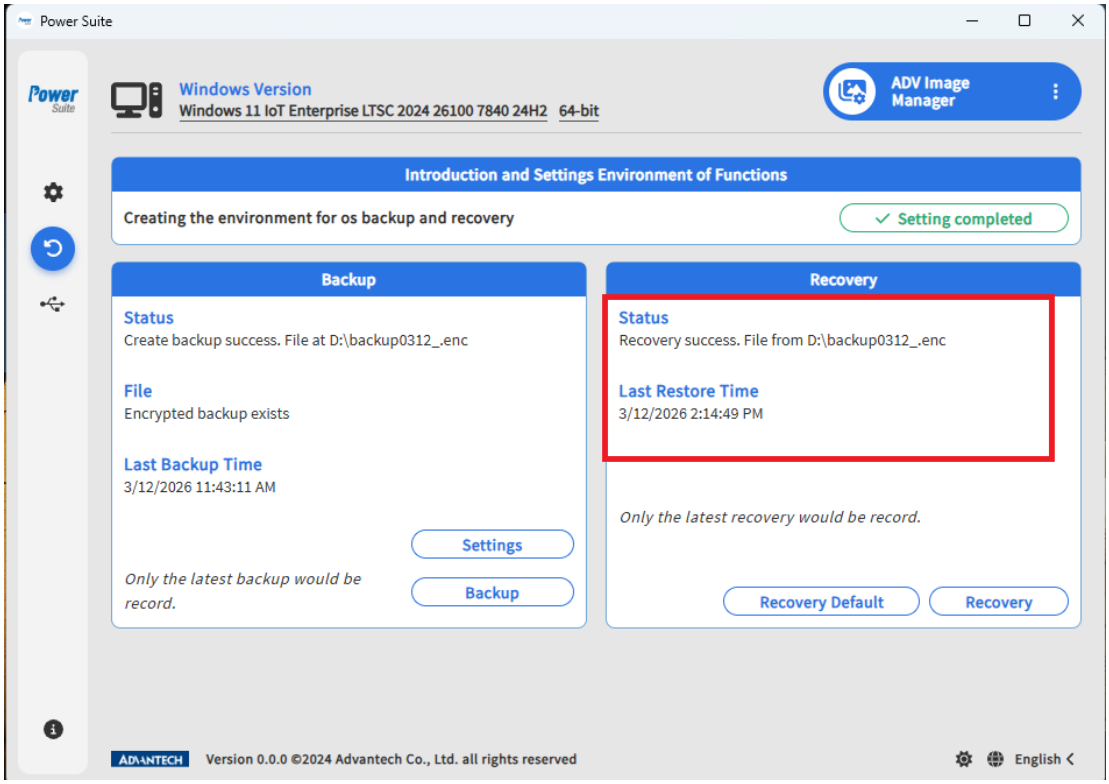
If you enter the correct password.


X:\windows\system32\cmd.exe
DiskPart successfully assigned the drive letter or mount point.
Partition 1 is now the selected partition.
DiskPart successfully removed the drive letter or mount point.
DiskPart successfully assigned the drive letter or mount point.
Volume 2 is the selected volume.
The selected volume has no letter or mount point to remove.
DiskPart successfully assigned the drive letter or mount point.
Leaving DiskPart...
[LOG] Starting decryption...
[LOG] Starting decryption process for AES-256
[LOG] Reading encryption header...
[LOG] Starting decryption...
[LOG] WIM header verified.
[LOG] Decryption completed successfully.
[LOG] Decryption completed successfully.
A subdirectory or file C:\Program Files (x86)\Advantech\ADV Image Manager\AdvBackupRecoveryPack
age already exists.
[LOG] Decryption completed successfully. Proceeding with recovery...
Active code page: 437


X:\windows\system32\cmd.exe
DiskPart successfully removed the drive letter or mount point.
DiskPart successfully assigned the drive letter or mount point.
Partition 1 is now the selected partition.
DiskPart successfully removed the drive letter or mount point.
DiskPart successfully assigned the drive letter or mount point.
Volume 2 is the selected volume.
The selected volume has no letter or mount point to remove.
DiskPart successfully assigned the drive letter or mount point.
Leaving DiskPart...
[LOG] Starting decryption...
[LOG] Starting decryption process for AES-256
[LOG] Reading encryption header...
[LOG] Starting decryption...
[LOG] WIM header verified.
[LOG] Decryption completed successfully.
[LOG] Decryption completed successfully.
A subdirectory or file C:\Program Files (x86)\Advantech\ADV Image Manager\AdvBackupRecoveryPack
age already exists.
[LOG] Decryption completed successfully. Proceeding with recovery...


X:\windows\system32\cmd.exe
100 percent completed
DiskPart successfully formatted the volume.
Partition 5 is now the selected partition.
100 percent completed
DiskPart successfully formatted the volume.
Partition 1 is now the selected partition.
100 percent completed
DiskPart successfully formatted the volume.
Partition 2 is now the selected partition.
DiskPart successfully deleted the selected partition.
DiskPart succeeded in creating the specified partition.
Leaving DiskPart...
ADV Image Manager Tool is powered by Advantech.Co
Deployment Image Servicing and Management tool
Version: 10.0.26100.1
Applying image
[1.0%]

When the recovery is finished, the system will auto restart and boot into Windows. In Windows, open the ADV Image Manager application to check the recovery result.



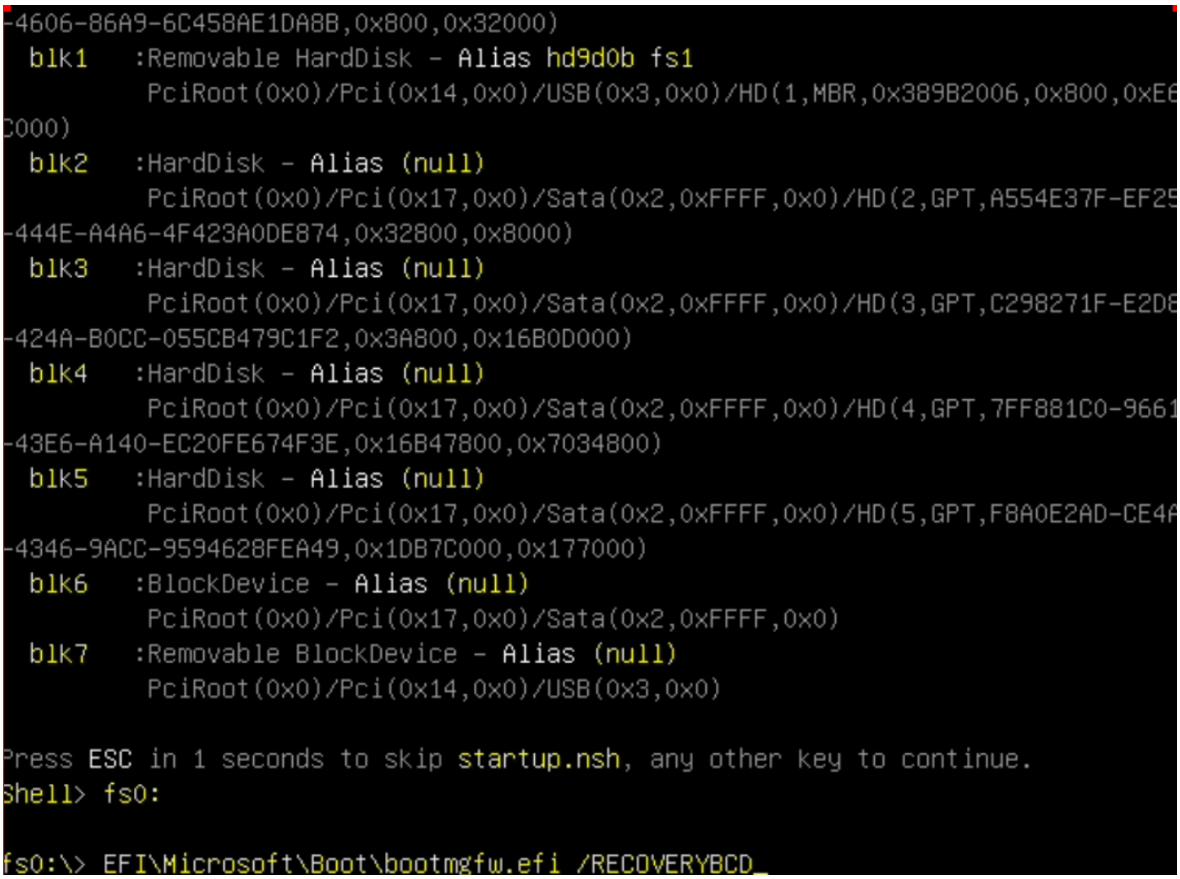
➢ **Recover Image from EFI Shell**

Besides starting recovery from the desktop application, ADV Image Manager can also start recover from WinRE. The WinRE entry points can reference on the Microsoft website. When the computer fails to enter the Windows system, you can use this method to recover your system.

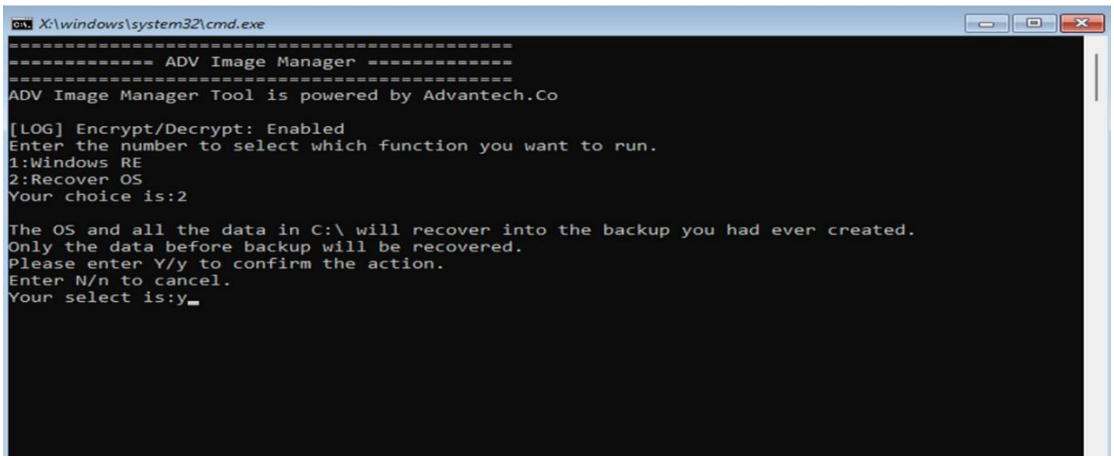
Note: This method has not been validated on Windows on ARM (WoA) systems and is therefore not supported.

I. Using the BIOS built-in EFI Shell or a USB drive that includes EFI Shell can start WinRE.
II. Using command “fsX:” and “EFI\Microsoft\Boot\bootmgfw.efi /RecoveryBCD” to enter WinRE.

III. X is the selected file system's number.

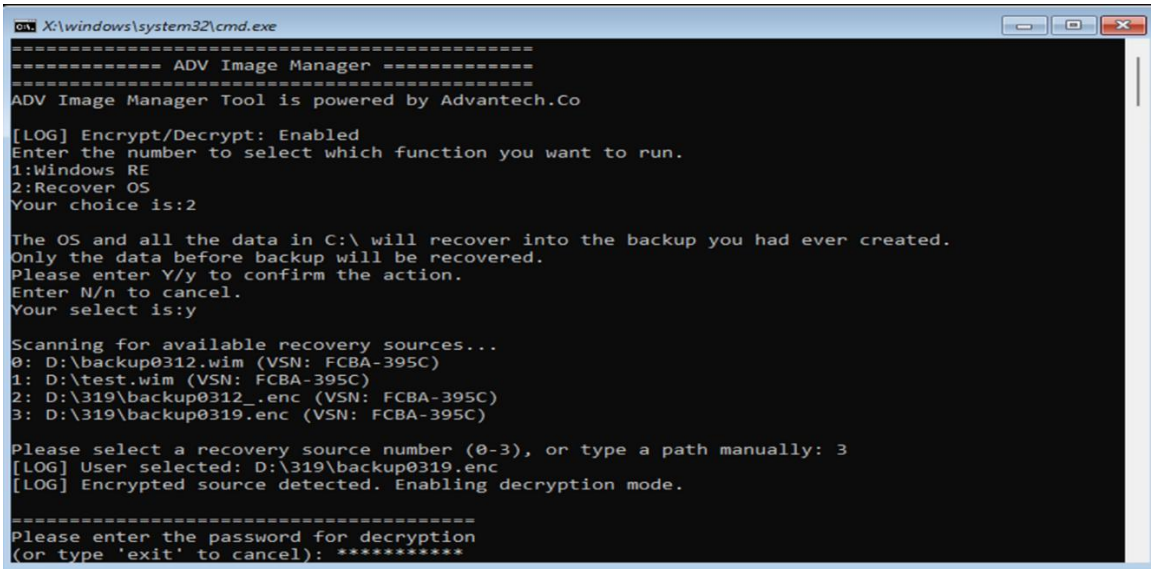


IV. Type "2" then press "Enter" to select the Recover OS function. Type "Y" or "y" then press "Enter" to start the recovery. After recovery, the system will reboot into Windows. If you want to cancel the recovery, please type "N" or "n" then press "Enter" to cancel.



The system will scan for available **.wim** or **.enc** files within the root directory and one level of subdirectories, and display them in a selection menu.

Please select the image you want to restore. *(The image shown is for illustration purposes only.)*
If the selected file is encrypted (.enc), you will be prompted to enter a password. Otherwise, no password is required.

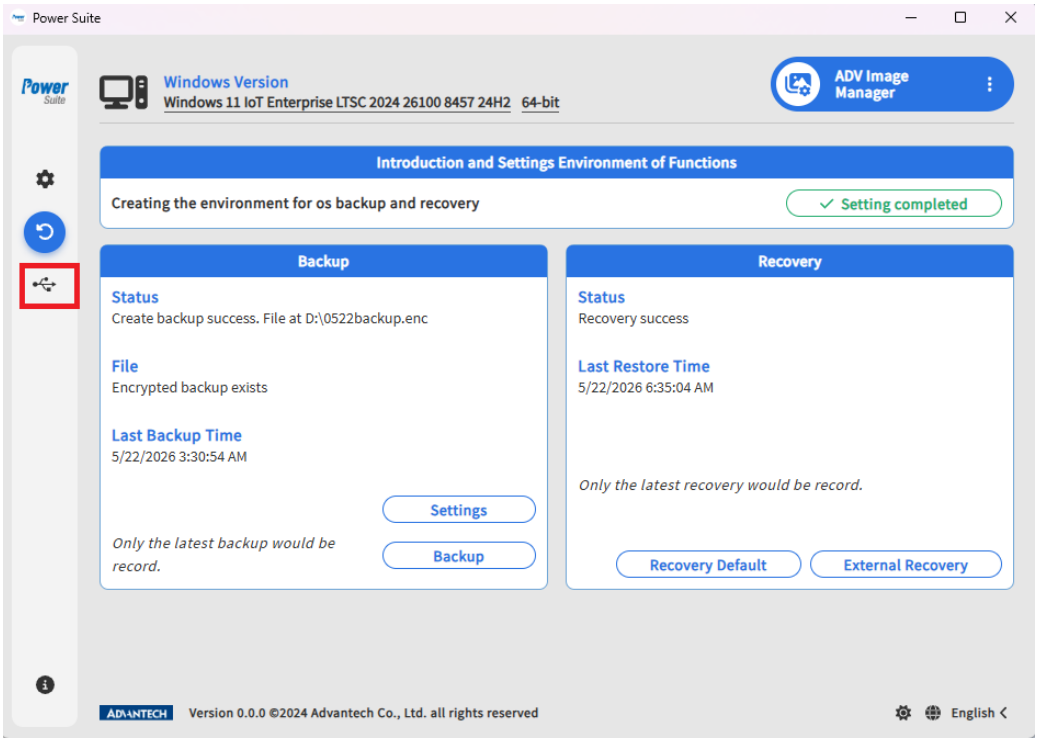


You have three chances to enter the correct password. After recovery, the system will reboot into Windows.

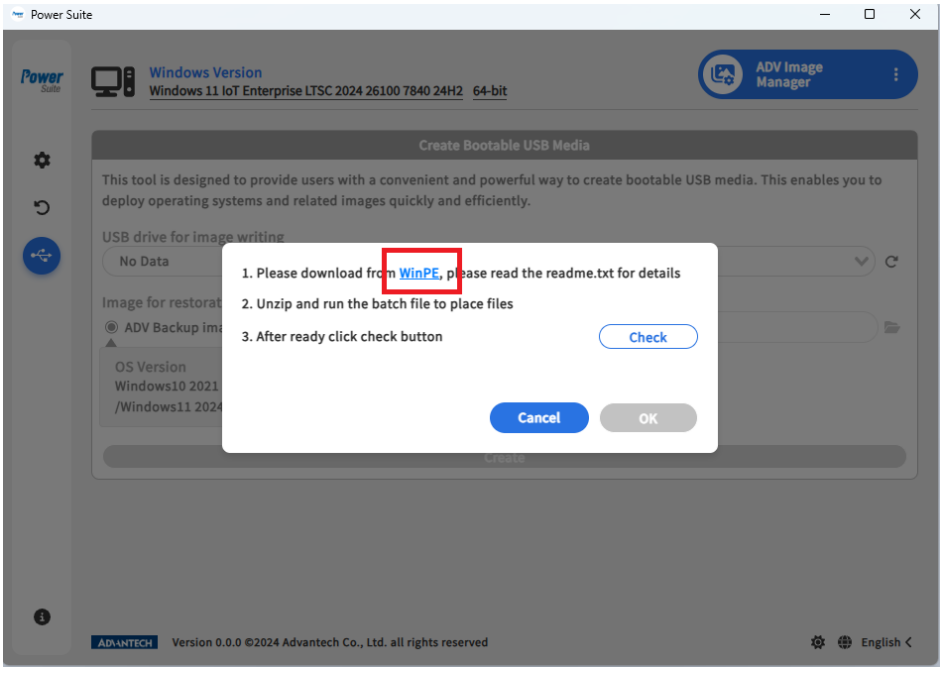
For other WinRE functions, please check 6.2.

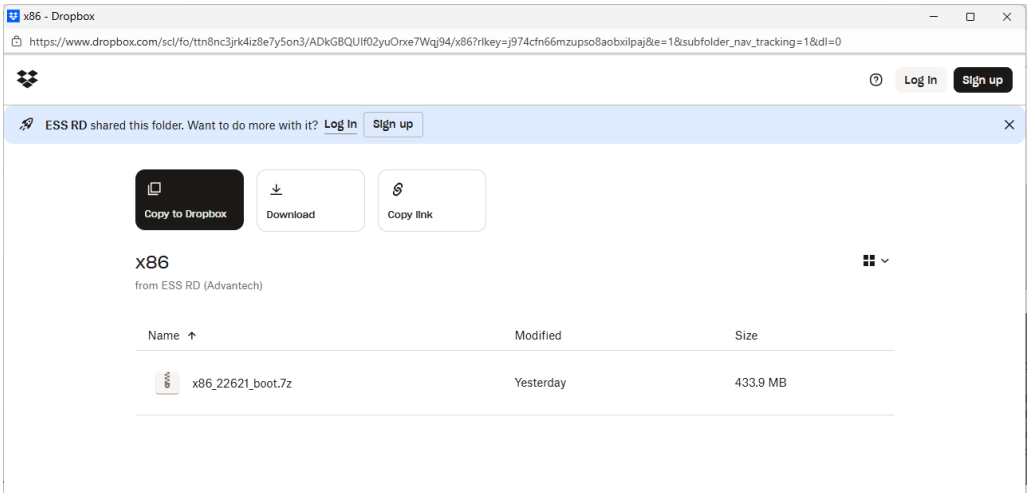
5.1.5 Bootable USB Media

After the base backup file is created, you can proceed to create a bootable USB. Click the option highlighted in the red box on the screen to open the bootable USB function page. (WoA not support)

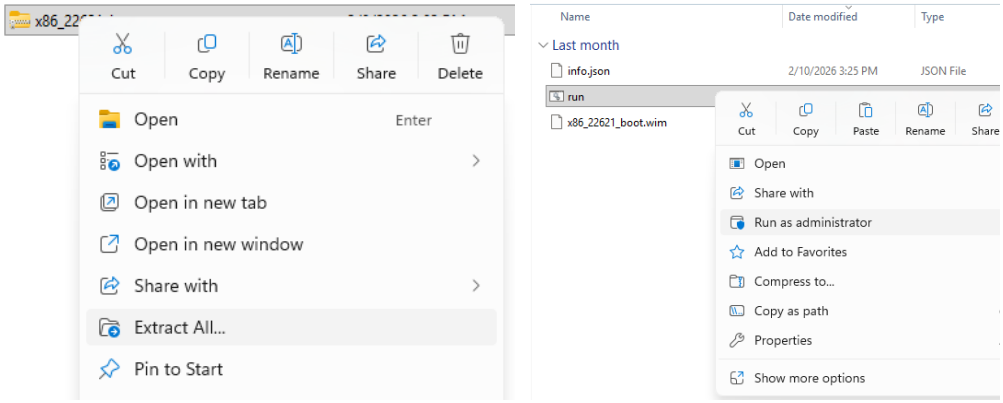


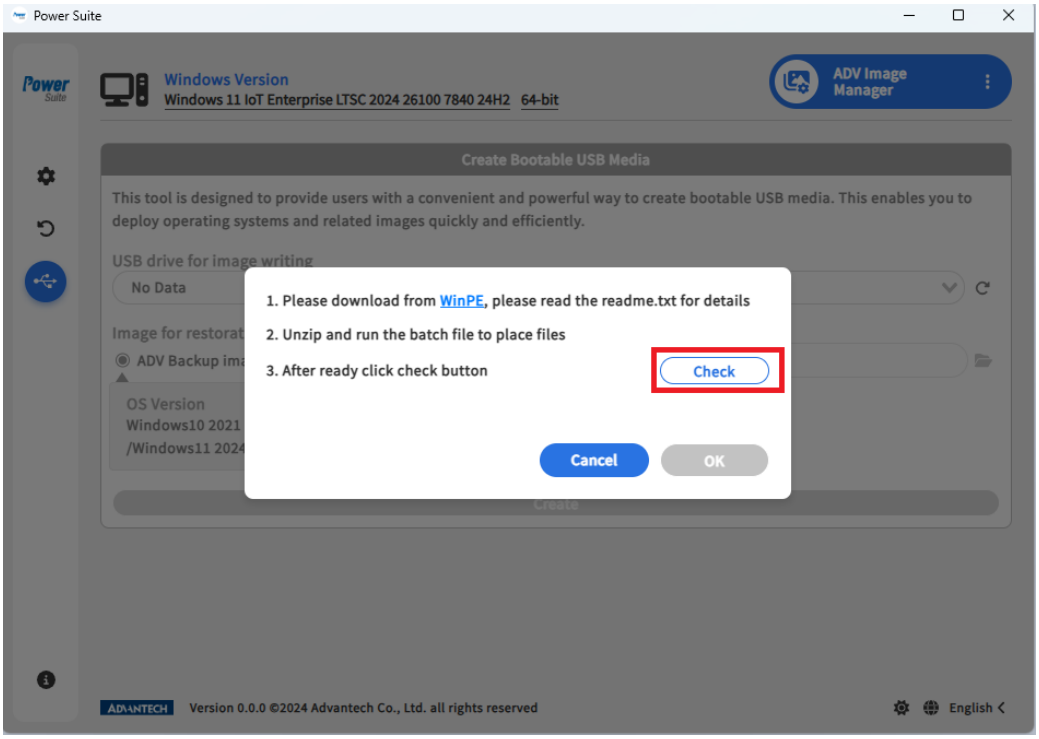
First, the following window will appear. Please follow the steps shown. Begin by opening the provided link and downloading the required compressed package according to the instructions on the page.



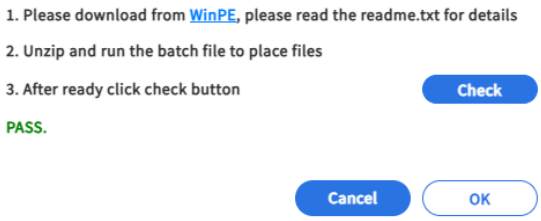


Extract the compressed file and run **run.bat**.

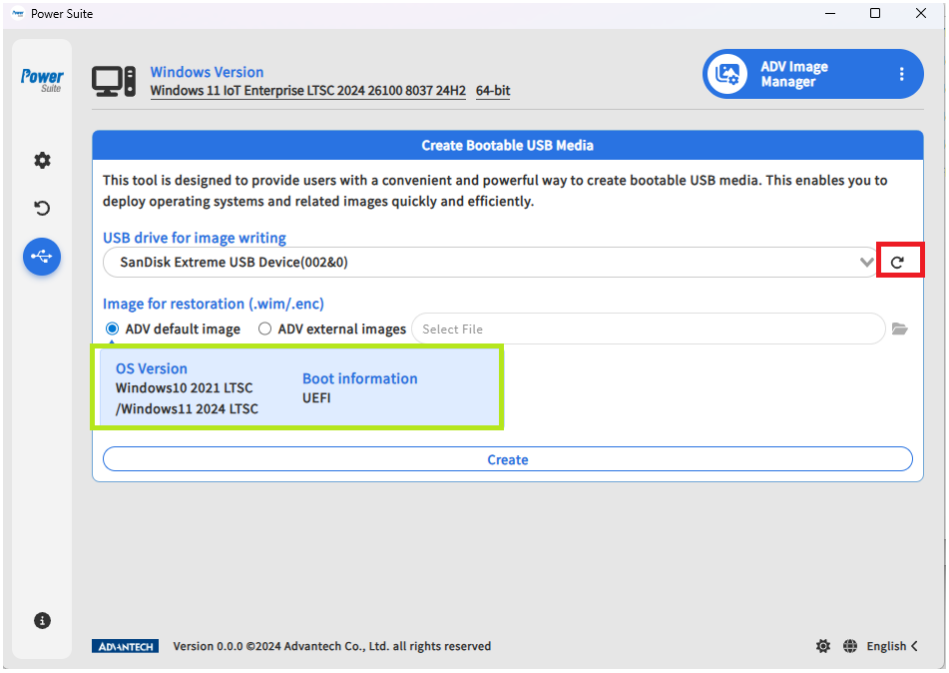




After the process finishes, click **Check** in the dialog box to perform the verification. If the verification is successful, **PASS** will be displayed and the page will be available. If the verification fails, the page will remain disabled.

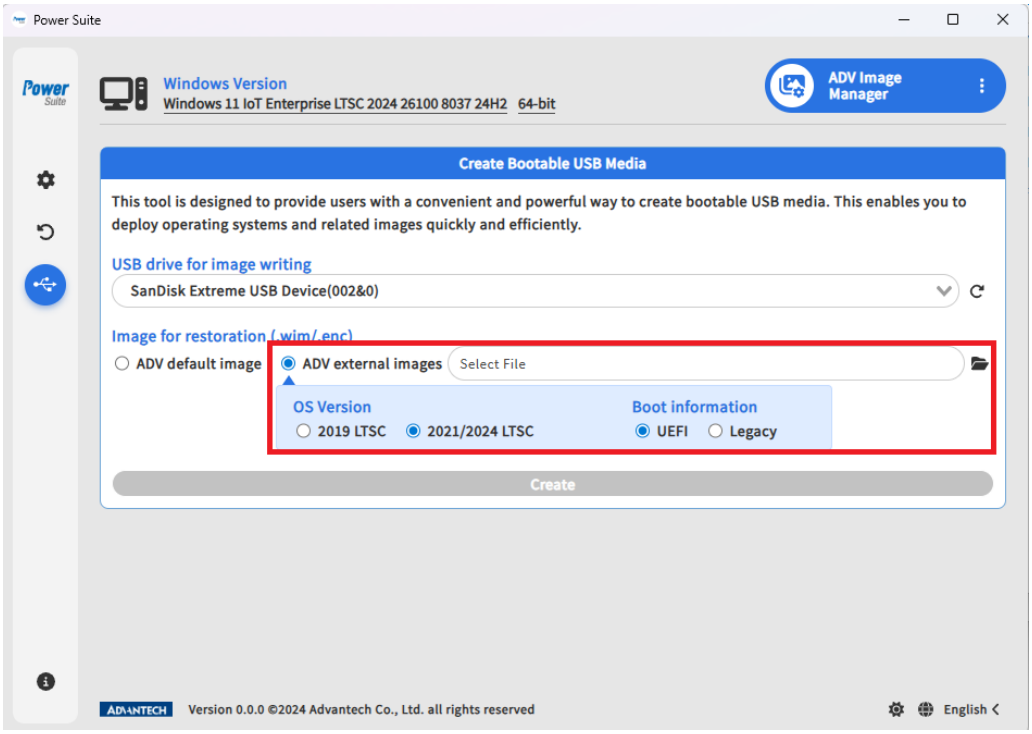


After entering the settings page, click the option highlighted in the red box to re-detect the USB device. If a backup file already exists in the system, the information will be displayed in the area highlighted in the green box.



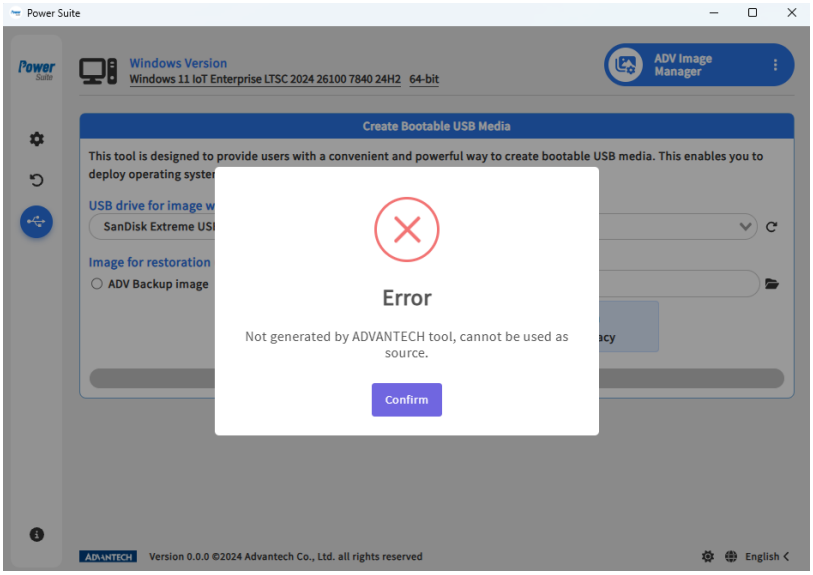
If you do not want to use the internal backup file, select **Other Images** and click the folder icon to open an external backup file.

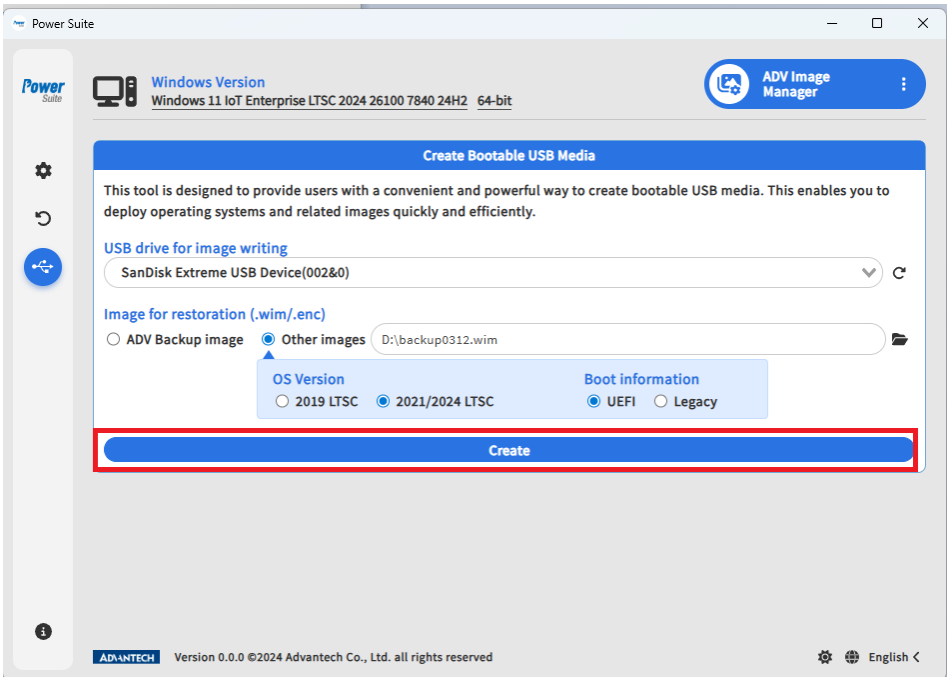
When using an external backup file, you must manually select the correct **OS version** and **Boot information**. If the selected settings do not match the external backup file, the recovery process may fail.

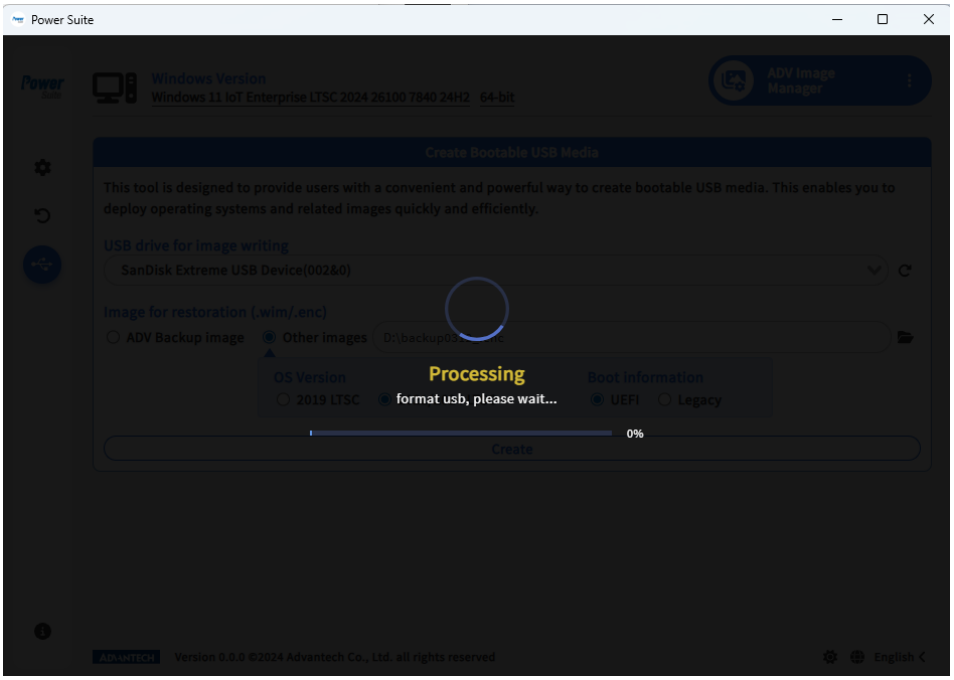


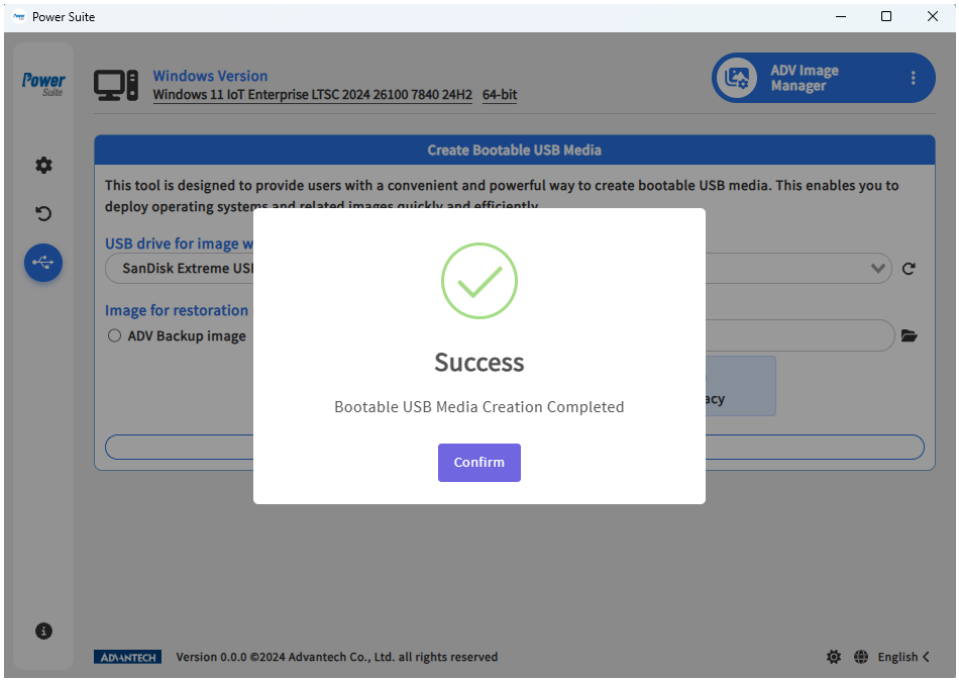
If the selected file is a **.wim** file, the system will perform a rule check. If the check passes, you can proceed with **Create**. If the check fails, an error message will be displayed as shown below.

For **.enc** files, no rule check is required.




Power Suite
Windows Version
Windows 11 IoT Enterprise LTSC 2024 26100 7840 24H2 64-bit
ADV Image Manager
Create Bootable USB Media
This tool is designed to provide users with a convenient and powerful way to create bootable USB media. This enables you to deploy operating systems and related images quickly and efficiently.
USB drive for image writing
SanDisk Extreme USB Device(002&0)
Image for restoration (.wim/.enc)
ADV Backup image
Other images
D:\backup0312.wim
OS Version
2019 LTSC
2021/2024 LTSC
Boot information
UEFI
Legacy
Create
Version 0.0.0 ©2024 Advantech Co., Ltd. all rights reserved
English


Power Suite
Processing
format usb, please wait...
0%
Create

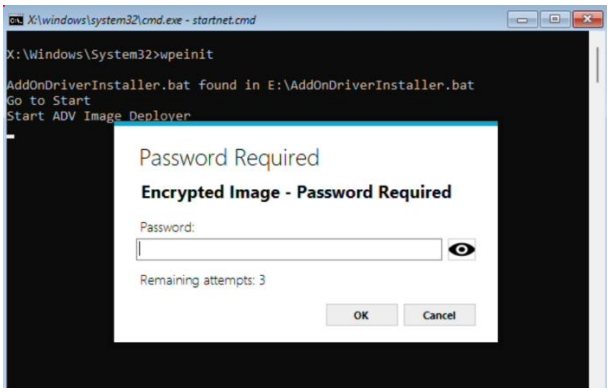


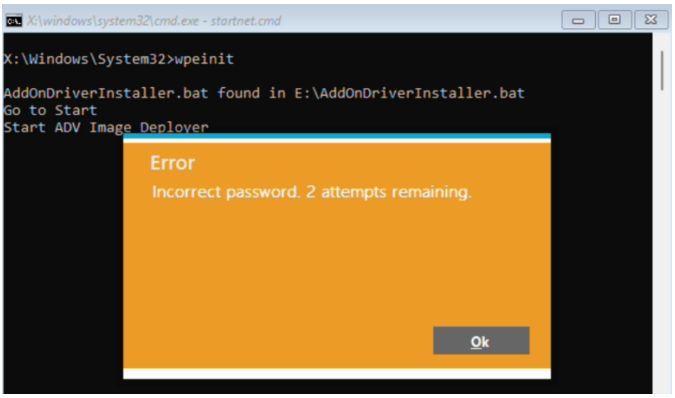
TIP: After the USB is created, if an **.enc** file is selected, make sure the remaining space on the USB drive is larger than the selected **.enc** file.

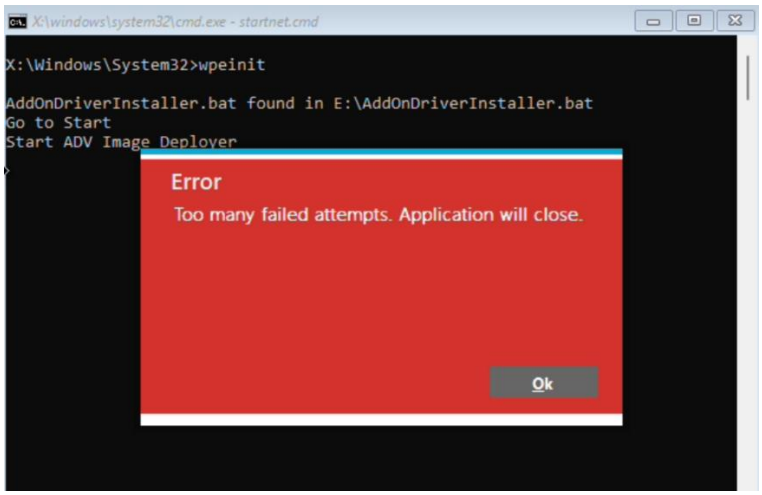
5.1.6 Recovery from Bootable USB

After the USB is created, you can test it by rebooting the system.
Enter the BIOS setup and change the boot order so that the system boots from the USB device.

If the image was created from an encrypted file (.enc), you will first be prompted to enter the password. You have three attempts to enter the correct password.
If a .wim file is used, the password verification step will be skipped. Click the eye icon to temporarily reveal the password you entered.

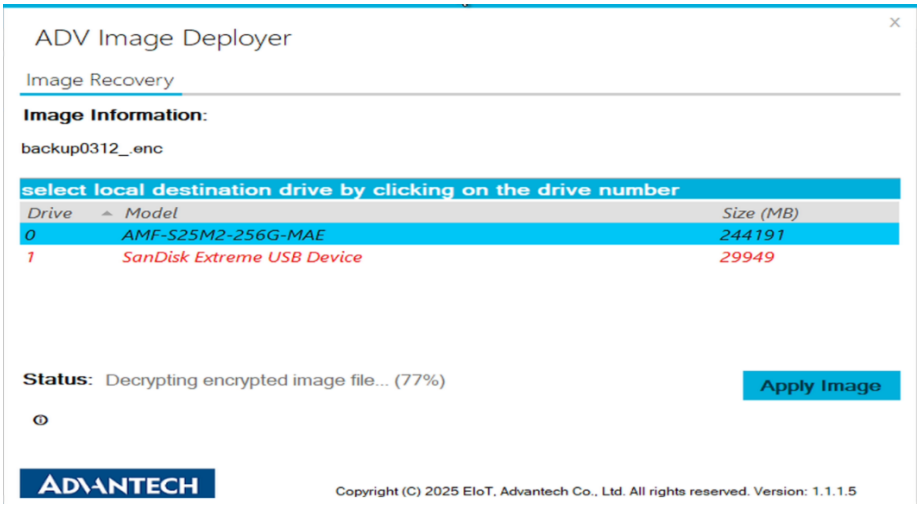




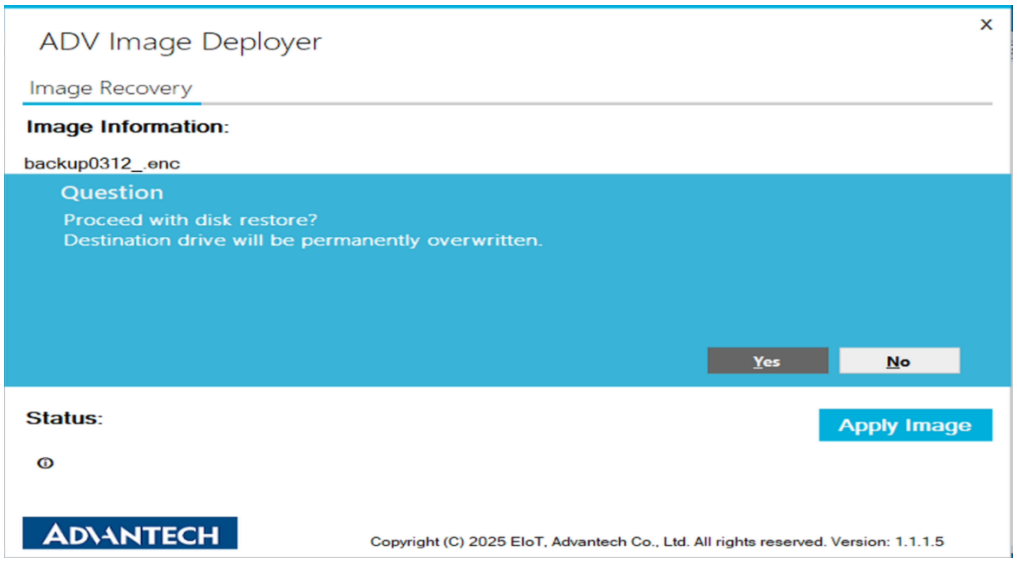


After entering the main screen as shown in the figure, the backup file name you created earlier will be displayed at the top.

At this point, select the destination where you want to restore the image. Please make sure the correct destination is selected

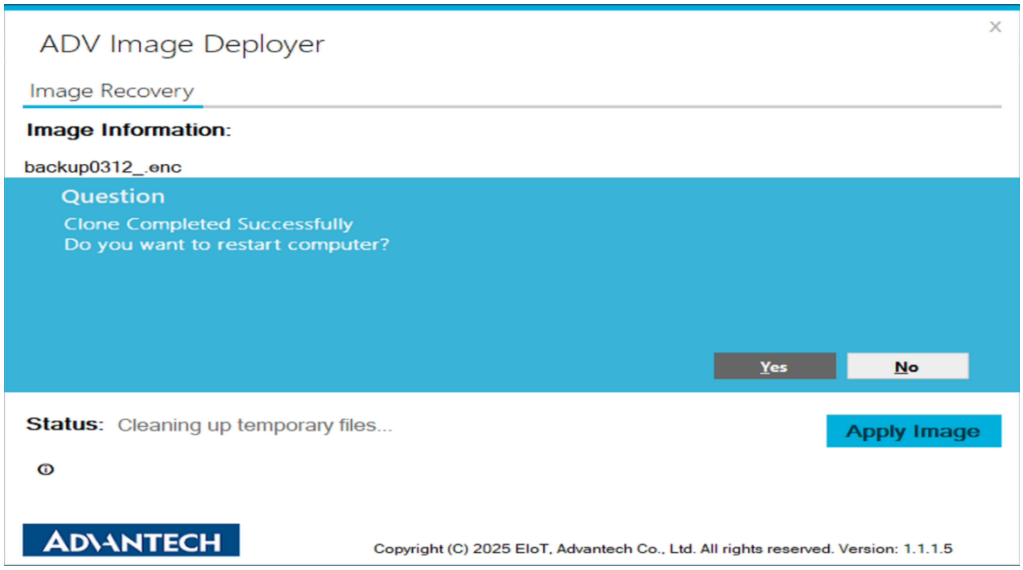


Click **“Apply Image.”** A confirmation message will appear. Click **“Yes”** to proceed.



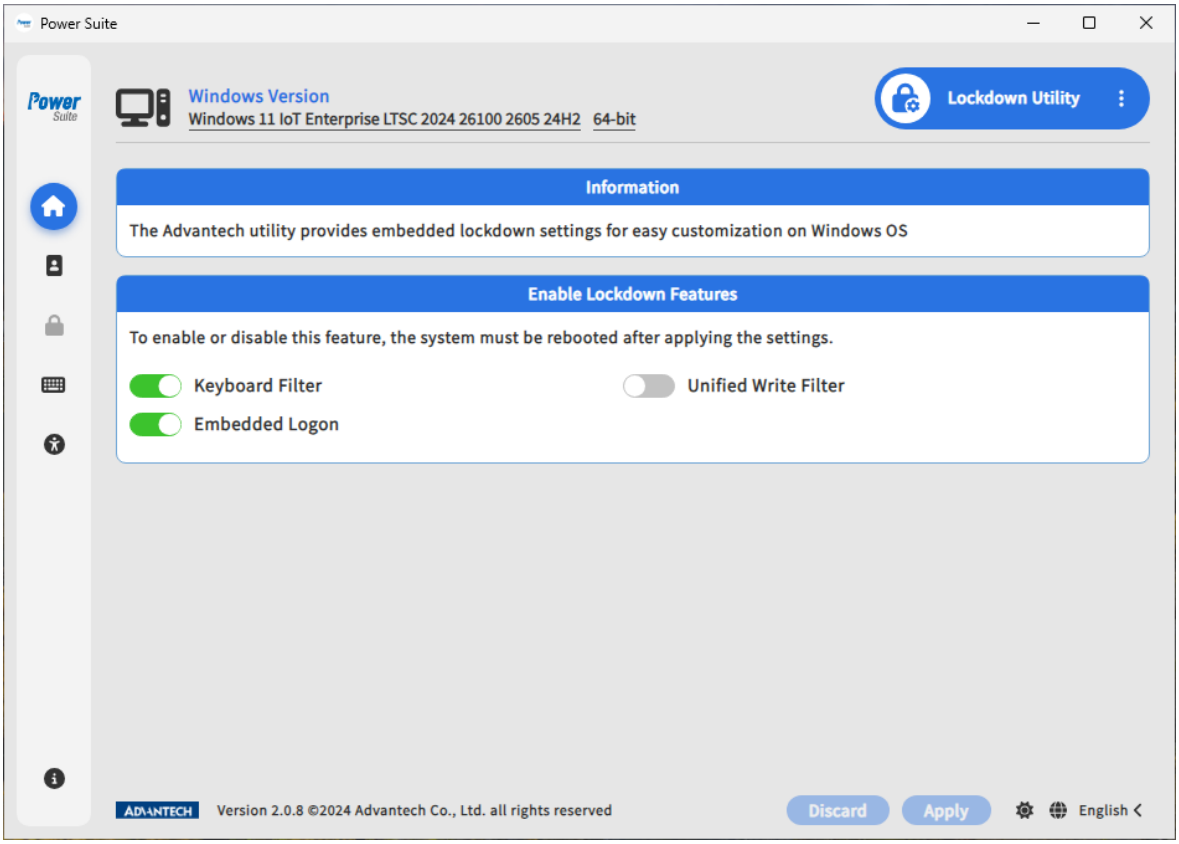
The progress can be monitored in the **Status** section.

After the process is completed, a message will appear prompting you to restart the system.

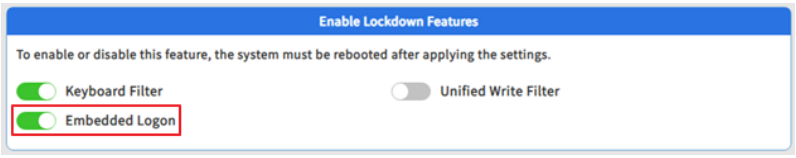


5.2 Lockdown Utility

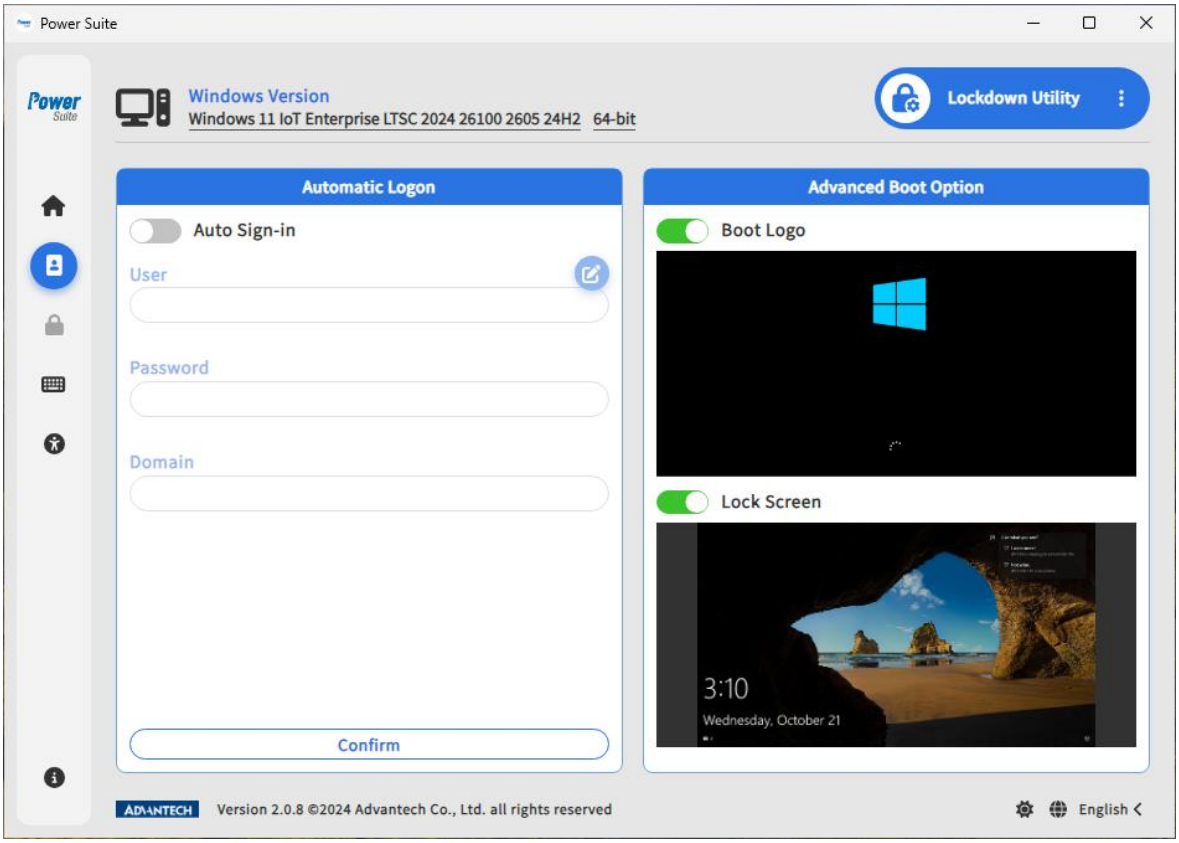
5.2.1 Lockdown Settings



- Enable Lockdown Features
  - There are some dependency settings to be designed onto the Enable Lockdown Features. You can directly enable or disable Windows Features without using DISM.
  - Each toggle switch is correspondence with the menu items on the left side. If you do not enable toggle switch, you will not be able to use the menu item functions.
  - Enable toggles before configuring functions from the left menu.
  - If **Embedded Logon** is enabled, the shutdown logo will not be displayed.



5.2.2 Automatic Logon and Boot Options



- Automatic Logon
  - Auto Sign-in: enabling this function to automatically logon with your **User Name**, **Password**, and **Domain Name** when boot up**.**

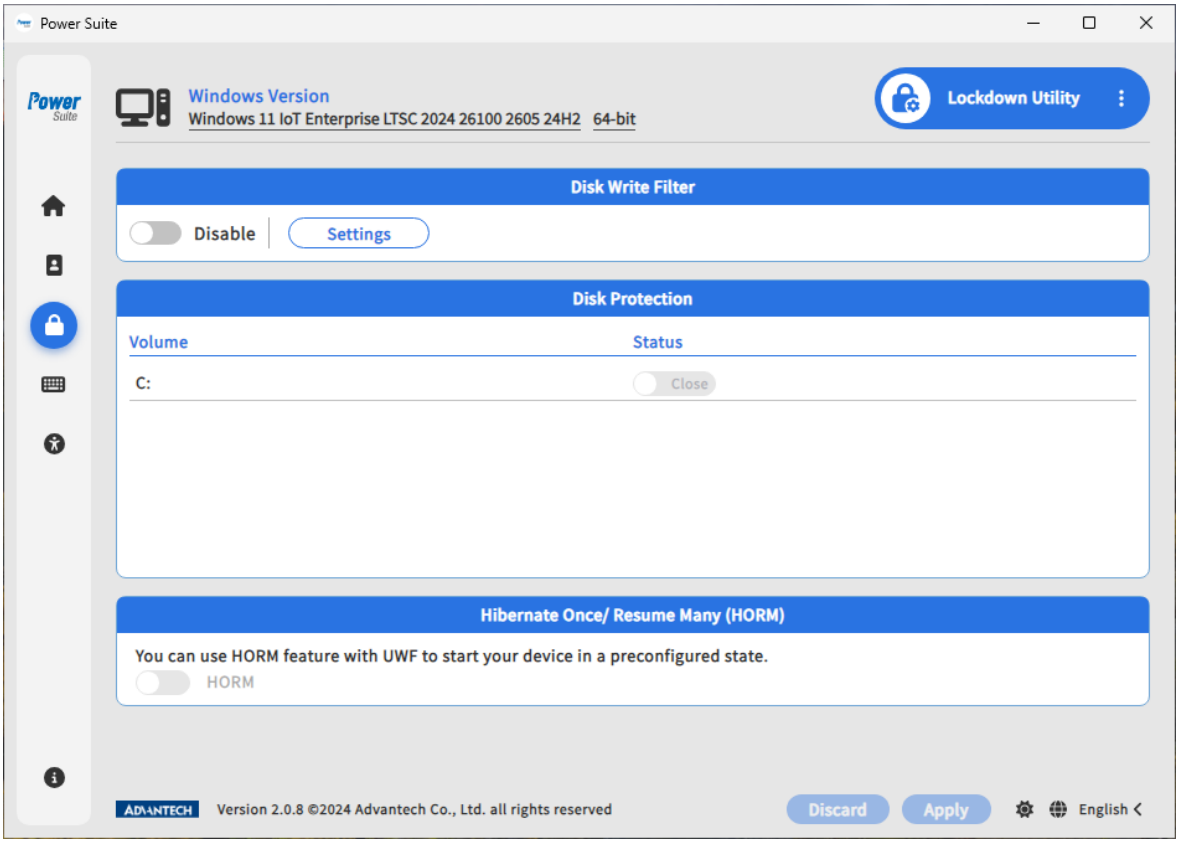
- Advanced Boot Option
  - Advanced Boot Option is designed for image customization to disable Microsoft boot logo and Microsoft lock screen.

5.2.3 Unified Write Filter

The Unified Write Filter (UWF) feature on your device is to help protect your physical storage media. With UWF enabled, your device will become read-only, which protect system from write operations.

To prevent the UWF overlay from running out of space, users are advised to restart the system regularly when UWF is enabled.

Note: Before enabling “Disk Write Filter”, be sure to remove all USB storages from the device to prevent UWF malfunctions or failures.



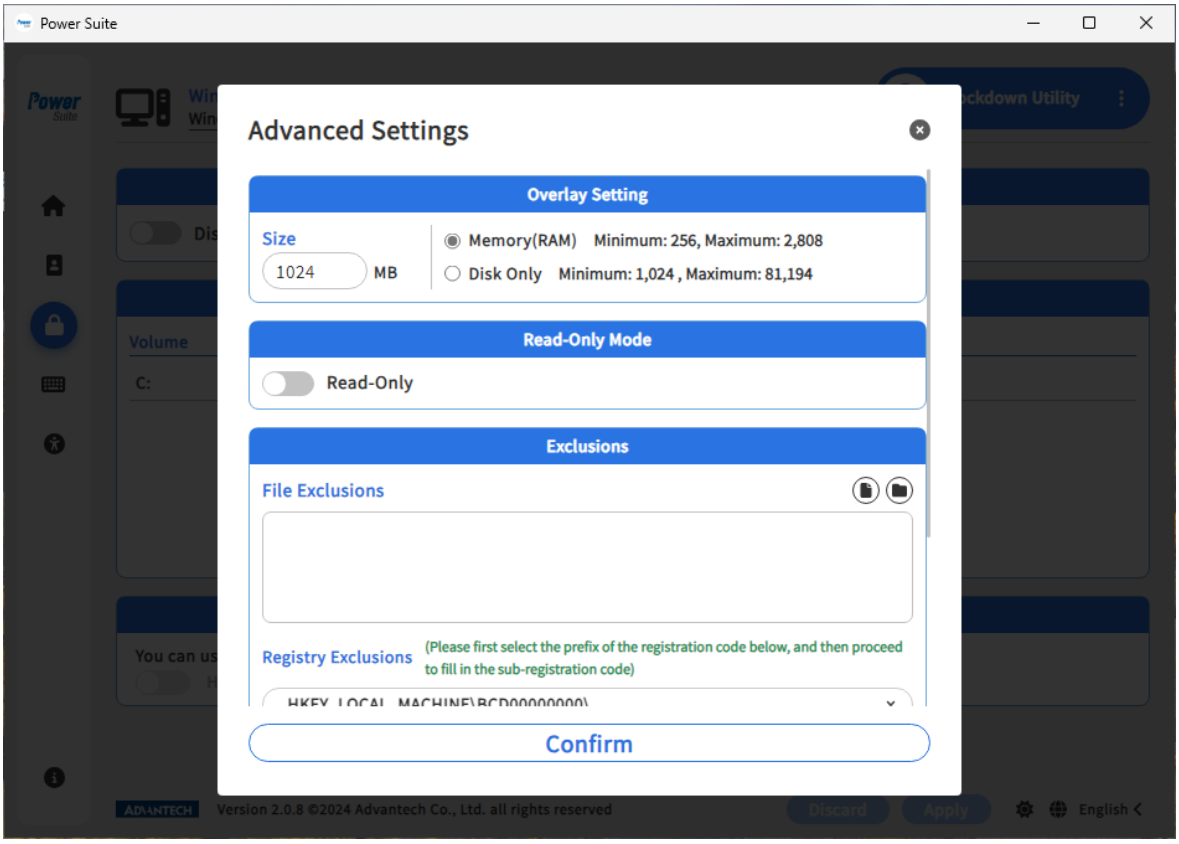
- Disk Write Filter

  After enabling Disk Write Filter, you **cannot modify advanced settings** because of dependency. The Advanced Settings include overlay setting and exclusions.

  More information is available at:

  - Unified Write Filter (UWF) overlay location and size
  - Write filter exclusion

Since the system will be in read-only mode, all the changes would be saved in a virtual overlay. You could decide where the virtual overlay to be saved, in RAM or in Disk. You could also decide which files/directories are exclusive from protection via below Windows.



- Disk Protection

  "Disk Write Filter" must be enabled before you can configure this section. This area lists all volumes on the device. If you want to use Disk Write Filter, it's necessary to indicate which volumes you would like to protect.

  Be aware that you CANNOT use UWF to protect external removable drives, USB devices or flash drives.

  More information is available at: Unified Write Filter (UWF) feature (unified-write-filter)

- HORM

  Hibernate Once/Resume Many helps to quickly turn off or shut down your system, and then restart into the preconfigured state, even in the event of a sudden power loss. When HORM is enabled, your system always resumes and restarts from the last saved hibernation file (hiberfil.sys).

  If you would like to activate HORM, Hibernate function must be enabled in advance. You can enable it through OS Enhancement Utility or Windows Control Panel.

  UWF must be enabled before you can enable HORM. UWF must be configured in the following ways to protect the hibernation file from becoming invalid:

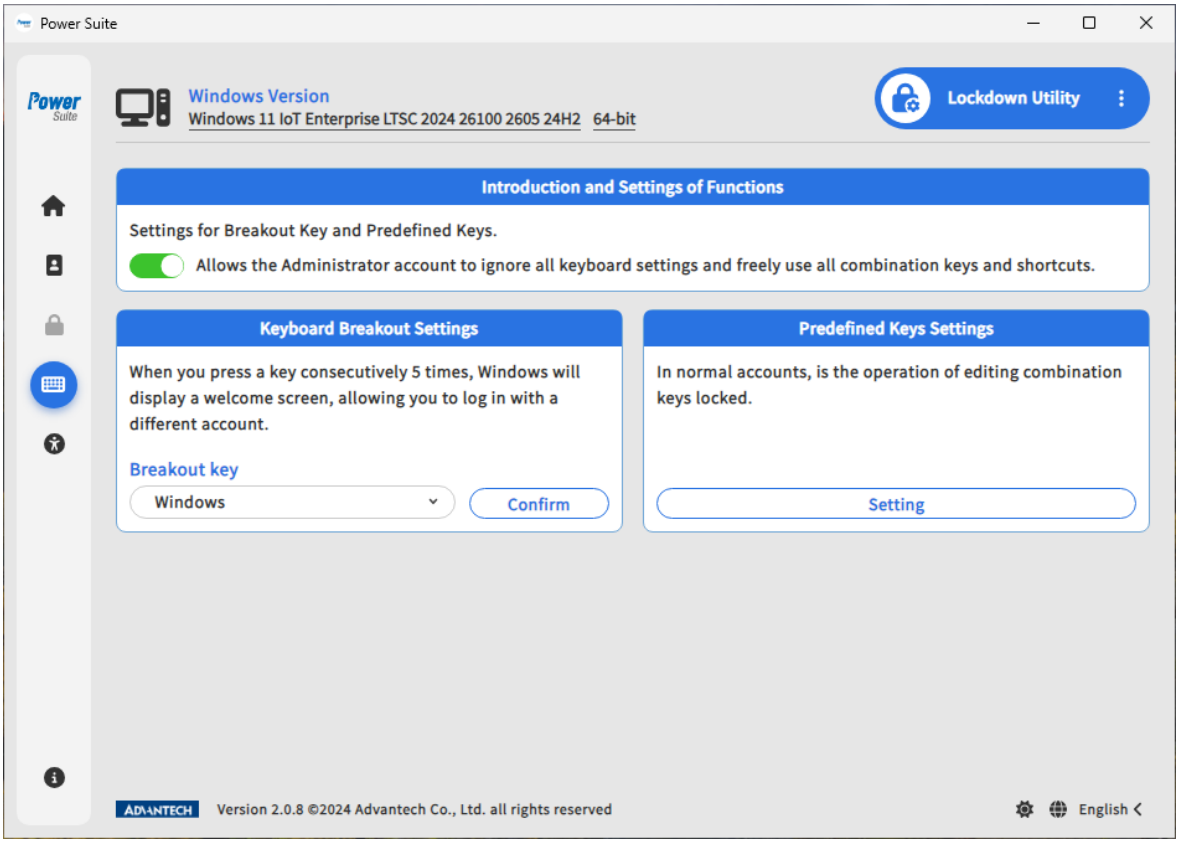
  I. The UWF overlay must be configured to use RAM mode. HORM does not support disk overlay.
  II. Enable Read-Only in Advanced Settings
  III. No file, folder, or registry exclusions configured for UWF.

  More information is available at: Hibernate Once/Resume Many (HORM)

  Note 1: HORM can be worked on a UEFI device when your Win 10 IoT Enterprise version is 1709 or newer, otherwise only Legacy. If you cannot use HORM, please try to make your windows update to the latest.

  Note 2: Once the system enters into Hibernate with HORM enable, the next HORM enable action will resume from the previous Hibernate status.

5.2.4 Keyboard Filter



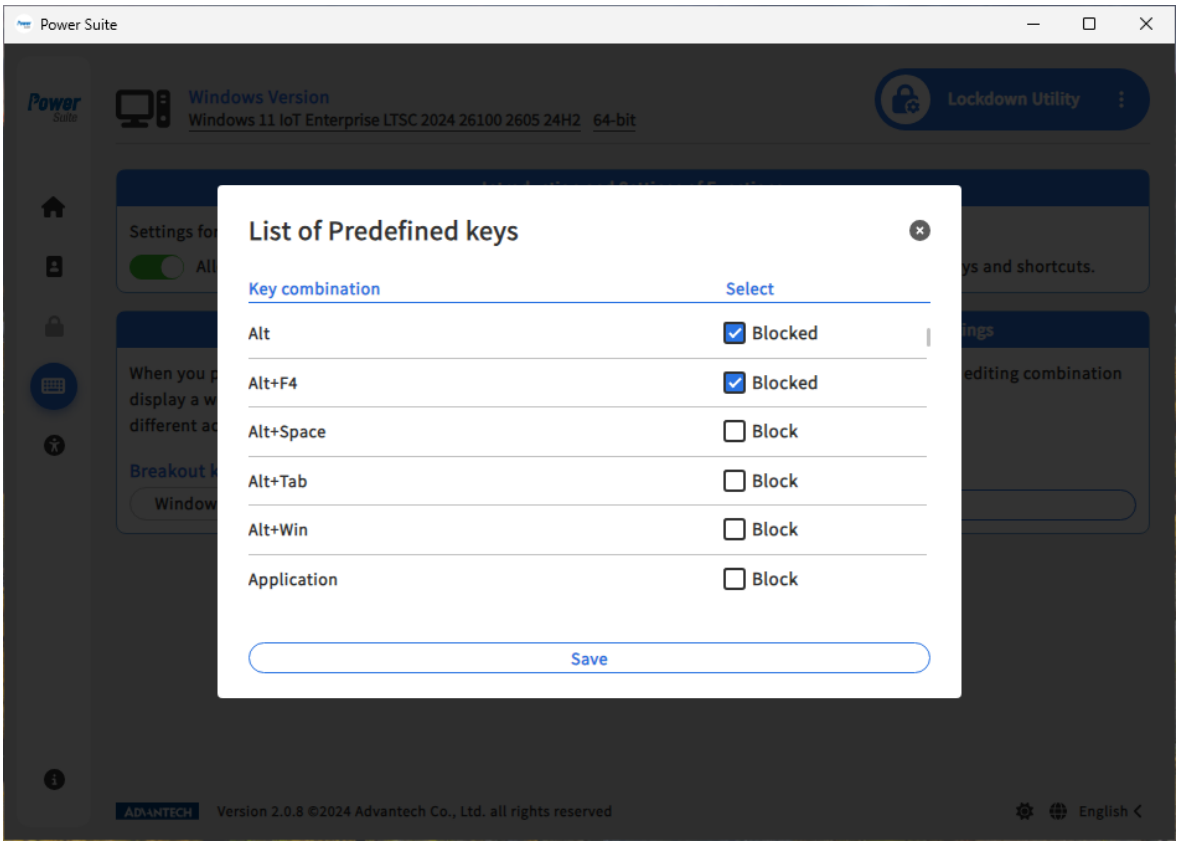
- Introduction and Settings of Functions
  Enable the setting to avoid being restricted keyboard use under administrator account.

- Keyboard Breakout Settings
  You can configure a breakout key sequence to switch out a locked down account by specifying a key scan code. When you press the Breakout Key 5 times consecutively, Windows presents the Welcome screen so that you can sign in to a different account.

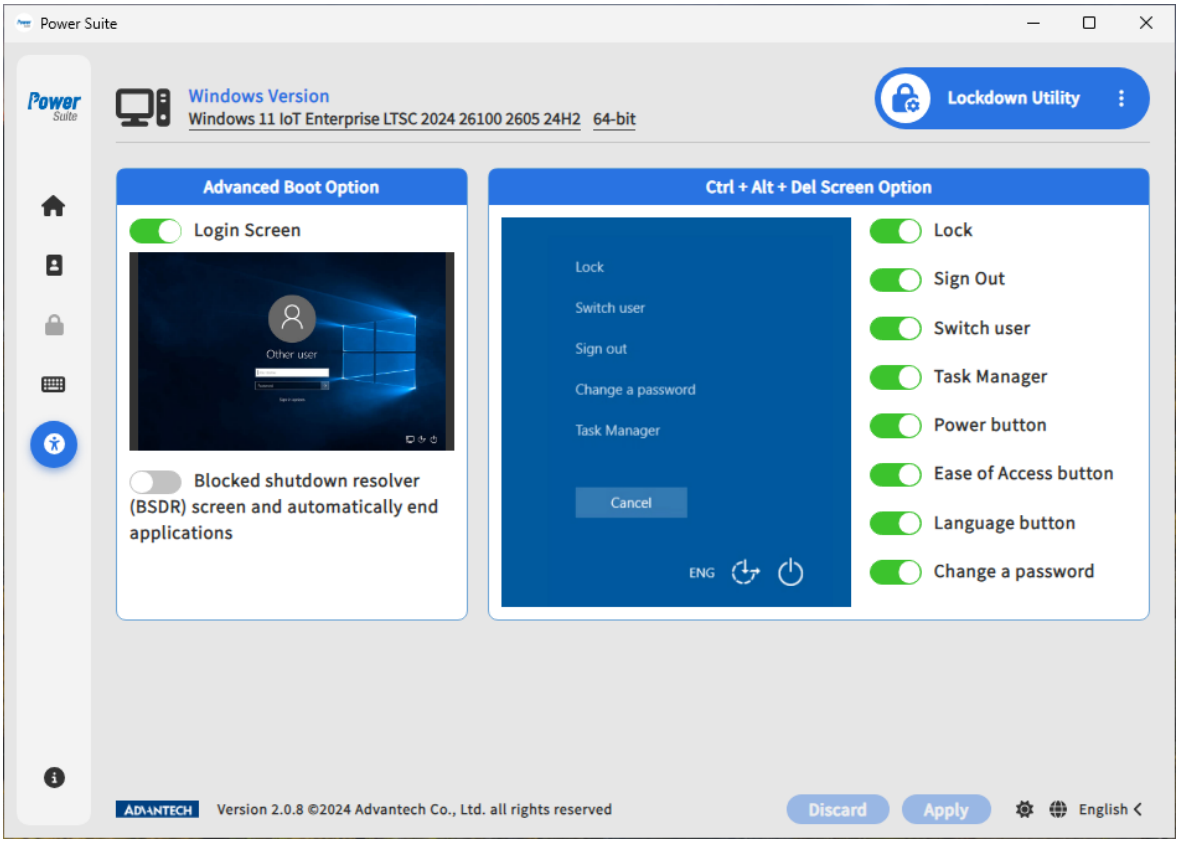
- Predefined Keys Settings

  We provide predefined keys which are defined by Microsoft.

  The default setting is to allow all of the predefine keys. If you want to block keys for your users, check the items that you want to block, and click "**Save**". The selected key combinations will be blocked.



5.2.5 Embedded Logon



- Advanced Boot Option

  You can hide logon screen by disabling “Login Screen”. Before configuring this setting, you must enable auto login in advance, which can be set on the “Automatic Logon and Boot Options” menu.

  When the BSDR screen is enabled, any open applications that blocking system from restarting or shutting down would be close immediately. No UI will be displayed to check again whether you are sure to restart system, and users are not given any chances to cancel the shutdown process. This action will result in losing data if there are any unsaved data.

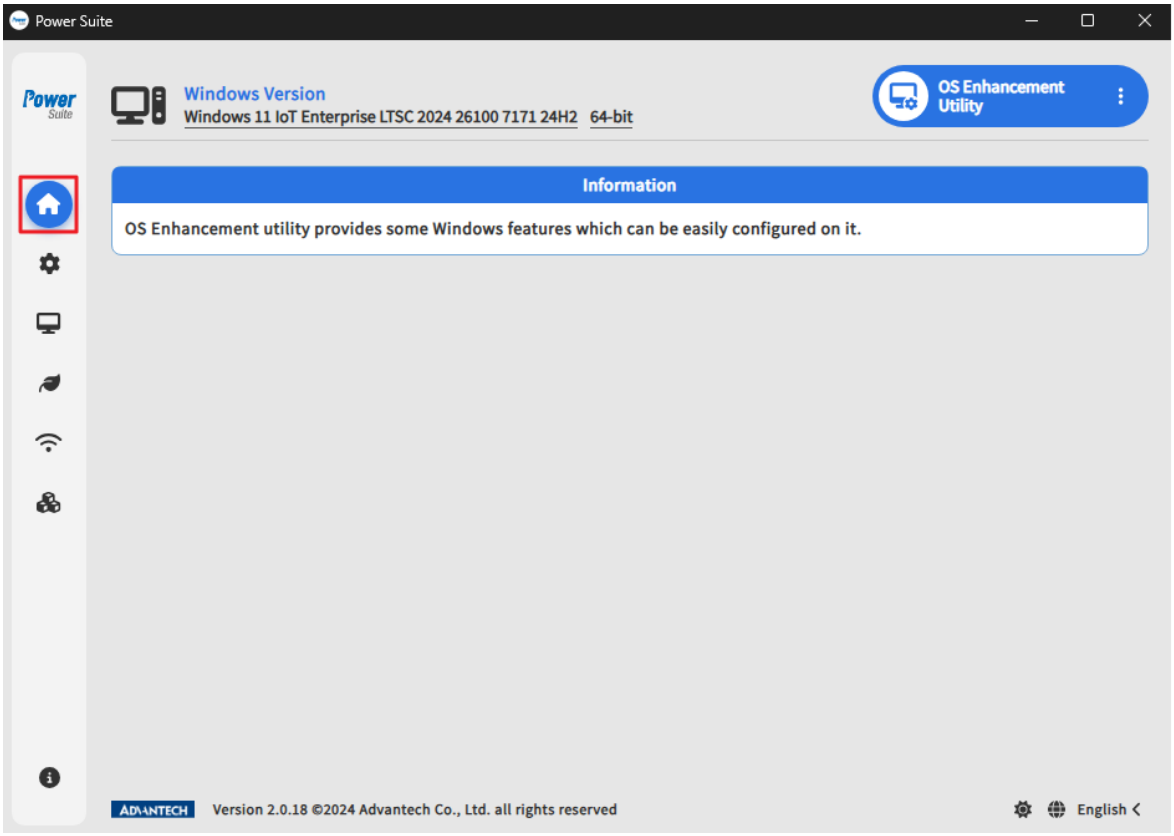
- Ctrl + Alt + Del Screen Option

  You can configure Ctrl + Alt + Del options to customize what kind of function to be run under the combination keys of Ctrl, Alt, and Del.

5.3 OS Enhancement Utility

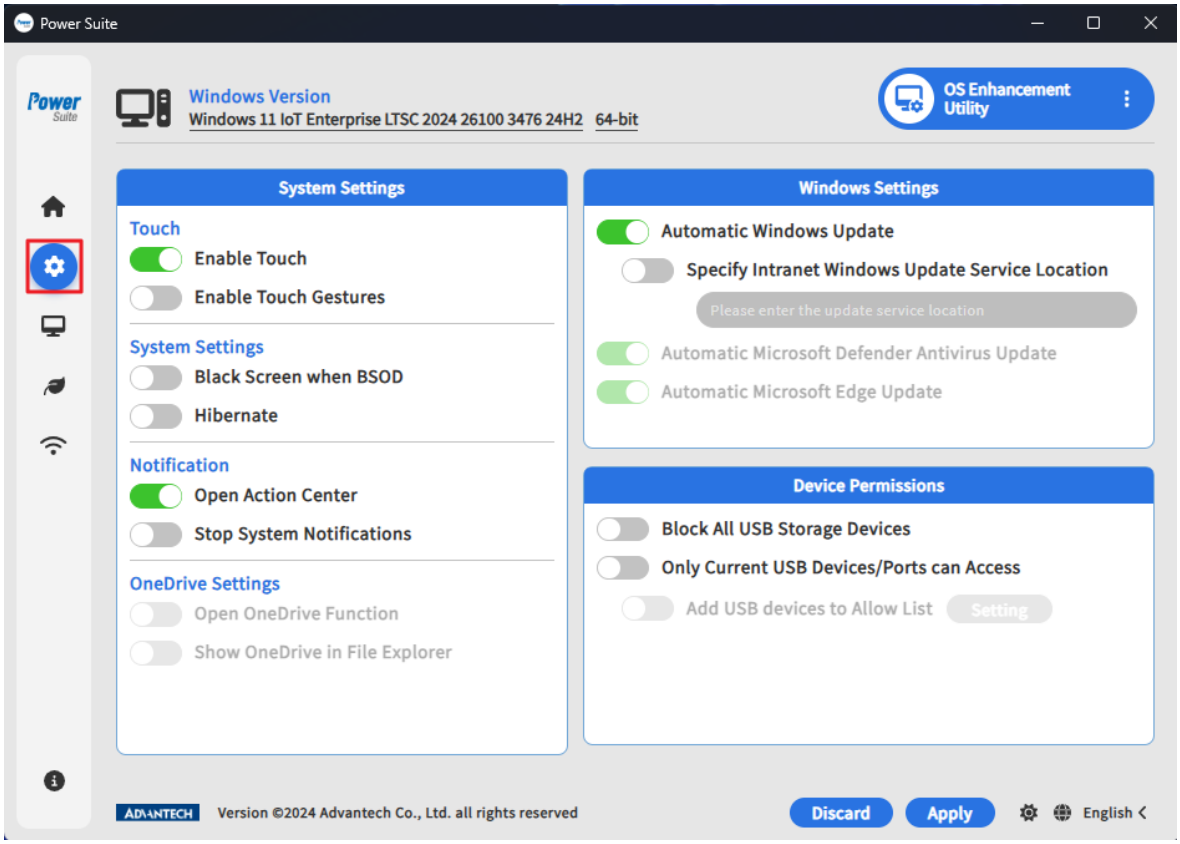
5.3.1 Information

Basic function description of the OS Enhancement Utility.



5.3.2 General Settings

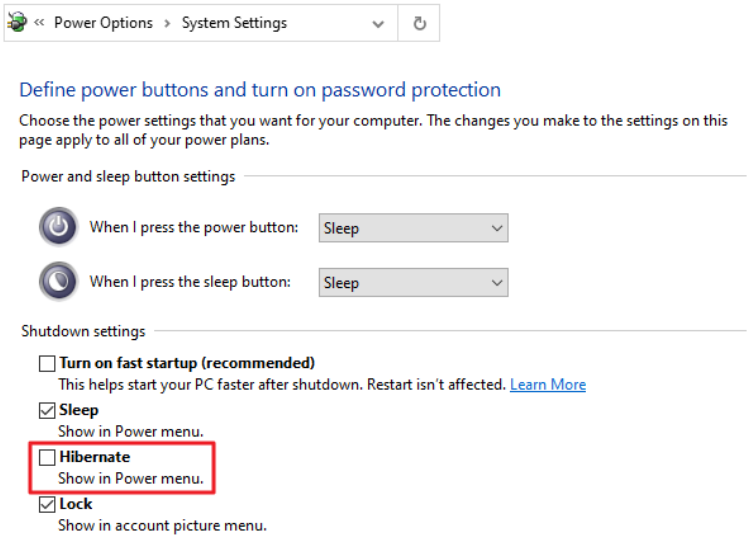
Provide interfaces that allow users to quickly configure frequently used Windows settings.



➢ System Settings

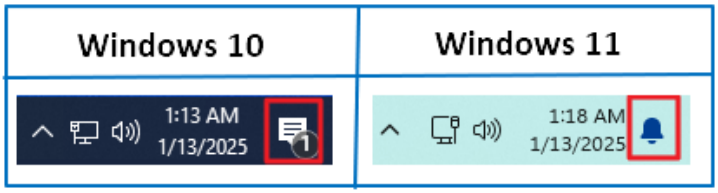
- Touch
  - **Enable Touch**: enable or disable touch function (only support capacitance touch device)
  - **Enable Touch** Gestures: enable or disable touch gestures

- System Settings
  - **Black screen when BSOD**: after enable this feature, screen will display black screen when system occurs BSOD instead of blue screen
  - **Hibernate**: enable to show hibernate option in showdown settings menu

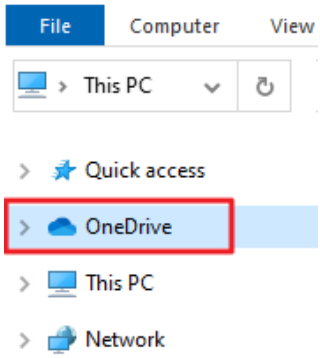


- Notification
  - **Open Action Center**: enable to show action center on task bar

  - **Stop System Notifications**: enable/disable to suppress/show system notifications

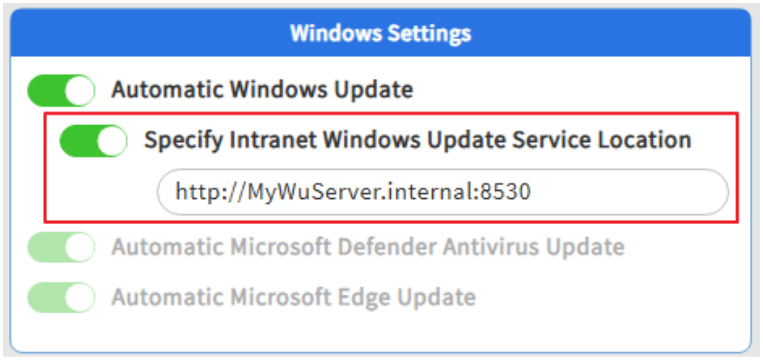


- OneDrive Settings
  - **Open OneDrive Function**: enable or disable OneDrive function
  - **Show OneDrive in File Explorer**: enable to show OneDrive node in file explorer

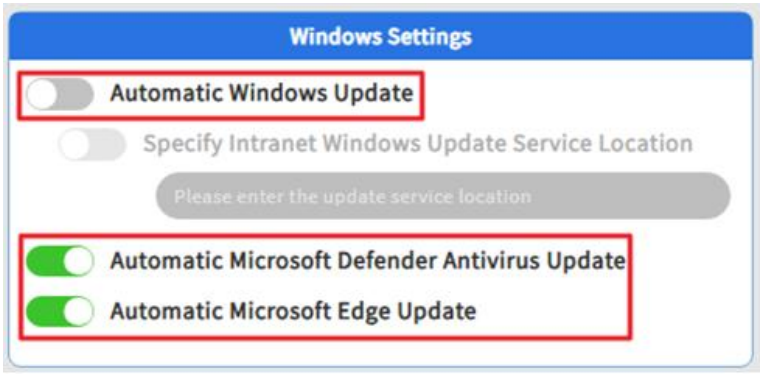


➢ Windows Settings

- **Automatic Windows Update**: enable or disable automatic Windows updates
  - **Specify Intranet Windows Update Service Location**: enable to assign an intranet URL as new Windows update location if A**utomatic Windows update** is enabled

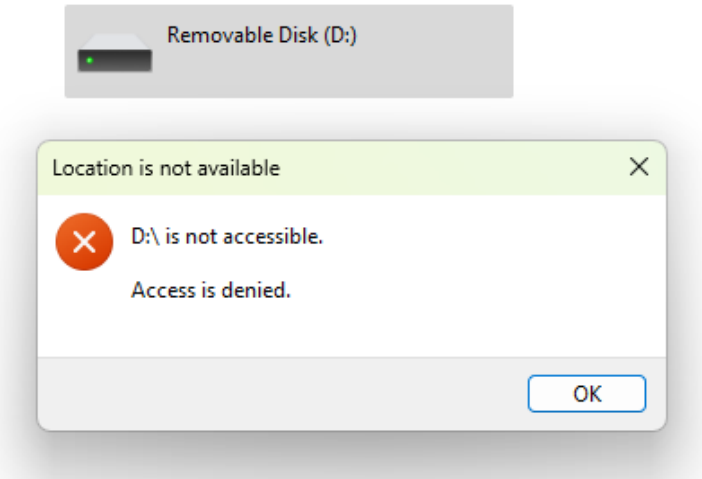


- **Automatic Microsoft Defender Antivirus Update**: turn ON this option to allow Microsoft Defender Antivirus to remain up to date even when **Automatic Windows Update** is disabled. This setting is forcibly enabled when **Automatic Windows Update** is turned on.
- **Automatic Microsoft Edge Update**: turn ON this option to keep Microsoft Edge Browser up to date even when **Automatic Windows Update** is disabled. This setting is forcibly enabled when **Automatic Windows Update** is turned on.

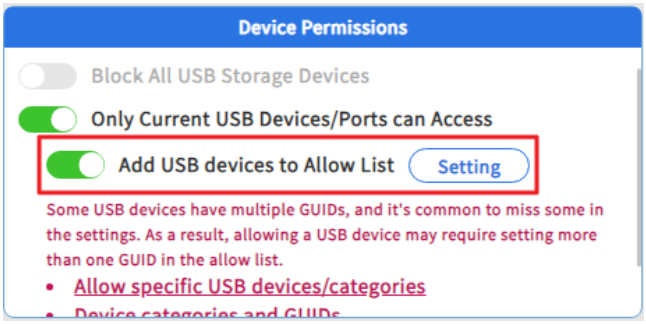


➢ Device Permissions

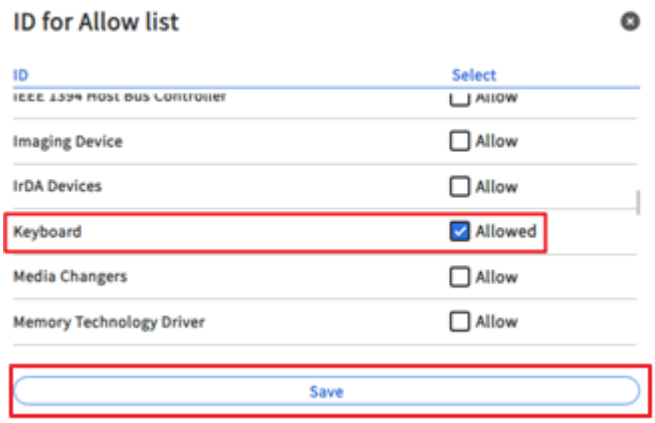
- **Block All USB Storage Devices**: Enable to block all USB storage devices, including read, write, and execute permissions



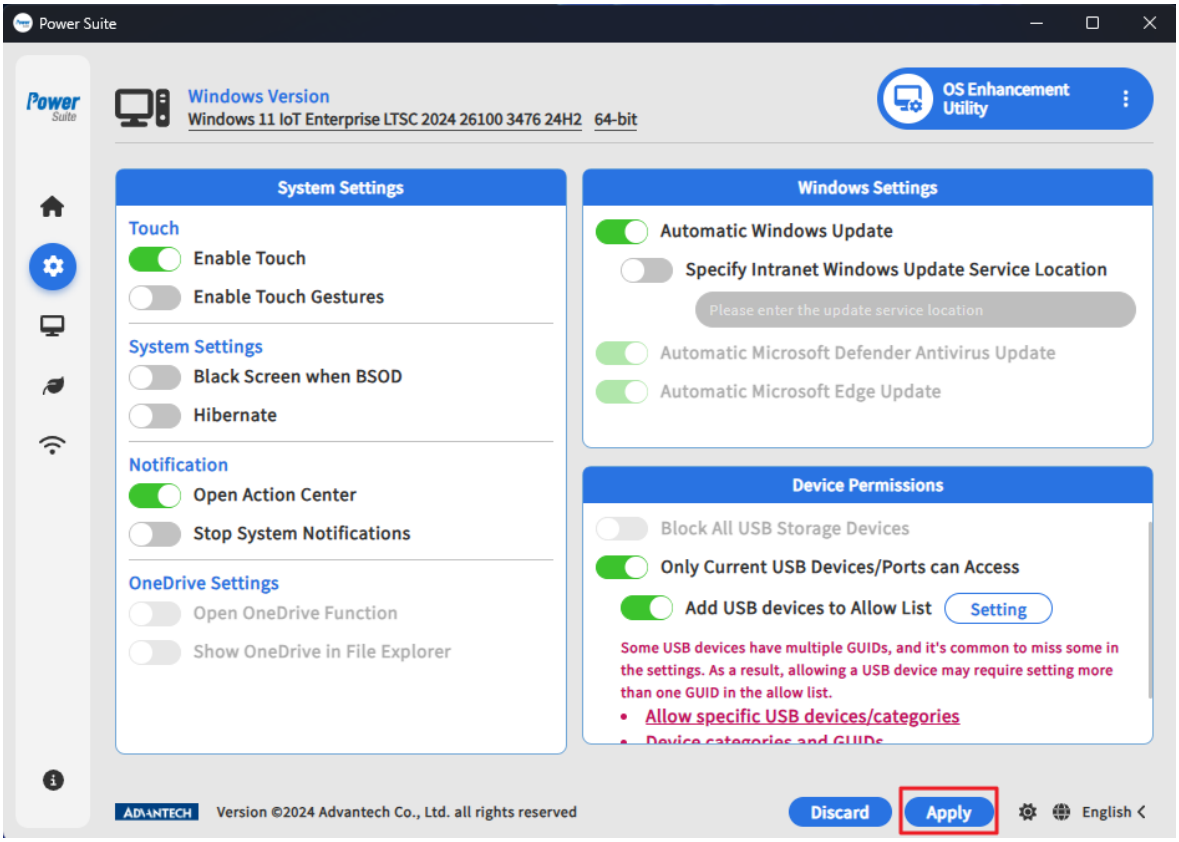
- **Only Current USB Device/Port can Access**: this is a device-based feature. If enabled, only the USB devices that had working in this computer could work, and no other USB devices could work further.
  For example, if only USB keyboard-A is already recognized by this computer, after enabling this feature, no other USB keyboards could work in this computer unless the device ID is added to the allow list.
  - **Add USB devices to Allow List**: users add device IDs into the allow list to make sure the selected device types still work on this computer while **Only Current USB Device/Port can Access** is enabled.
    For example, if a user can apply following steps to use another keyboard:
    1. Enable **Add USB devices to Allow List**
    2. Click "**Setting**" button to open dialog



3. Select all required device IDs (state from “Allow” to “Allowed”)
4. Click “**Save**” button to close dialog



5. Click “**Apply**” button to finish setup and reboot device

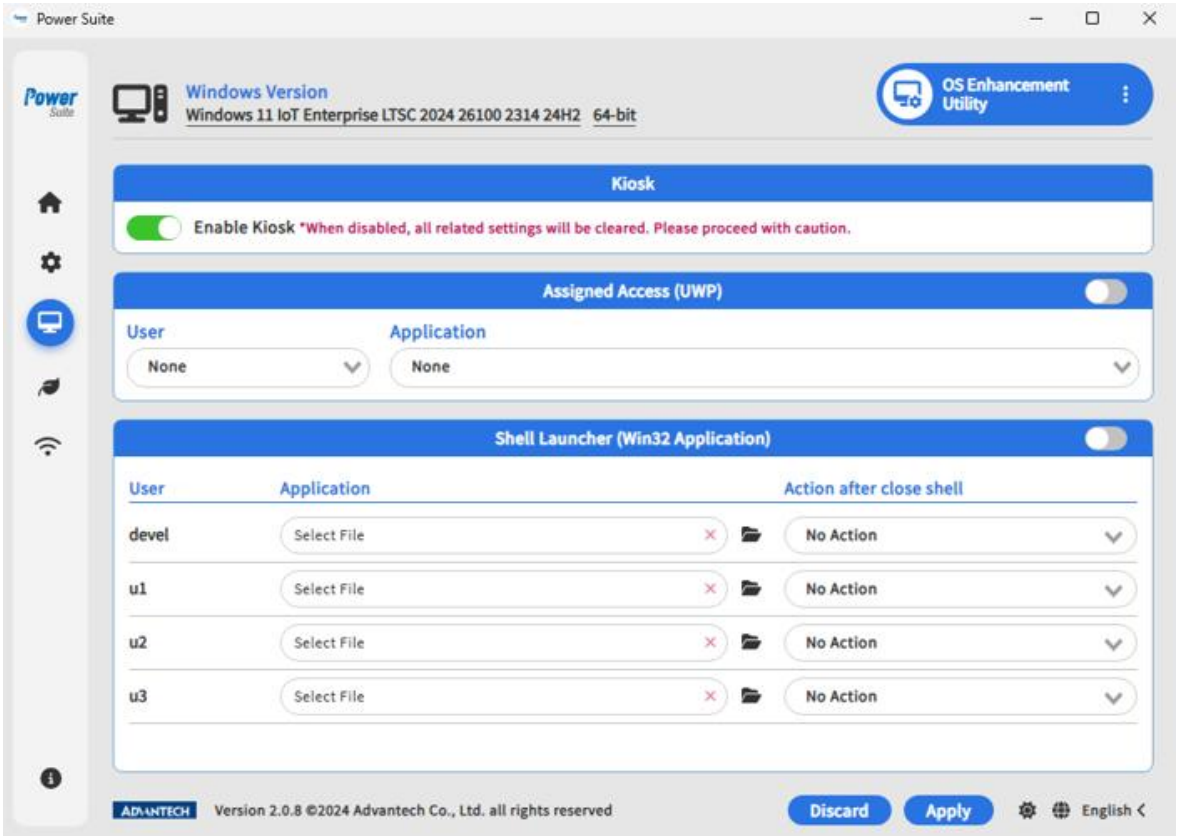


Note: add a device type may need selecting multiple class IDs from allow list.

For example, if a user wants to add new keyboard devices, in addition to the Keyboard ID, the Human Interface Device (HID) ID is also required to make the Keyboard ID effective.

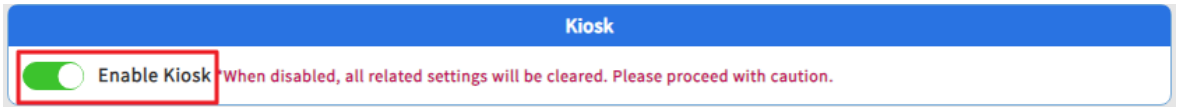
5.3.3 Kiosk

Kiosk mode is a common way to lock down a Windows device while the device is used for a specific task or used in a public setting.



➢ Kiosk

- **Enable Kiosk**: enable or disable kiosk feature



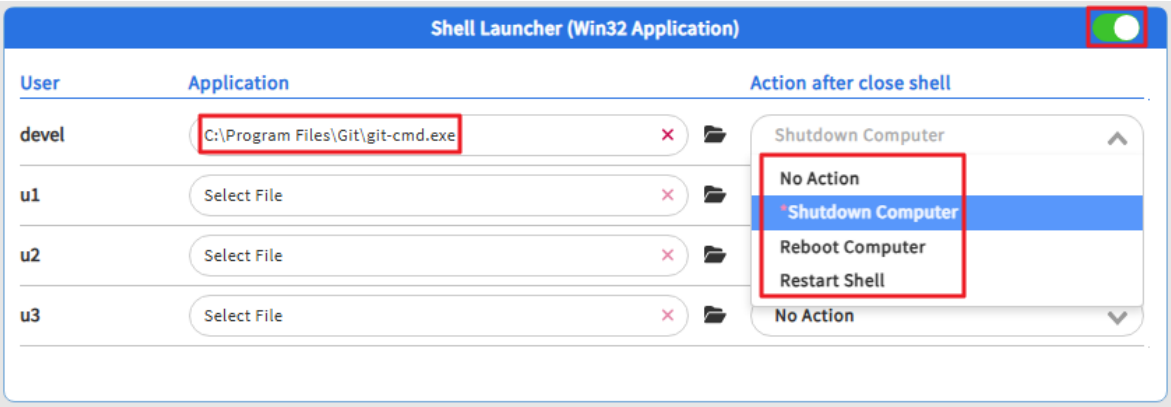
Note: all current kiosk settings will be purged if the toggle is set to disable and applied

➢ Assigned Access (UWP)

- **Assigned Access (UWP)**: set enable to launch the selected UWP application when the selected user logs on
  - **User**: select a local account other than current user
  - **Application**: select an UWP application

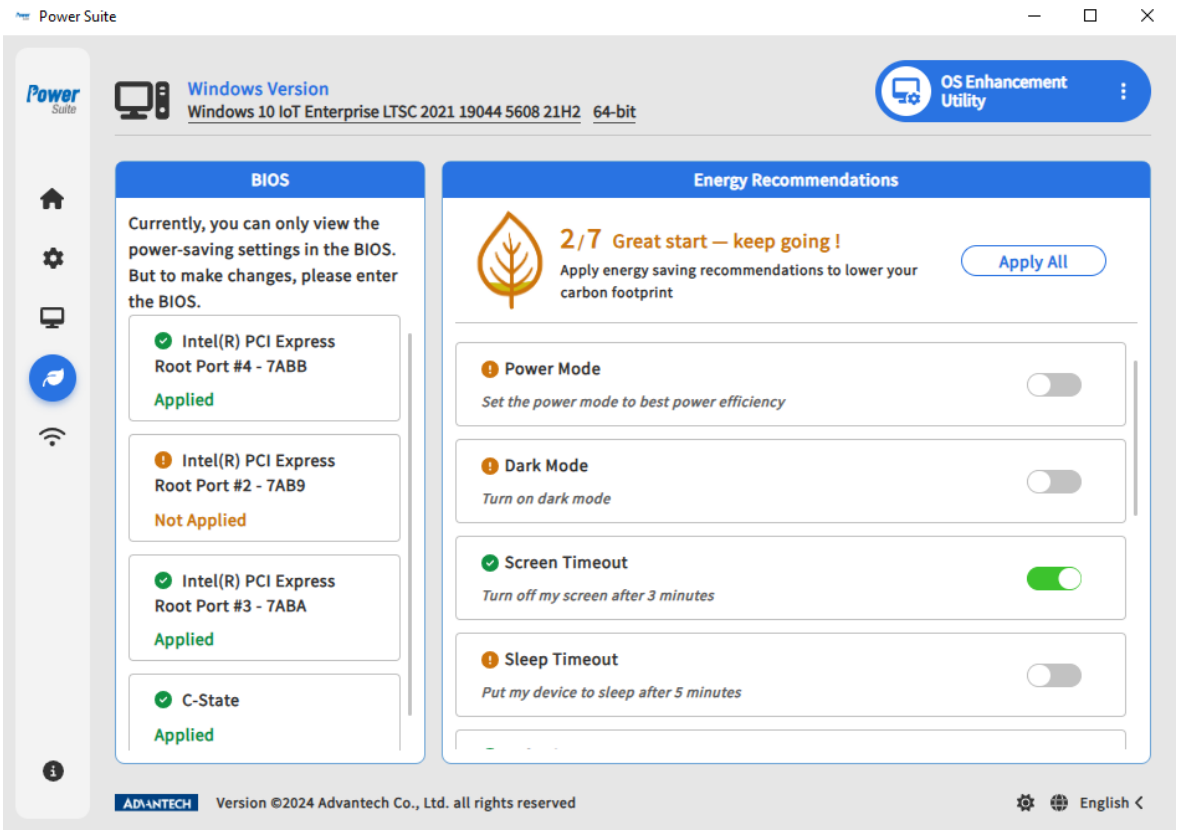
➢ Shell Launcher (Win32 Application)

- **Shell Launcher (Win32 Application)**: set enable to launch the selected Win32 application when the corresponding user logs on
  - **Application**: select a Win32 application to be launched when the user logs on
  - **Action after close shell**: choose the action to take if the selected Win32 application is terminated. Available actions are: No Action, Shutdown Computer, Reboot Computer, and Restart Shell.



5.3.4 Energy

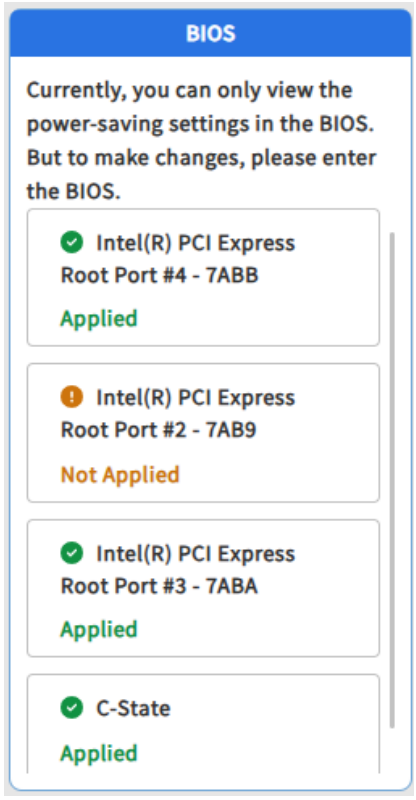
Collect settings that have an impact on power consumption. By apply recommendation values, user can reduce power use, improve battery life and lower the carbon footprint.



Note: utility tries to read some information using Advantech SUSI APIs. This means that the status will show “No Data”, “Not Available”, or “Not Support” if Advantech SUSI package is not installed on the device.

➢ BIOS

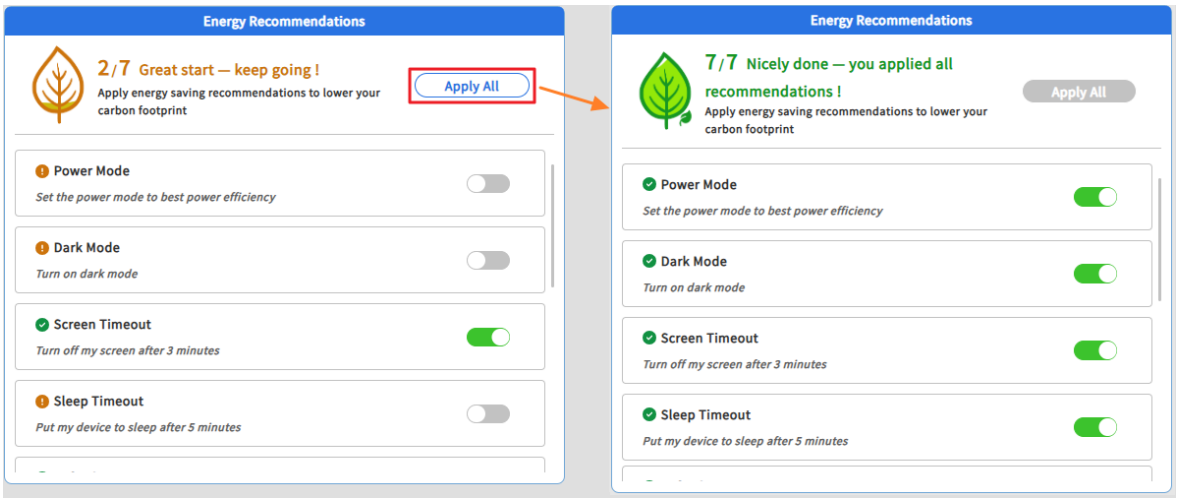
- Display current status of BIOS energy recommendation settings. These values are read from BIOS and can't be modified by utility.



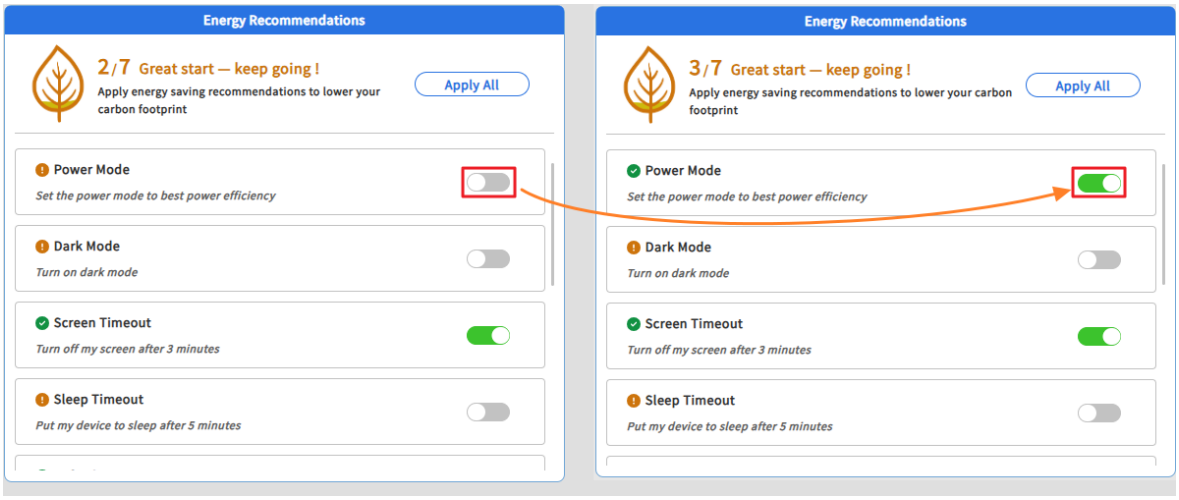
Note: specific Intel CPUs are supported at this time. This feature is not available for all platforms/products.

➢ Energy Recommendations

- Click "**Apply All**" button to automatically apply recommended values to all items.

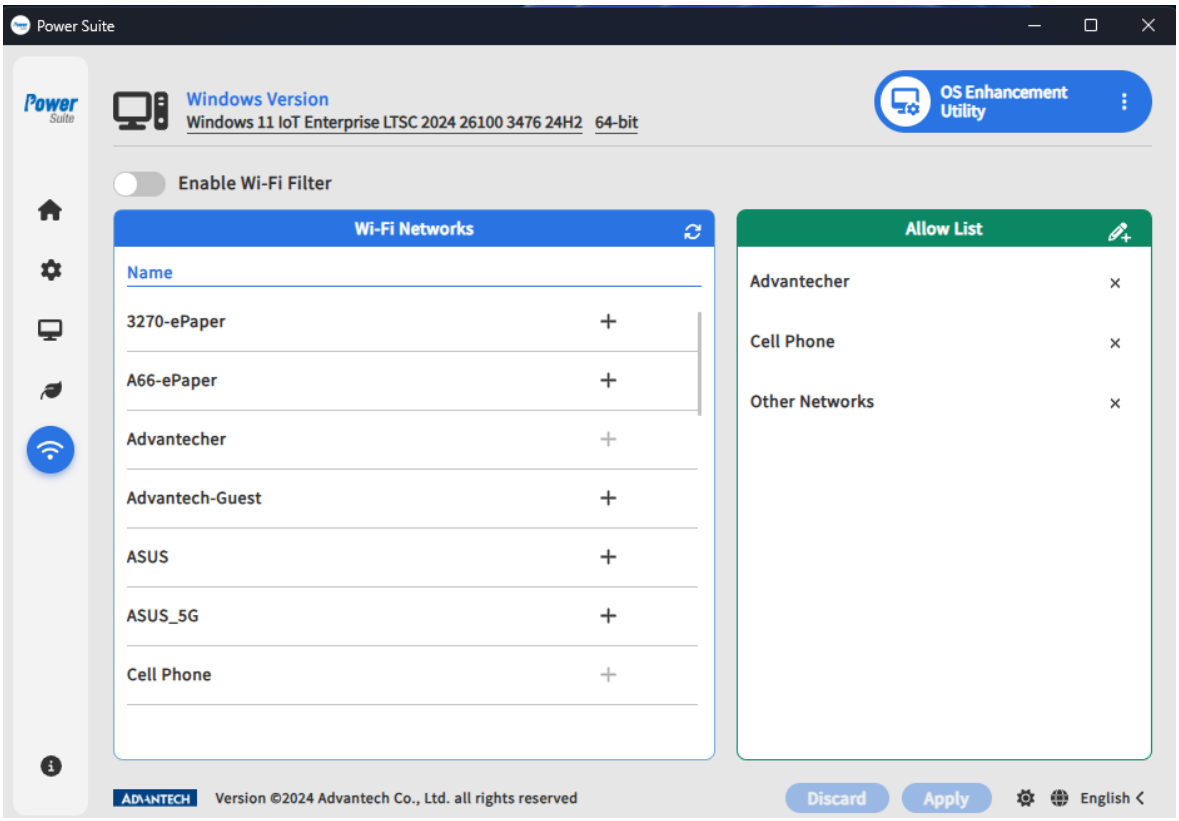


- Click the toggle to enable or disable individual power-saving features.



5.3.5 Wi-Fi Filter

Windows displays a list of available Wi-Fi network names (SSIDs). Users may want to ensure that corporate devices within corporate premises connect only to specific networks. The Wi-Fi Filter allows users to connect only known wireless networks in the available Wi-Fi networks list, hiding any network names that are not in the allowed list.



Note: SSIDs with emojis or Unicode characters are unsupported and will be hidden from the available list

➢ Enable Wi-Fi Filter

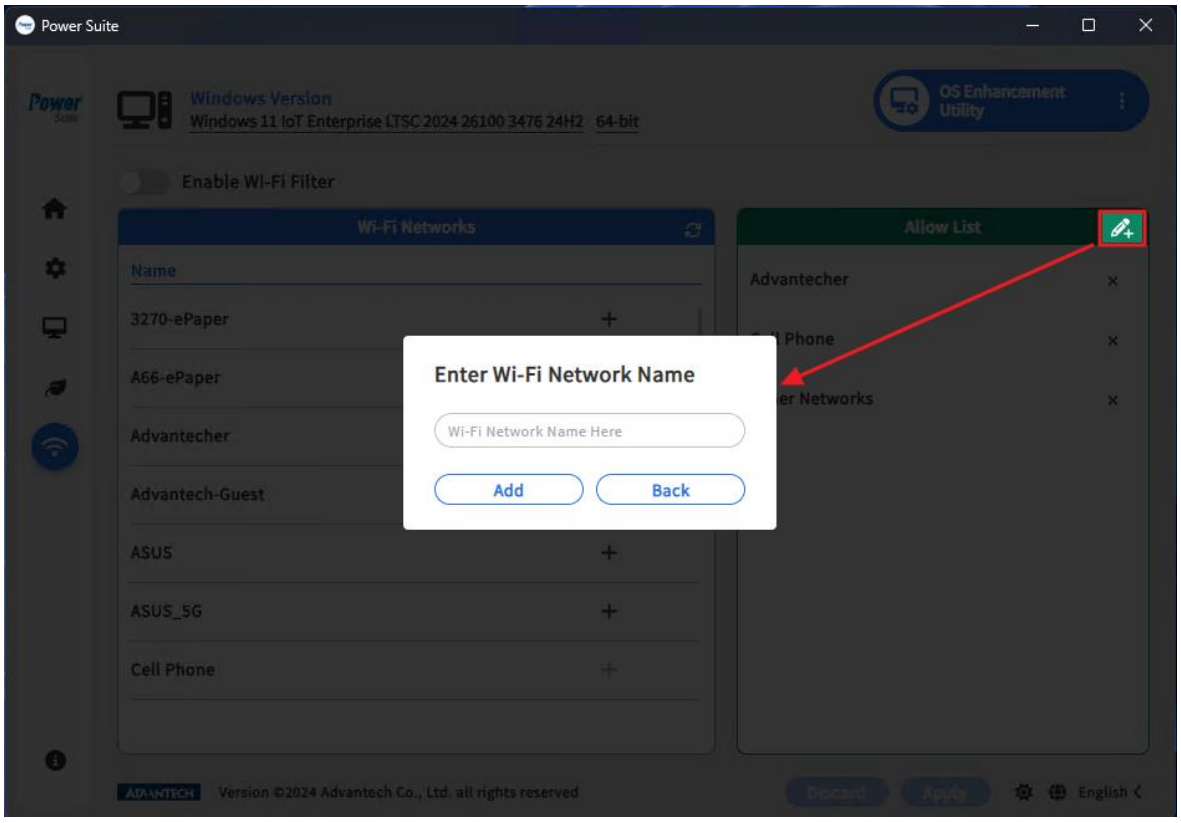
- **Enable Wi-Fi Filter**: enable or disable Wi-Fi filter.

➢ Wi-Fi Networks

- The list of available **Wi-Fi Networks**
- Click icon to refresh available **Wi-Fi Networks**
- Click + icon to add the network name to **Allow List**
- If Wi-Fi filter is enabled, only network names in **Allow List** are available.

➢ Allow List

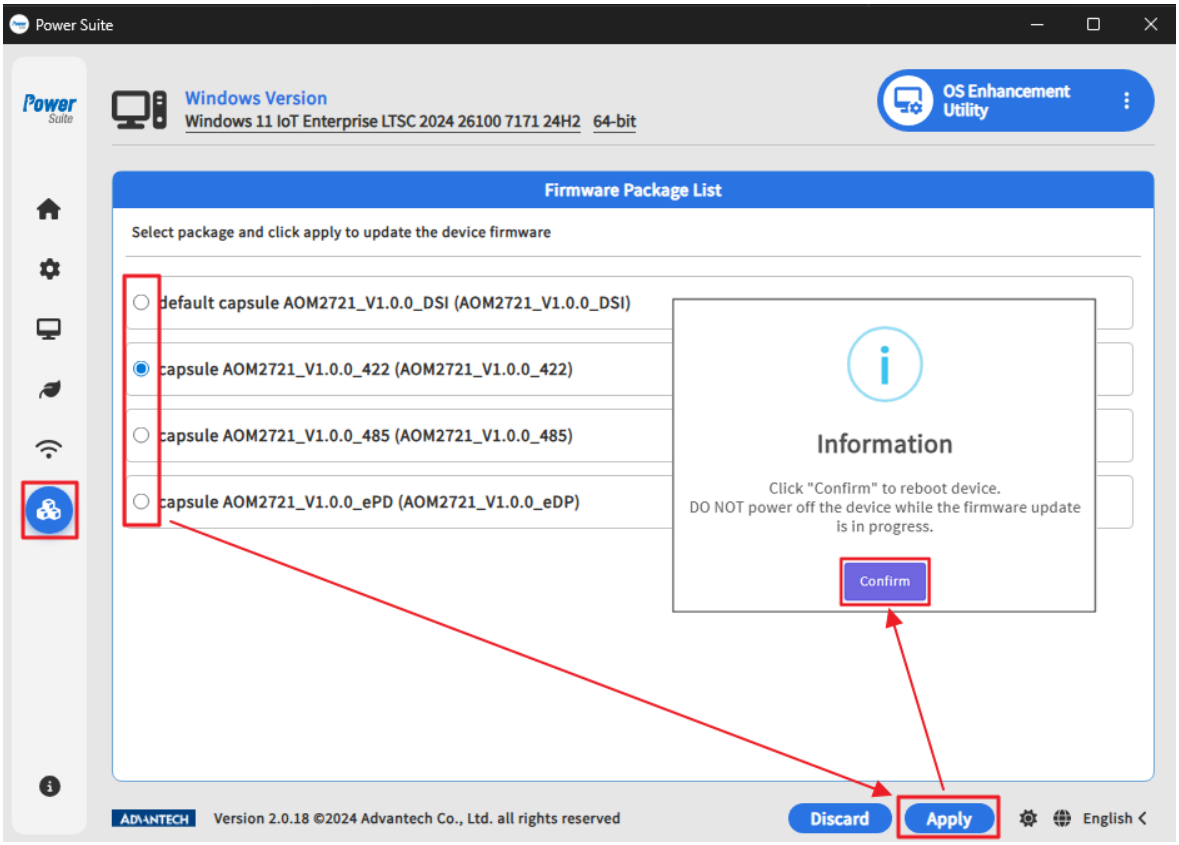
- The list of network names that already added to **Allow List**
- Click ✕ icon to remove the network name from **Allow List**
- Click icon to manually add SSID to **Allow List**
  - Type network name in the text field (only accepts allowed characters)
  - Click "**Add**" to add network name to **Allow List**
  - Click "**Back**" to close the dialog



After all items are configured, be sure to click the "**Apply**" button to save the settings or click the "**Discard**" button to restore them.on

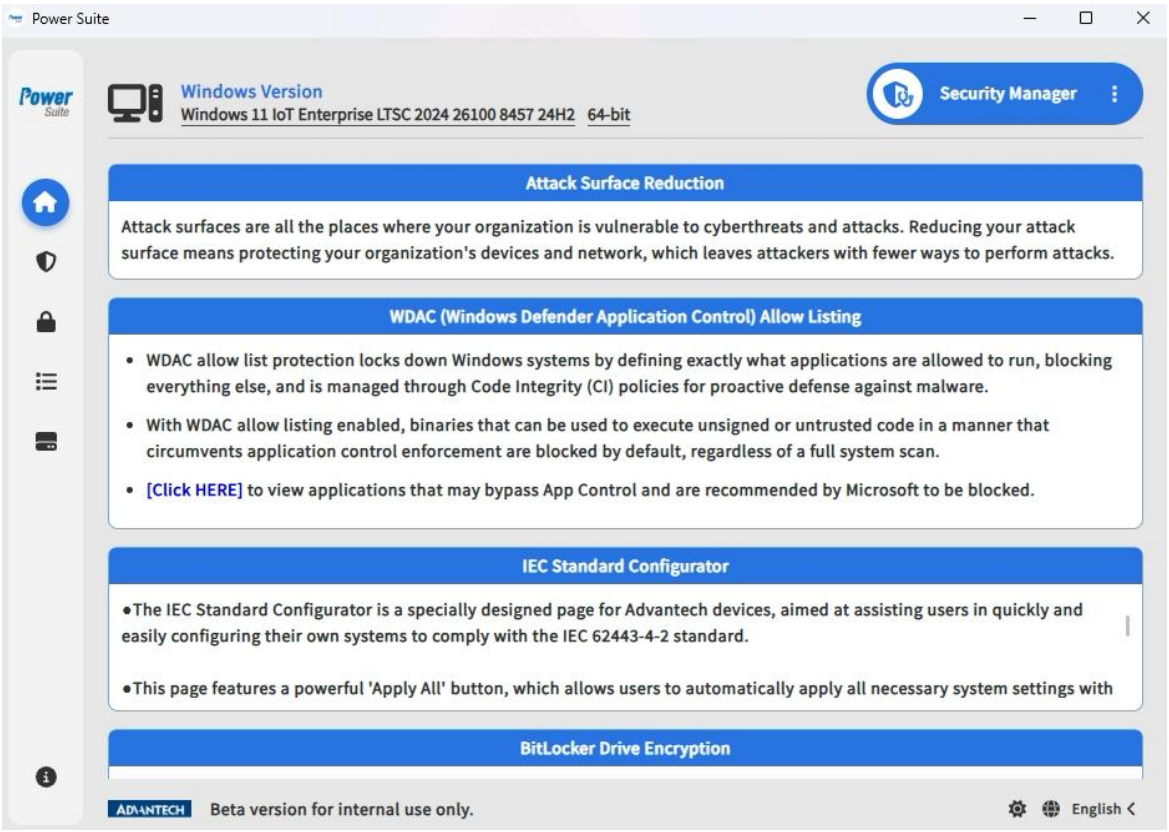
5.3.6 Firmware Update (WoA devices only)

This feature is only available on WoA devices. All firmware packages are protected with AES-256 encryption and saved in a specific folder. After selecting the desired firmware package and clicking “Apply,” Windows delivers the package to the device and automatically installs it during the next reboot. This ensures that important system components stay up to date for improved stability and performance.



5.4 Security Manager

5.4.1 Information



➢ Attack Surface Reduction Feature Introduction

Attack Surface Reduction (ASR) refers to a collection of controls introduced by Microsoft to restrict common malware and exploit techniques on Windows endpoints. These controls target software behaviors that are frequently exploited by attackers. By enabling or disabling ASR rules, organizations can constrain these risky behaviors and enhance their overall security posture.

➢ IEC Standard Configurator Feature Description

The IEC Standard Configurator is a specially designed page for Advantech devices, aimed at assisting users in quickly and easily configuring their own systems to comply with the IEC 62443-4-2 standard.

This page features a powerful 'Apply All' button, which allows users to automatically apply all necessary system settings with one click. This ensures that the device meets the security standards as declared by Advantech. Not only does this save a significant amount of time and effort, but it also reduces the risk of configuration errors, greatly enhancing system security. Whether you are an experienced system administrator or a newcomer to Advantech devices, the IEC Standard Configurator helps you effortlessly achieve best practices in system security.

The Advantech IEC 62443-4-2 certification (Verification of Conformity, VoC) report indicates that the Advantech has successfully met 51 standard requirements. Among these, the IEC Standard Configurator provides a quick application function covering 23 items, while the remaining items are either integrated into Advantech's IEC-compliant systems at the factory or require manual configuration by the user. The main reason for requiring the user to manually configure the settings is to avoid overly restrictive cybersecurity configurations when the device reaches the client, which could prevent users from fulfilling other needs. By allowing manual cybersecurity configuration, it provides more flexibility in gradually meeting the IEC 62443-4-2 requirements for the customer.

➢ WDAC (Windows Defender Application Control) Allow Listing

Windows Defender Application Control (WDAC) is a robust security feature in Microsoft Windows 10/11 that creates a strict "allow list", permitting only authorized code, executables, and drivers to run. It mitigates malware by default, requiring policies based on file hash or publisher certificates.

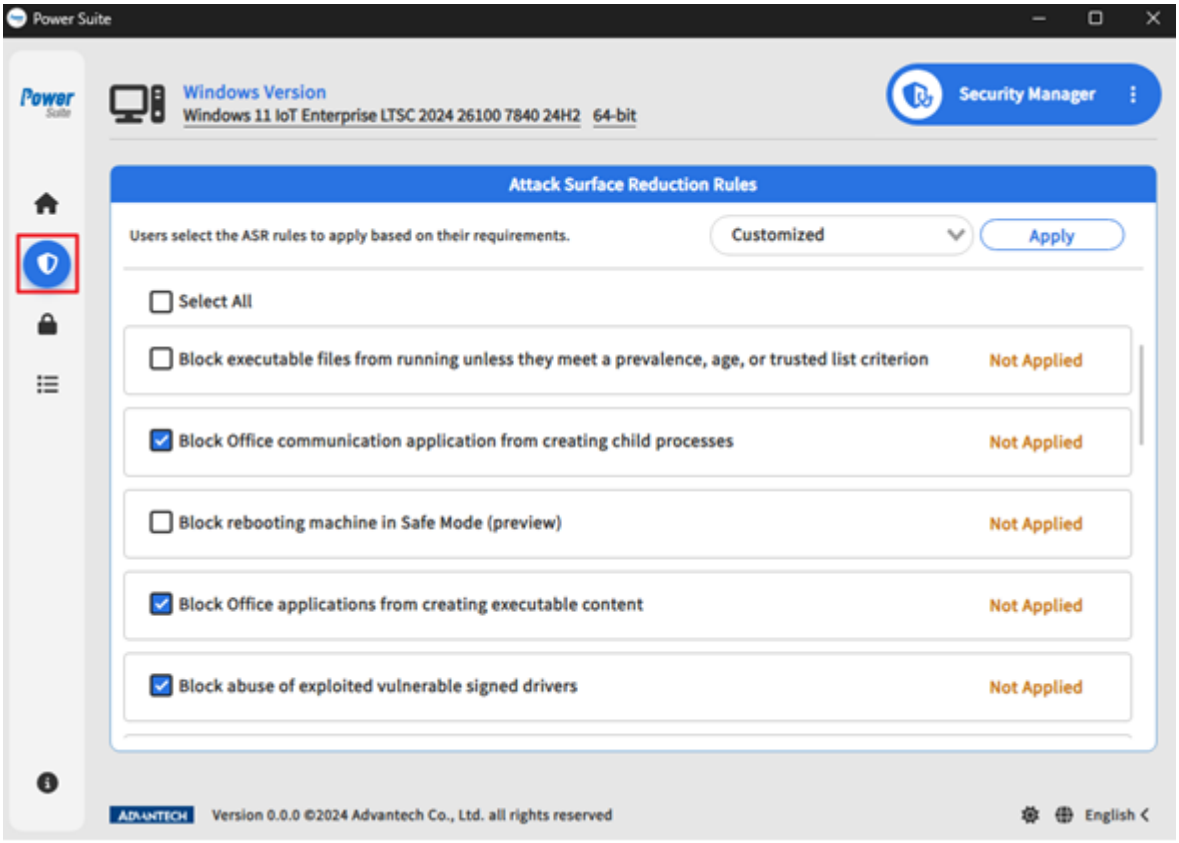
Unless explicitly required for specific use scenarios, Microsoft recommends blocking applications that can be used to execute unsigned or untrusted code in ways that circumvent application control enforcement, regardless of whether they are included in the allow list. For more information, take a look at: Applications that can bypass App Control

➢ BitLocker Drive Encryption

BitLocker is a full volume encryption feature included with Microsoft Windows. It is designed to protect data by providing encryption for entire volumes.

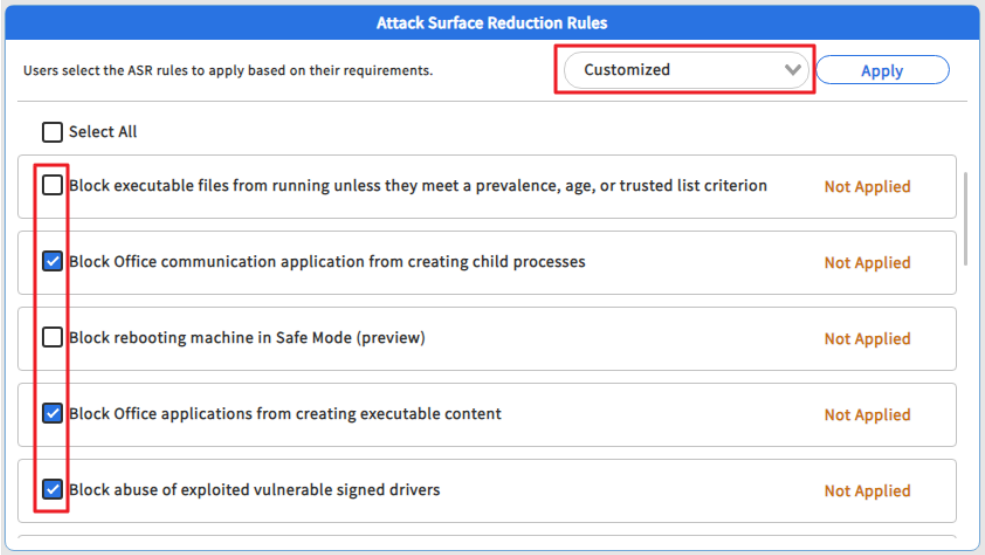
By encrypting the entire drive that Windows and your data reside on, BitLocker can help prevent unauthorized users from tampering with the system and from accessing your data."

5.4.2 Attack Surface Reduction

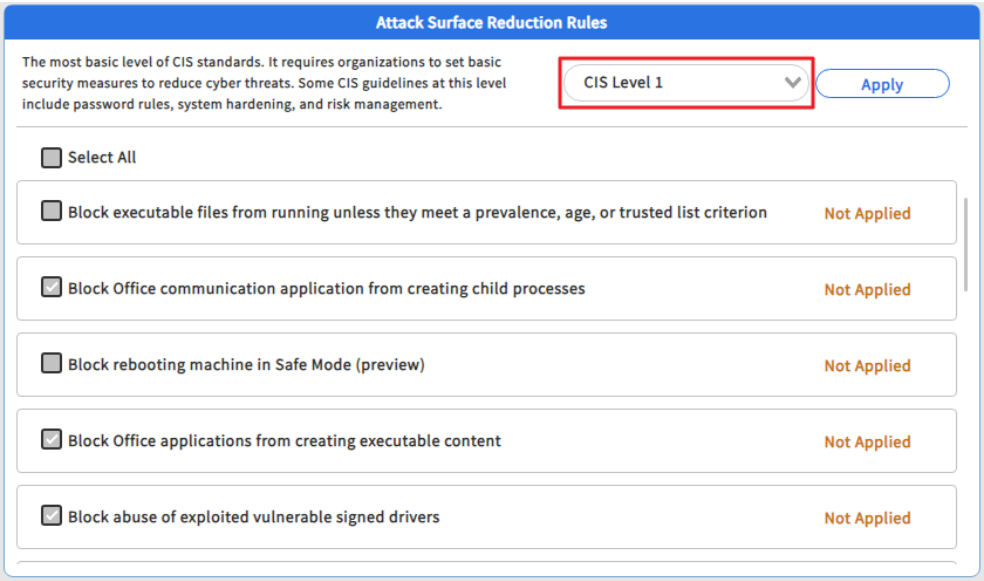


I. Select an option from the dropdown list

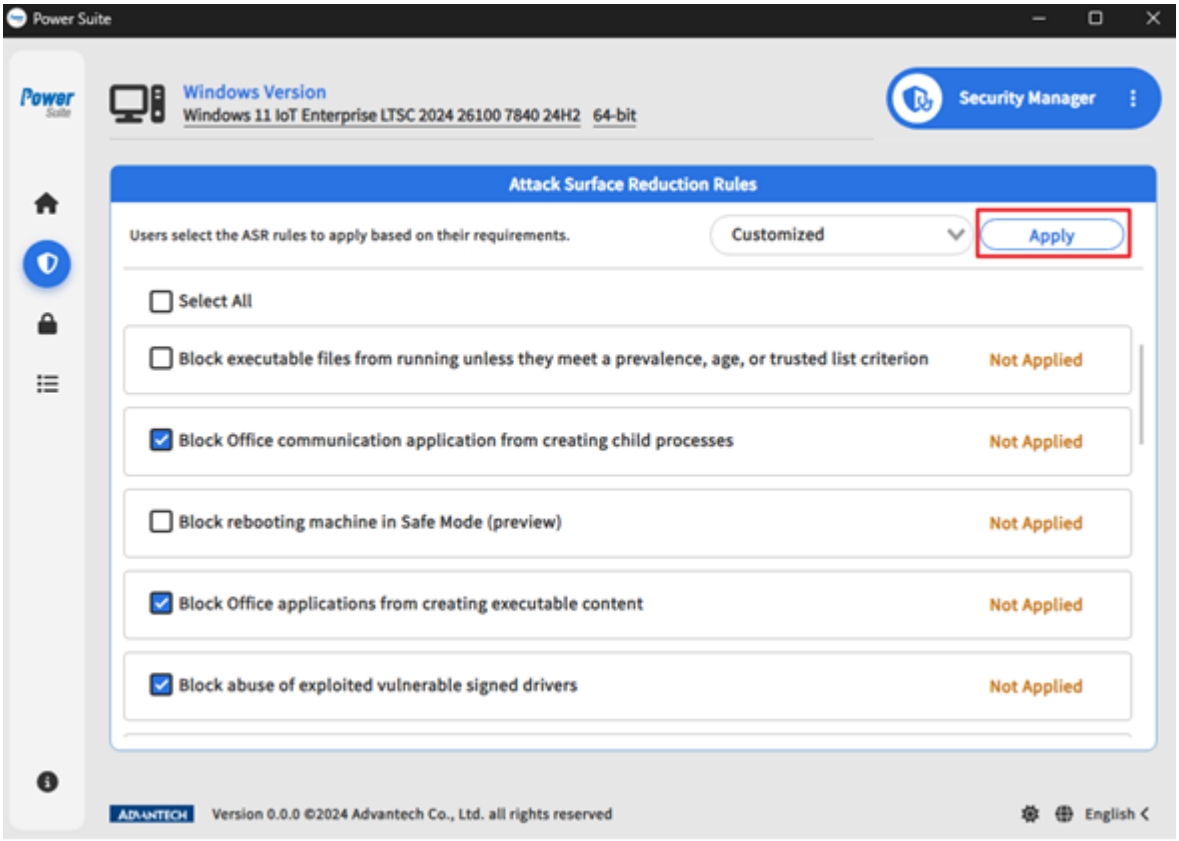
- Customized: users can select ASR rules based on their requirements



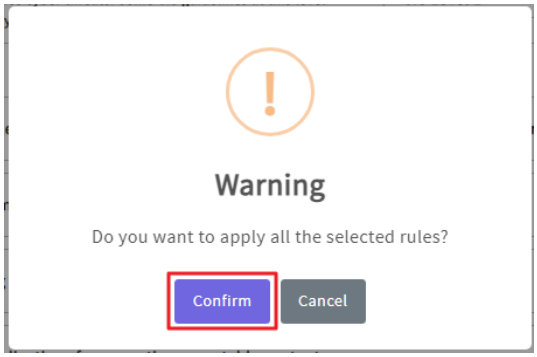
- CIS Level 1: basic security requirements that are recommended by the Center for Internet Security (CIS). These predefined rules can be configured on any system and should cause little or no interruption of service or reduced functionality.



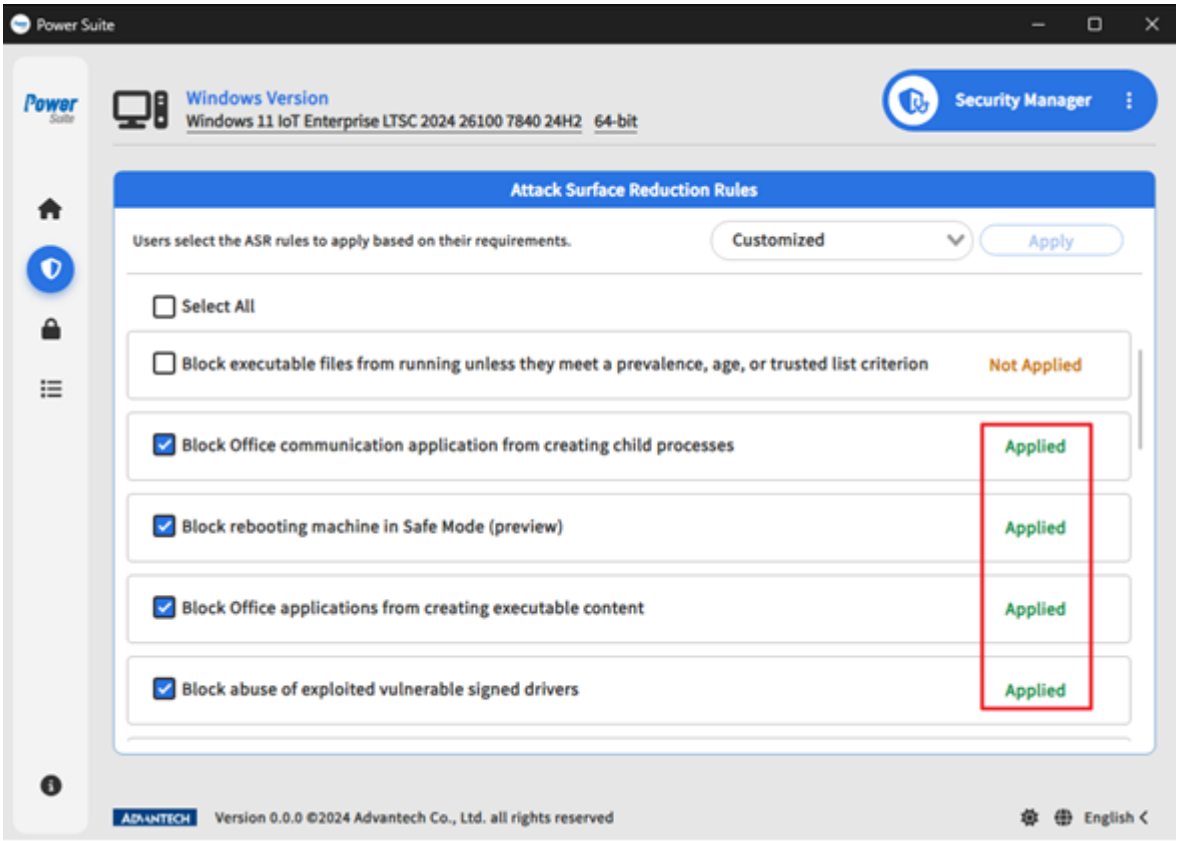
II. Click "**Apply**" button



III. Click “**Confirm**” button on dialog



IV. The selected rules are applied to system

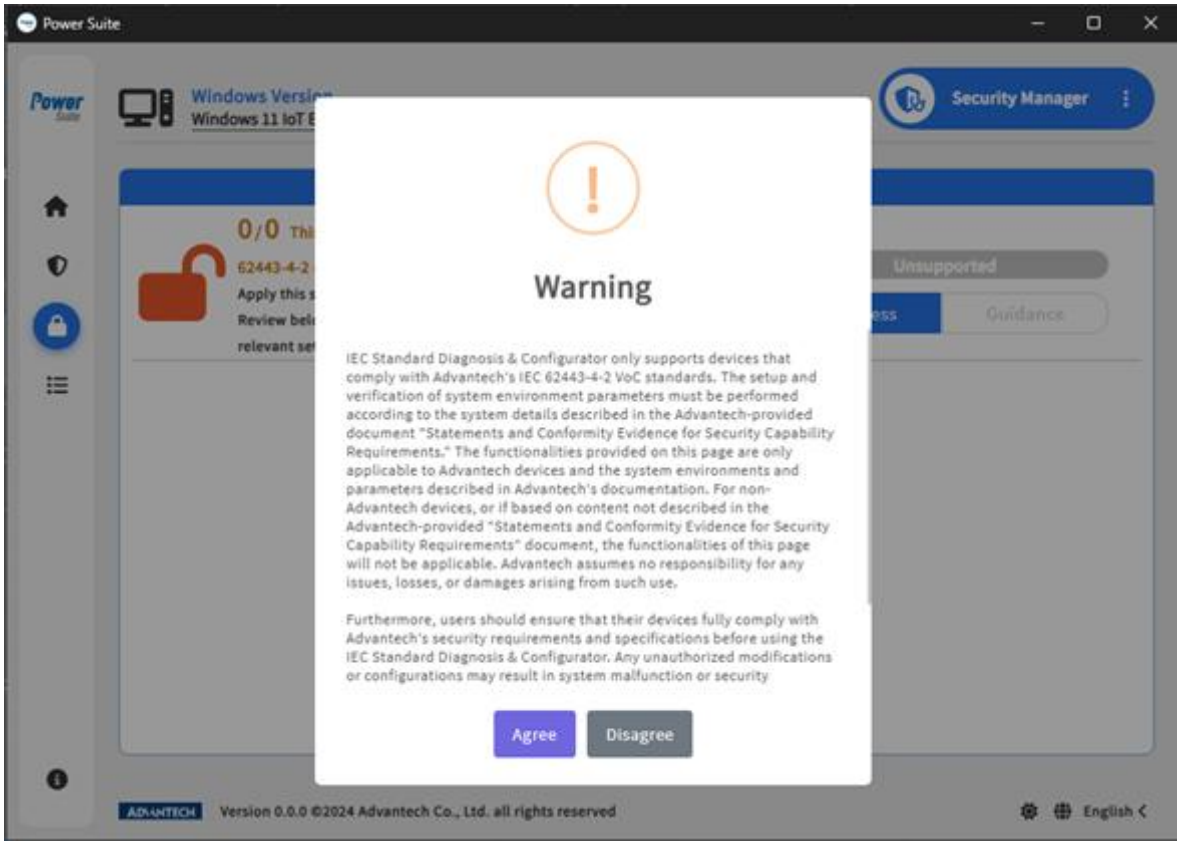


Please make sure Microsoft Defender Antivirus and antimalware updates are installed before applying ASR rules to system.

- Minimum platform release requirement: 4.18.2008.9
- Minimum engine release requirement: 1.1.17400.5

Take a look at Attack surface reduction rules overview for more information.

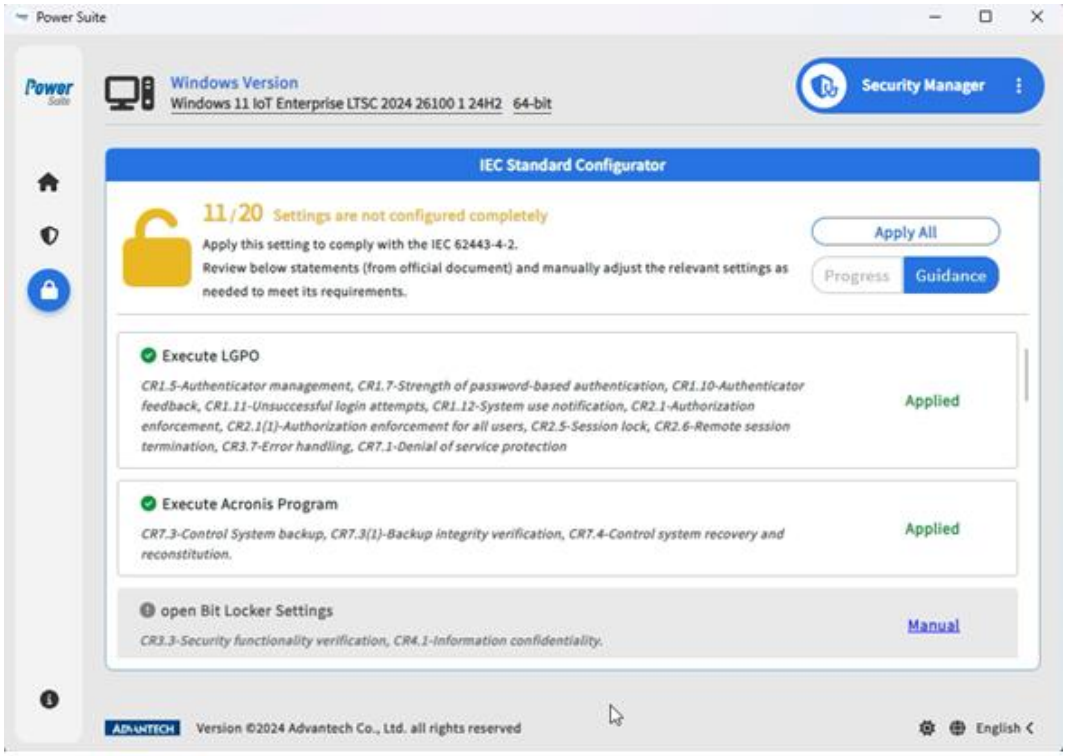
5.4.3 IEC Standard Configurator



- Disclaimer
  - When accessing the IEC Standard Configurator page for the first time, please read the content carefully and click the "Agree" button to use the features on this page.

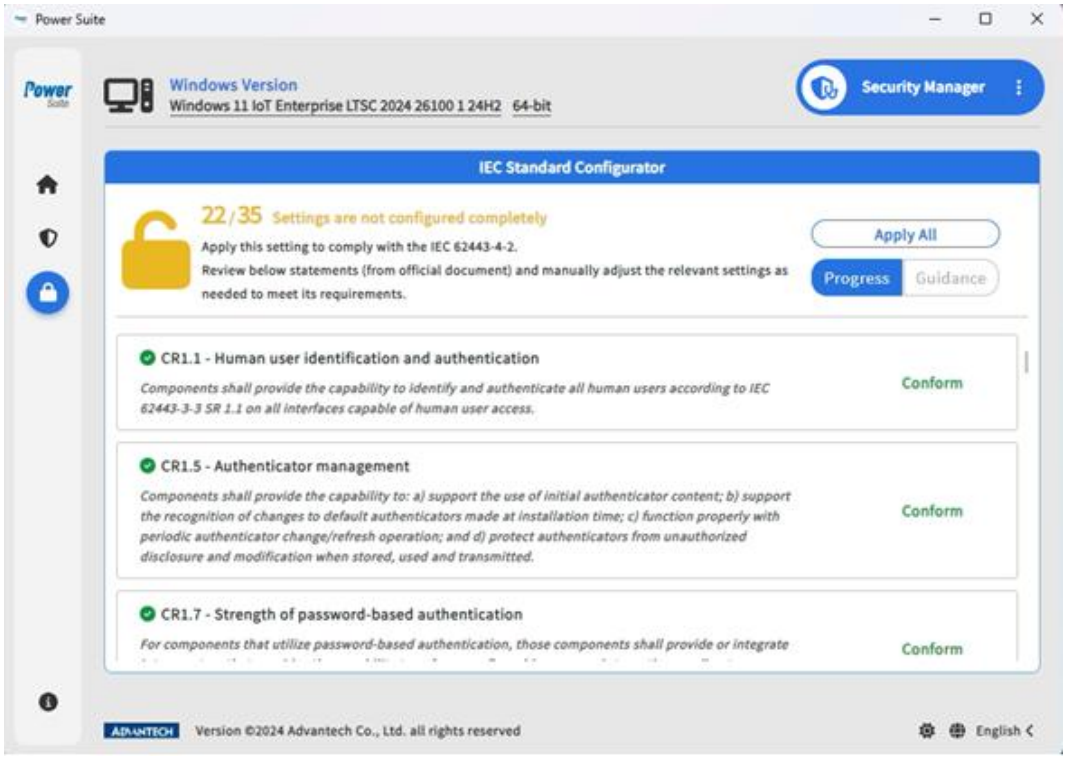
➢ Guidance

- Displays which system functions comply with the IEC 62443-4-2 standard.



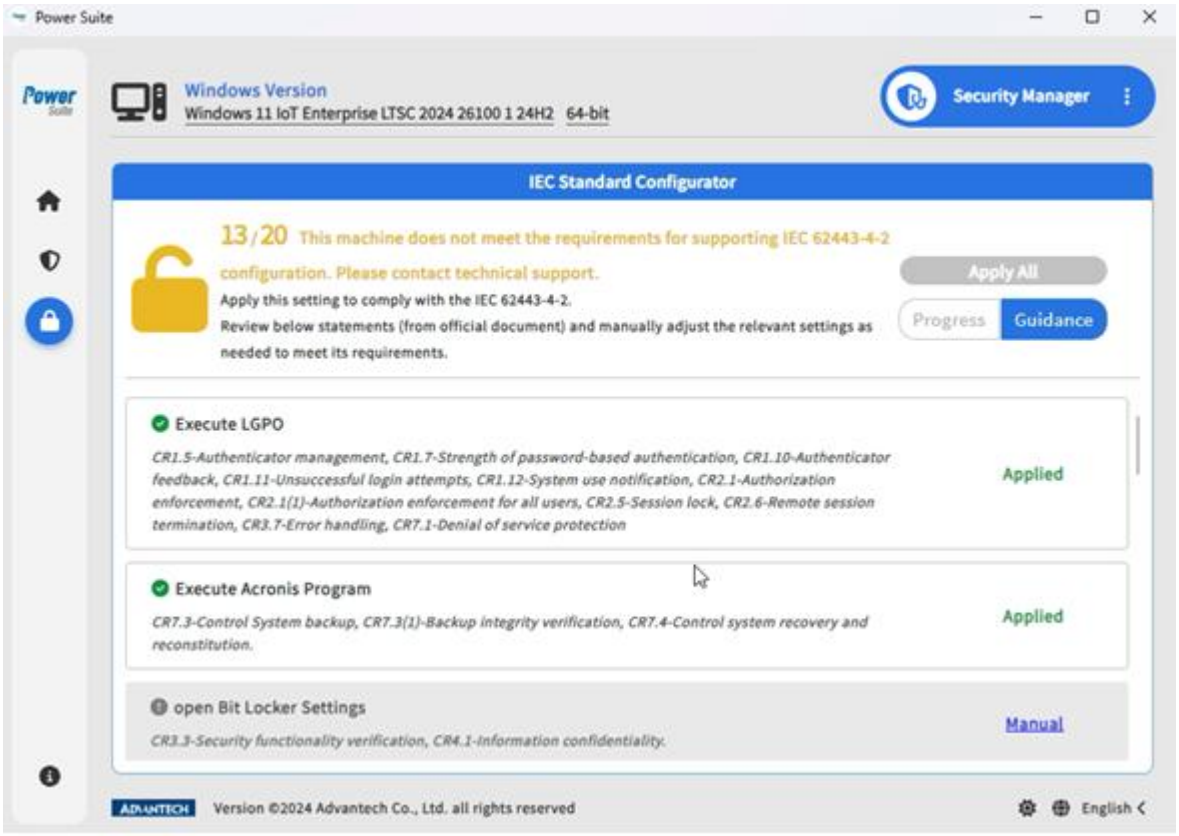
➢ Progress

- Displays which IEC 62443-4-2 clauses the system currently complies with.

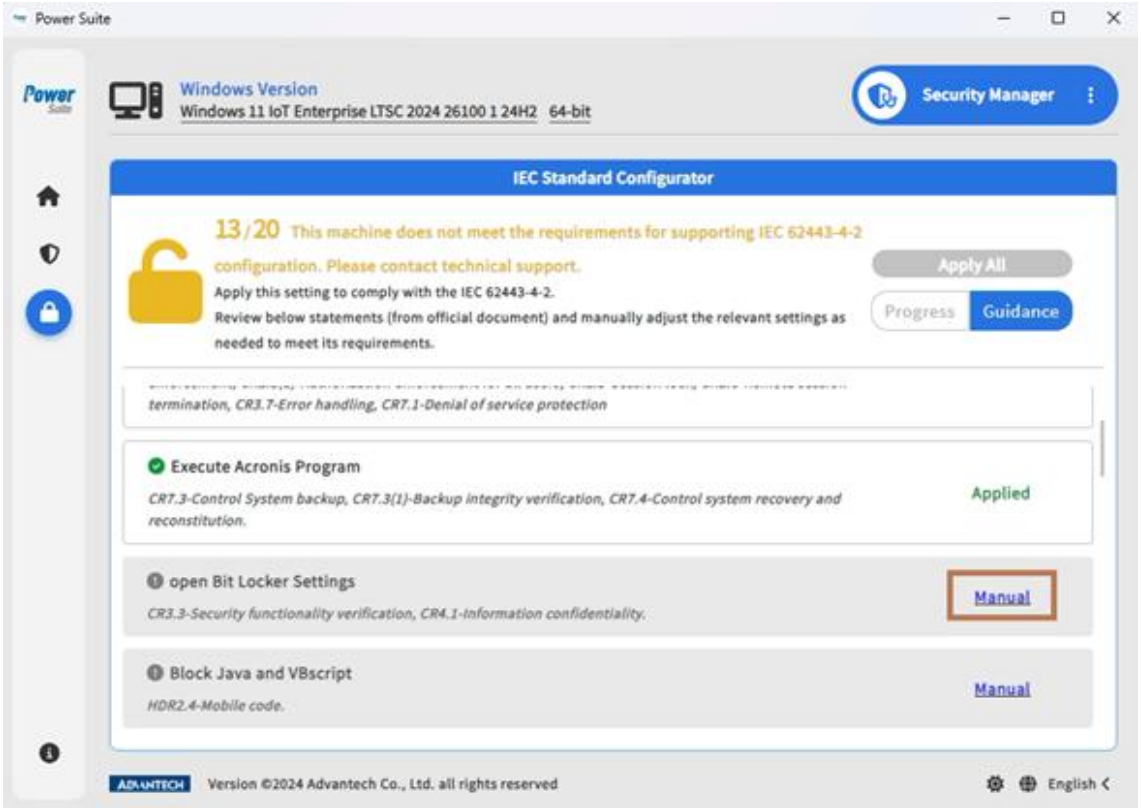


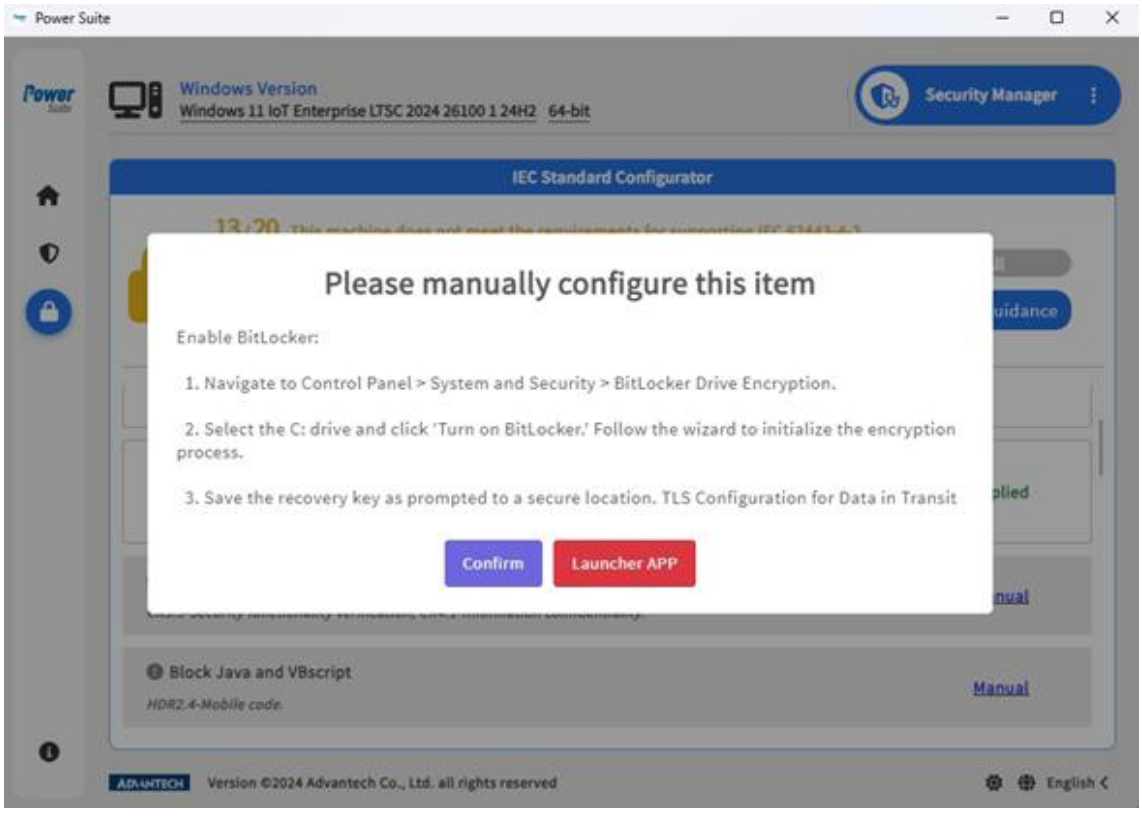
➢ Apply All

- Updates the system settings to meet the IEC 62443-4-2 standard.
- After executing this function, the following screen will appear:



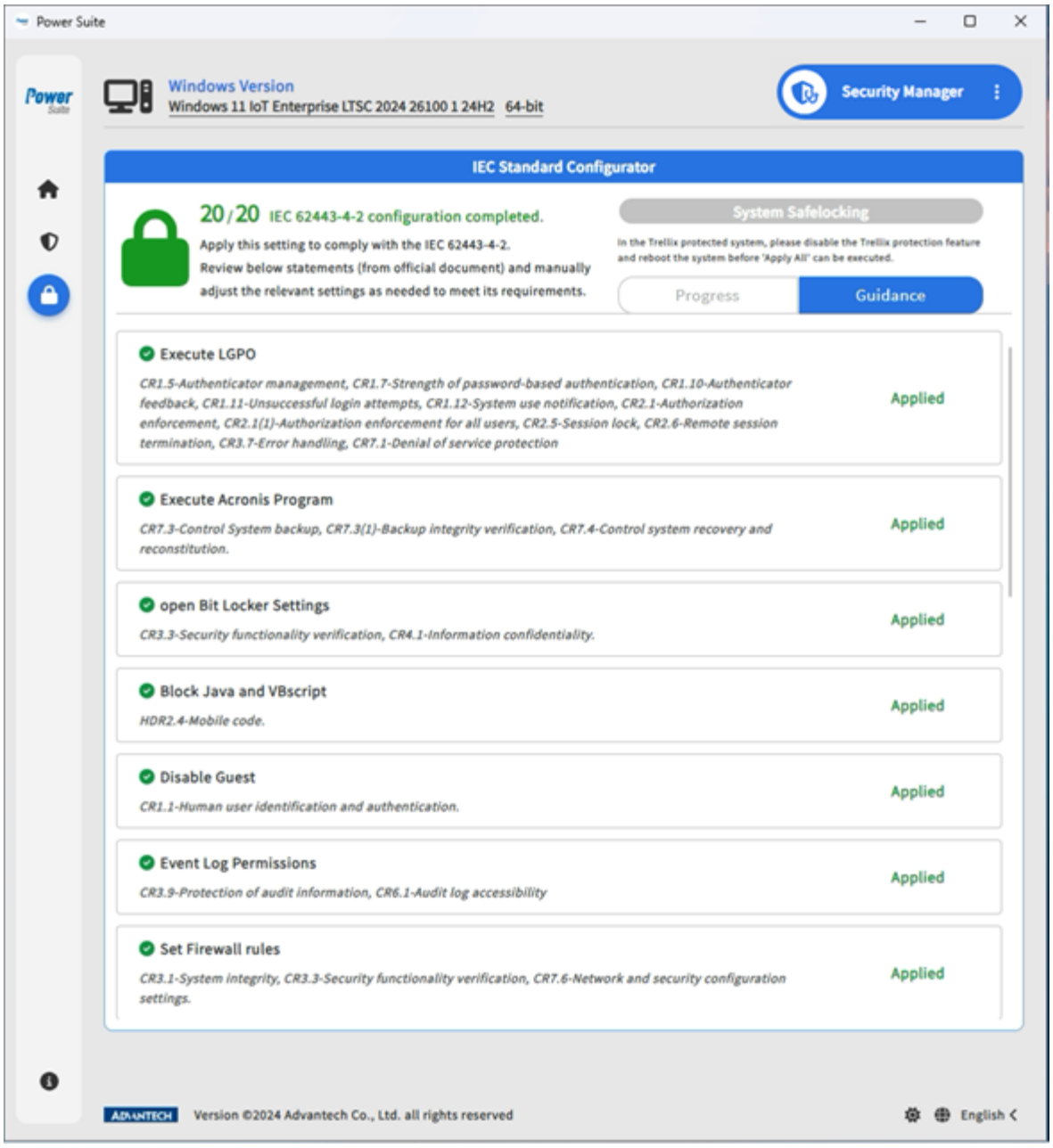
- Some items require manual execution. Click the "Manual" button to follow the steps, and use the "Launcher APP" button to quickly launch the corresponding app. Then, configure the app according to the reference steps. Ensure that Trellix manual steps are performed last.





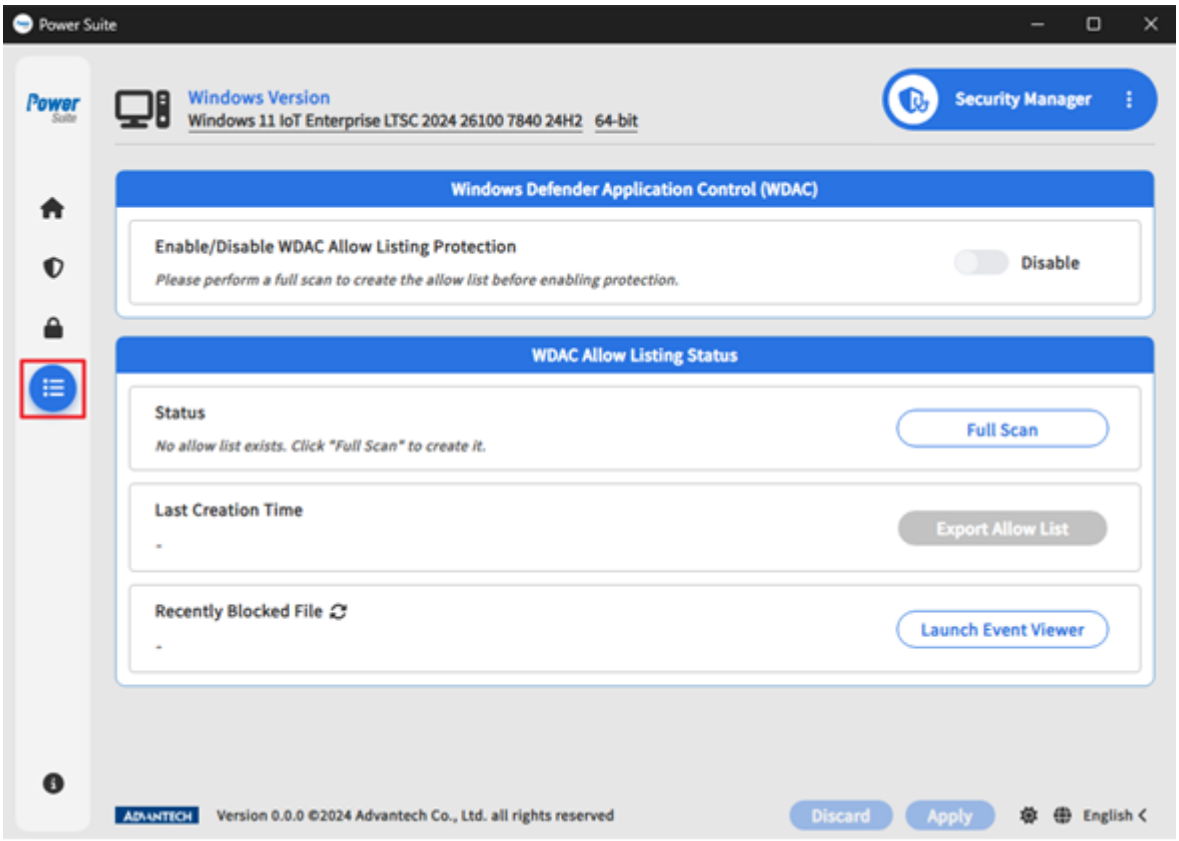
➢ Diagnosis(Applied)

■ If the computer settings comply with the IEC 62443-4-2 standard, the following screen should appear:



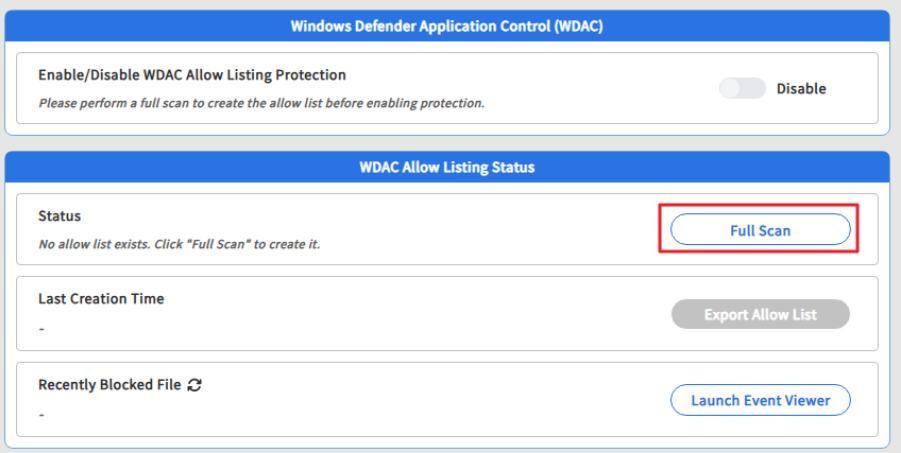
5.4.4 WDAC (Windows Defender Application Control) Allow Listing

WDAC (Windows Defender Application Control) is a Windows security mechanism feature that controls what applications and code are allowed to run on a system. Instead of letting everything run by default, it enforces a “only trusted/approved apps can run” model.

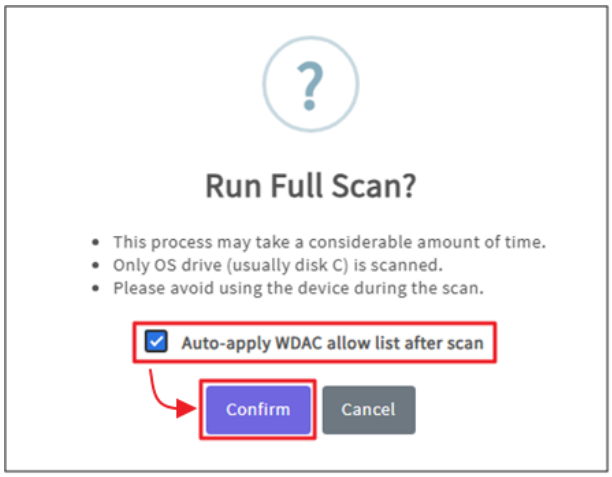


I. On first use, or when the allow list is unavailable, the “Enable/Disable” toggle and the “Export Allow List” button cannot be clicked.

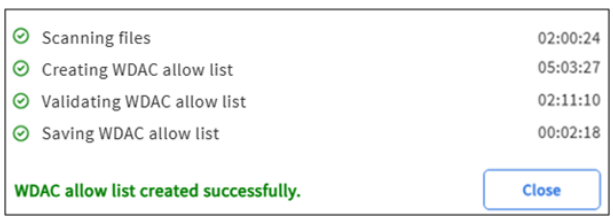
- Click “Full Scan” to scan the OS drive (usually disk C) and generate the allow list.



- If “Auto-apply WDAC allow list after scan” is checked, the user will be prompted to reboot the device after the scan completes successfully.

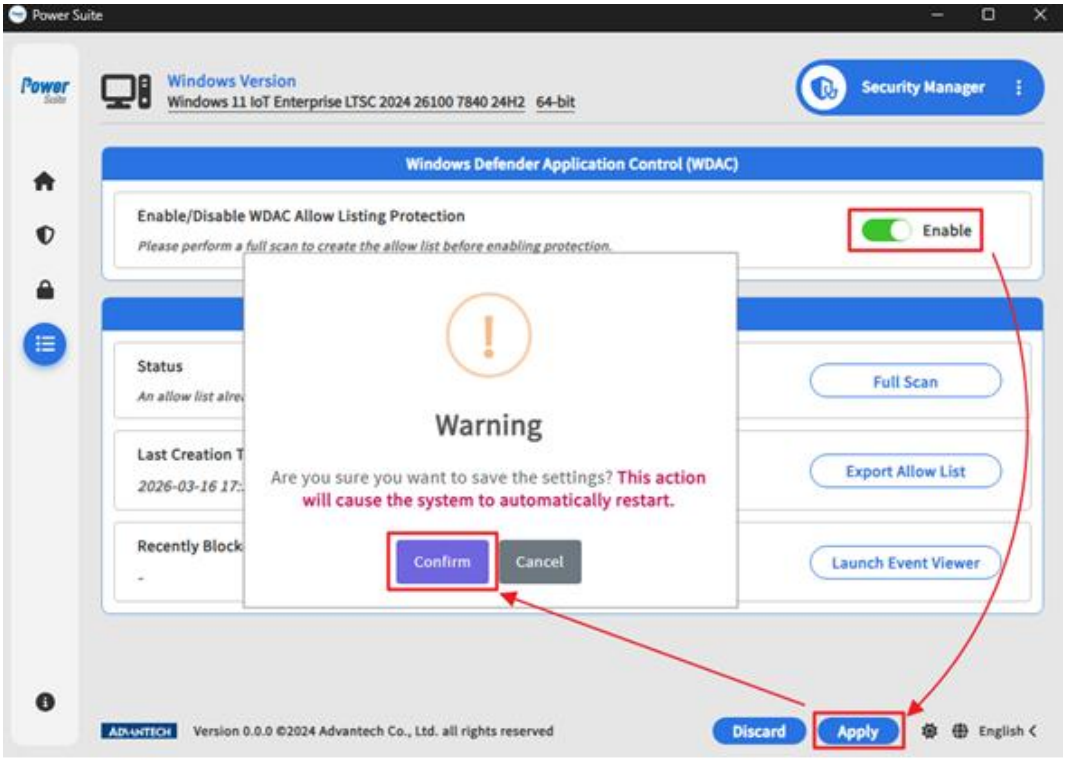


- A full scan may take some time. Please avoid using the system during the scan.

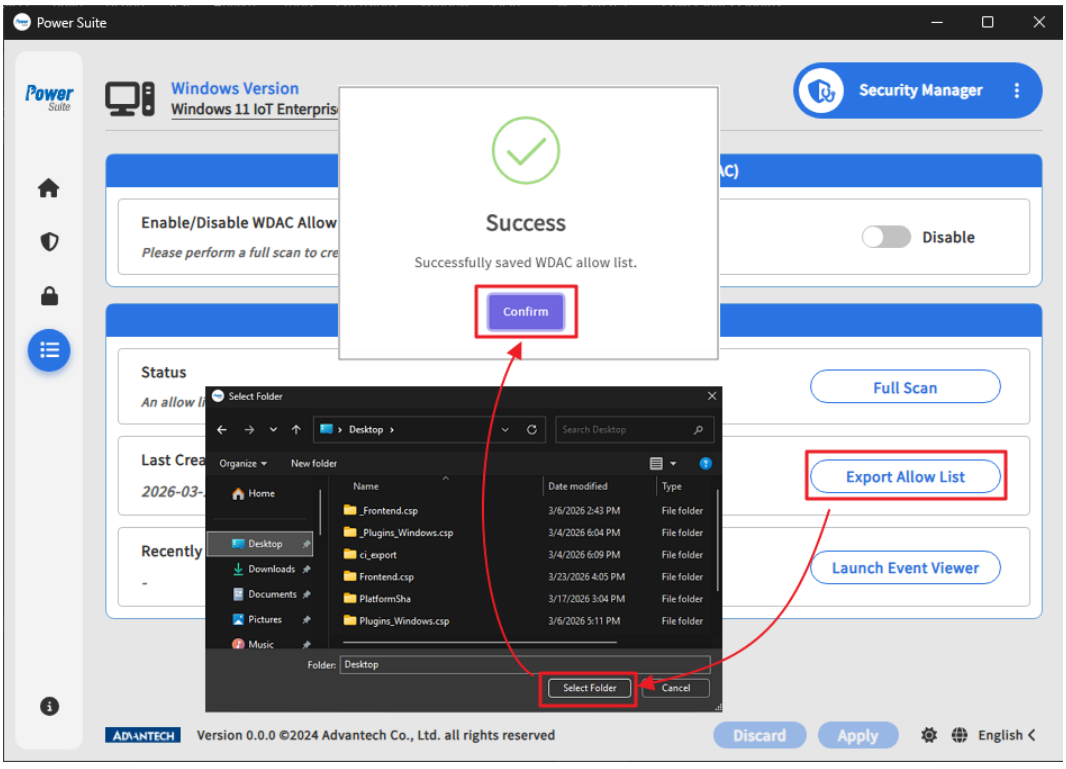


II. After the full scan completes successfully, an allow list is generated. Users can then export the allow list or manually enable or disable WDAC allow list protection.

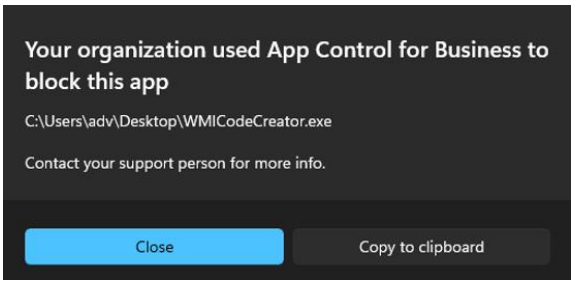
■ Use the toggle to enable or disable WDAC allow list protection, then click “Apply”.



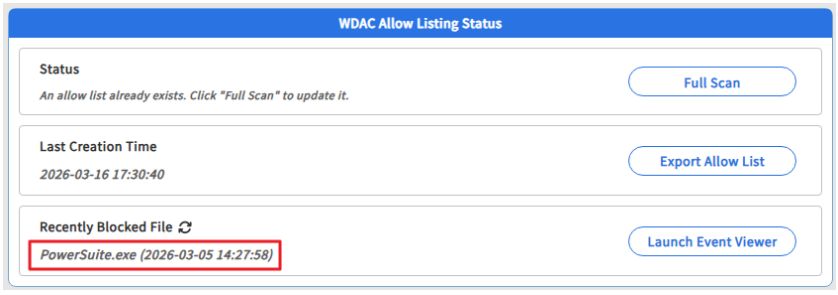
■ Click “Export Allow List” to save the WDAC allow list as “CIExport_{xxxxxxxxxxxx}.txt”.



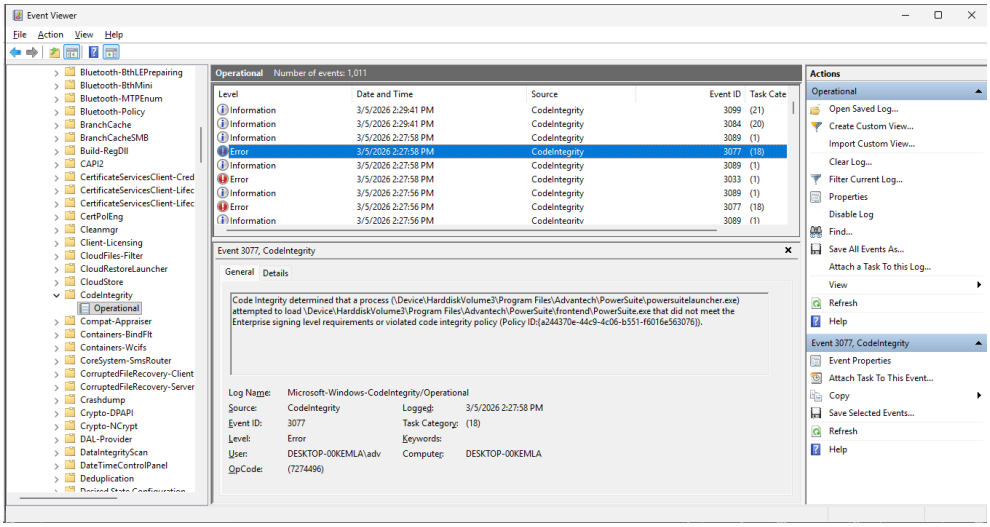
III. This dialog appears when a user runs an executable not on the allow list.



- The "Recently Blocked File" section shows the most recent file blocked by WDAC (if any). This allows users to quickly identify the latest enforcement event.



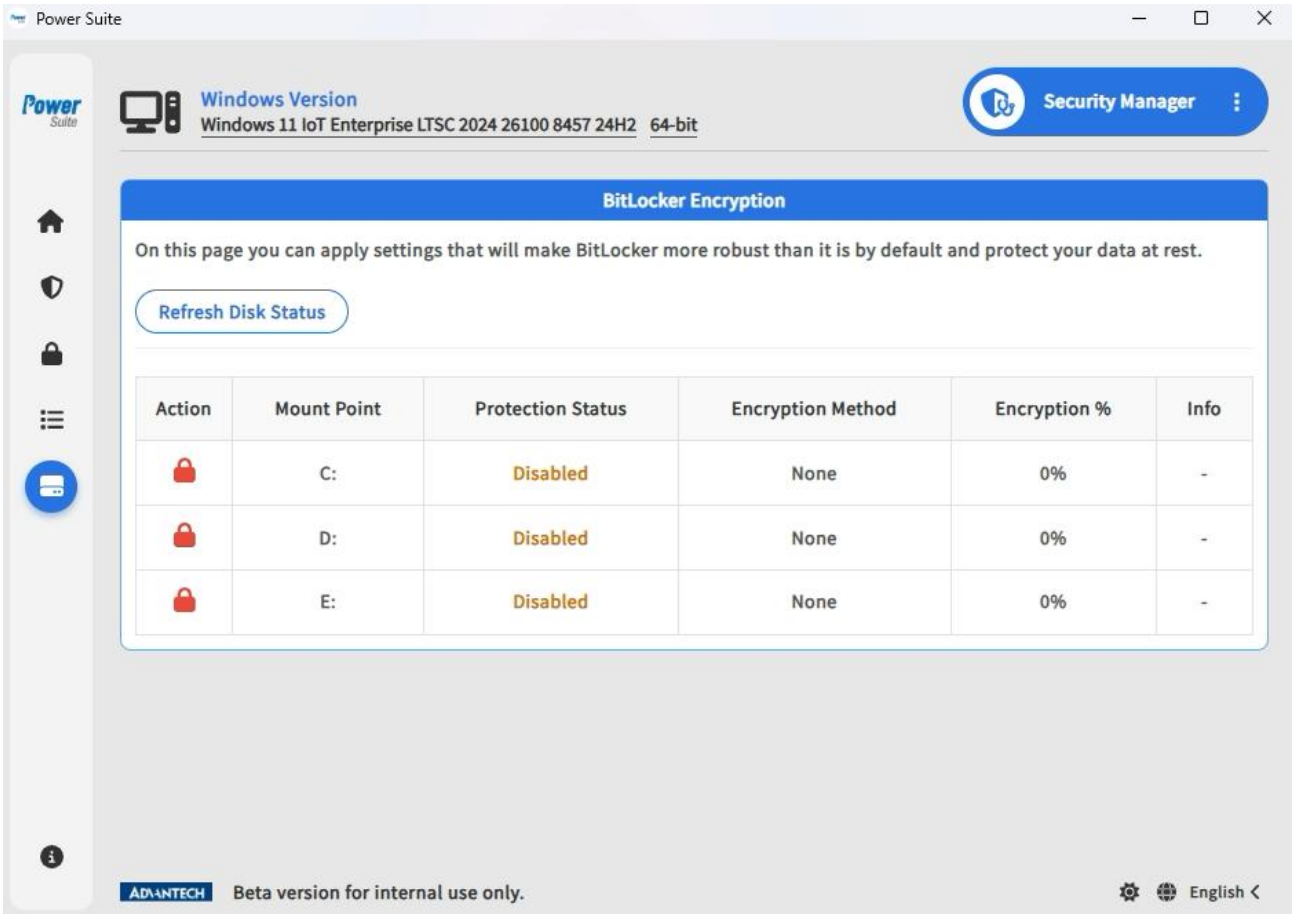
- To view detailed log information, click "Launch Event Viewer". This action opens the Windows Event Viewer and automatically navigates to the log location: Applications and Services Logs/Microsoft/Windows/CodeIntegrity/Operational



- When the WDAC allow list protection is enabled, any file that is not included in the allow list will be blocked if it is executed or loaded. The system logs these blocked activities in the Windows Event Log for further review.

5.4.5 BitLocker

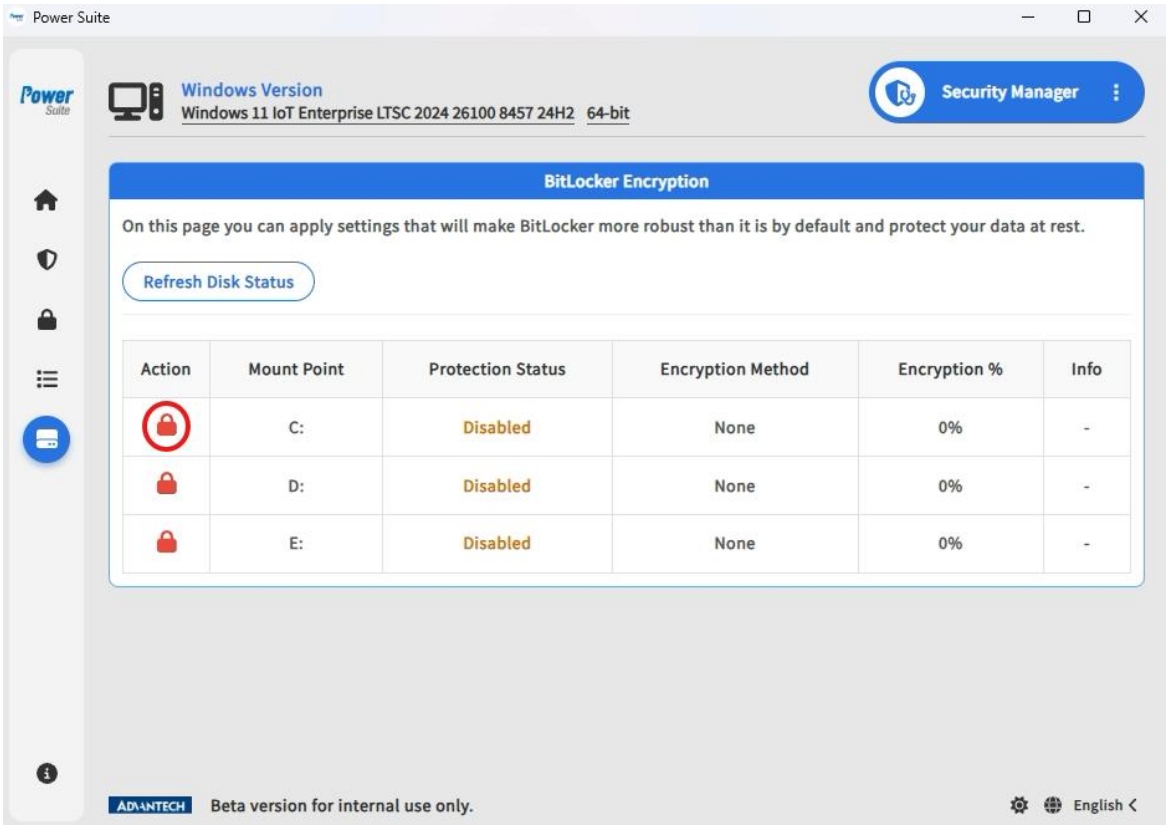
On this page, you can apply advanced settings to enhance BitLocker beyond its default configuration and provide superior protection for your data at rest. BitLocker targets Operating System (OS) drives, fixed data drives, and removable data drives. Available encryption options vary depending on the drive type. This page also provides features for unlocking drives and viewing encryption details.



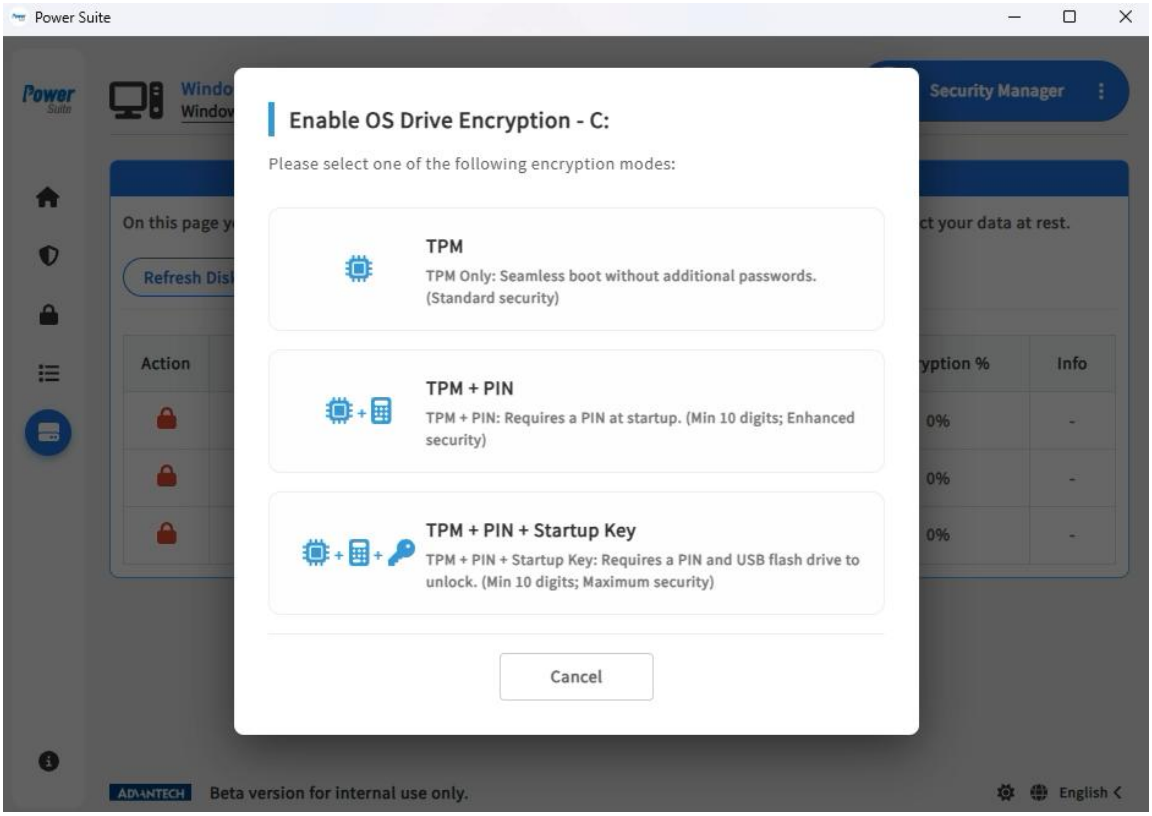
Note: If a flash drive or hard drive device has not been assigned a drive letter (such as F:, G:, etc.), the "Refresh Disk Status" feature will not be able to detect it.

I. Encrypting the Operating System (OS) Drive

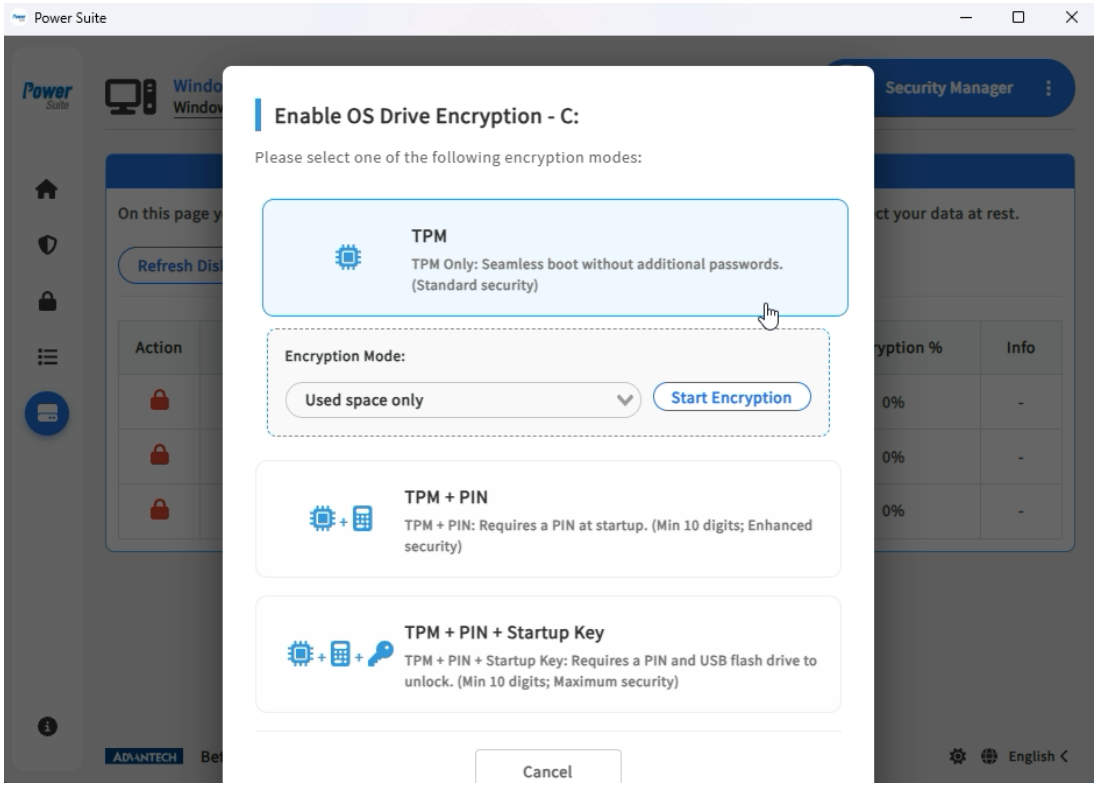
- **Click the lock icon** in the **Action** column for the **C: drive** (OS Drive).



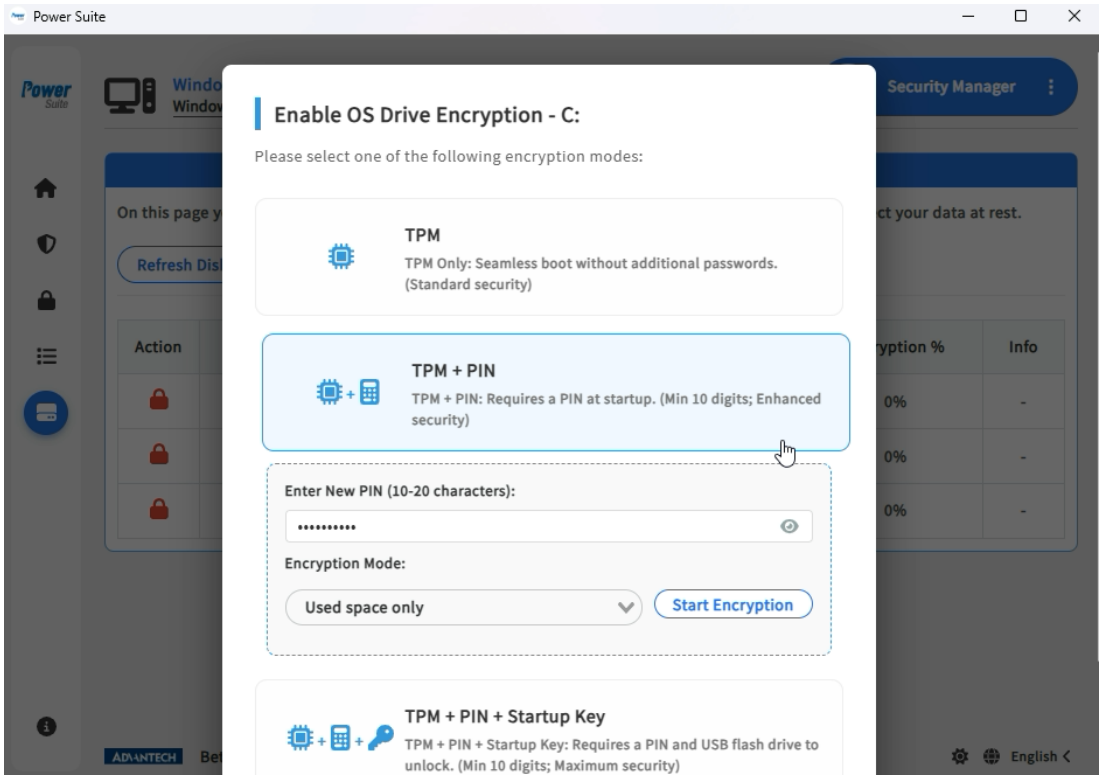
- Select an Encryption Type: The OS drive offers three types of encryption:



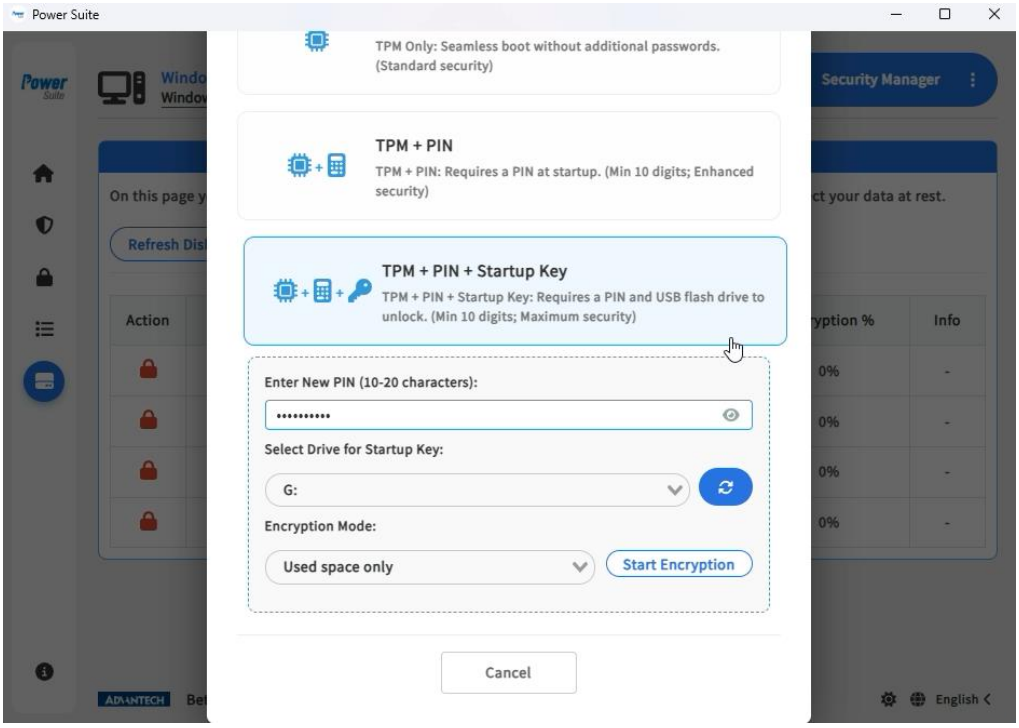
TPM Only: Relies solely on the TPM for unlocking. Select an encryption mode (Used Space Only or Full Disk Encryption) and click Start Encryption.



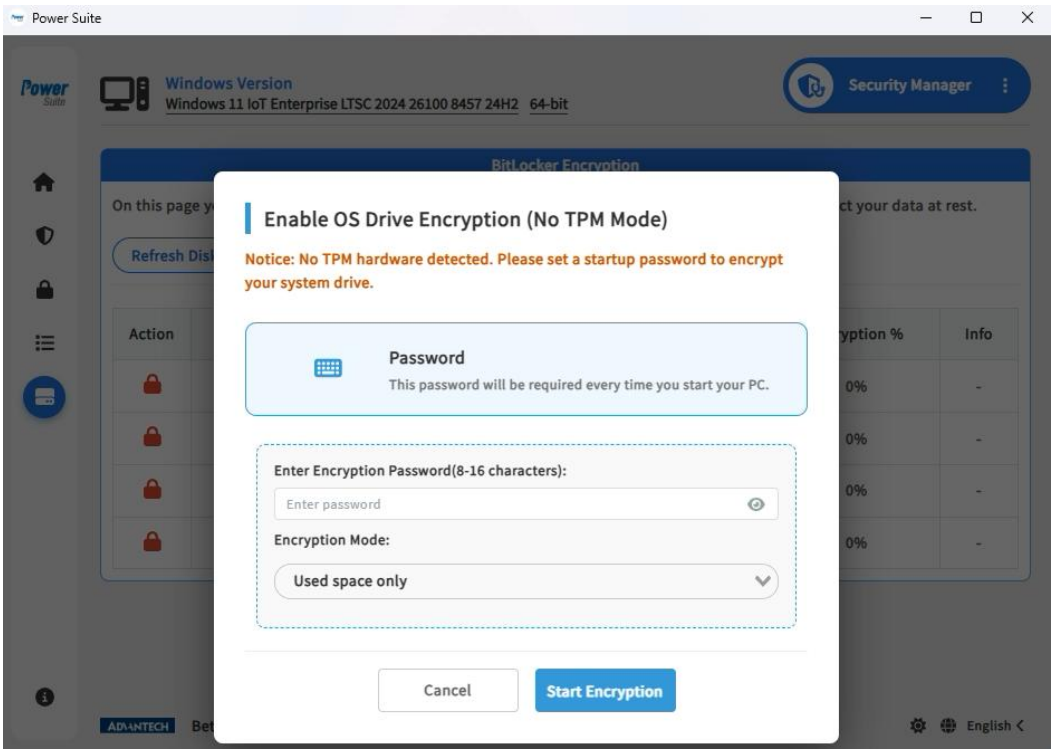
TPM + PIN: Requires both the TPM and a user-defined PIN (10–20 characters) for unlocking. Enter the PIN, select a mode, and click Start Encryption.



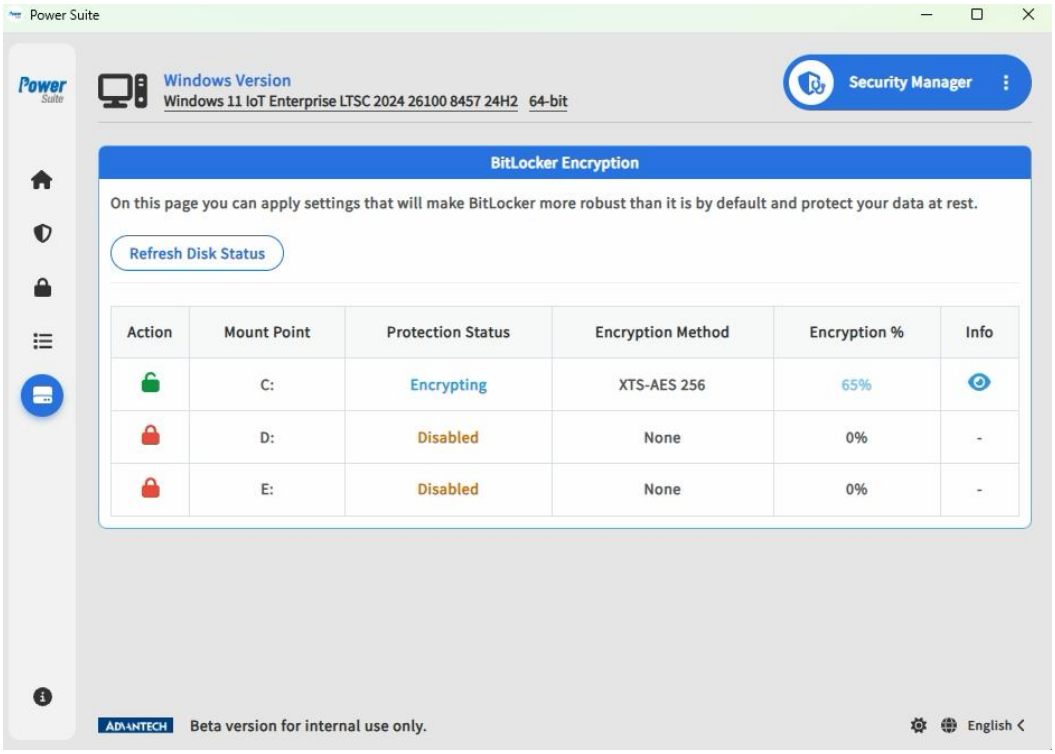
TPM + PIN + Startup Key: Requires the TPM, a PIN (10–20 characters), and a physical Startup Key (USB flash drive) for unlocking. Enter the PIN, select the target removable drive for the key, choose a mode, and click Start Encryption. If there are no selectable drives, you can insert a new, available USB flash drive and press the refresh button. The new drive will then appear in the dropdown menu for selection.



Non-TPM: If the host does not support TPM, only a password is used for unlocking. Enter your password, select a mode, and click Start Encryption.

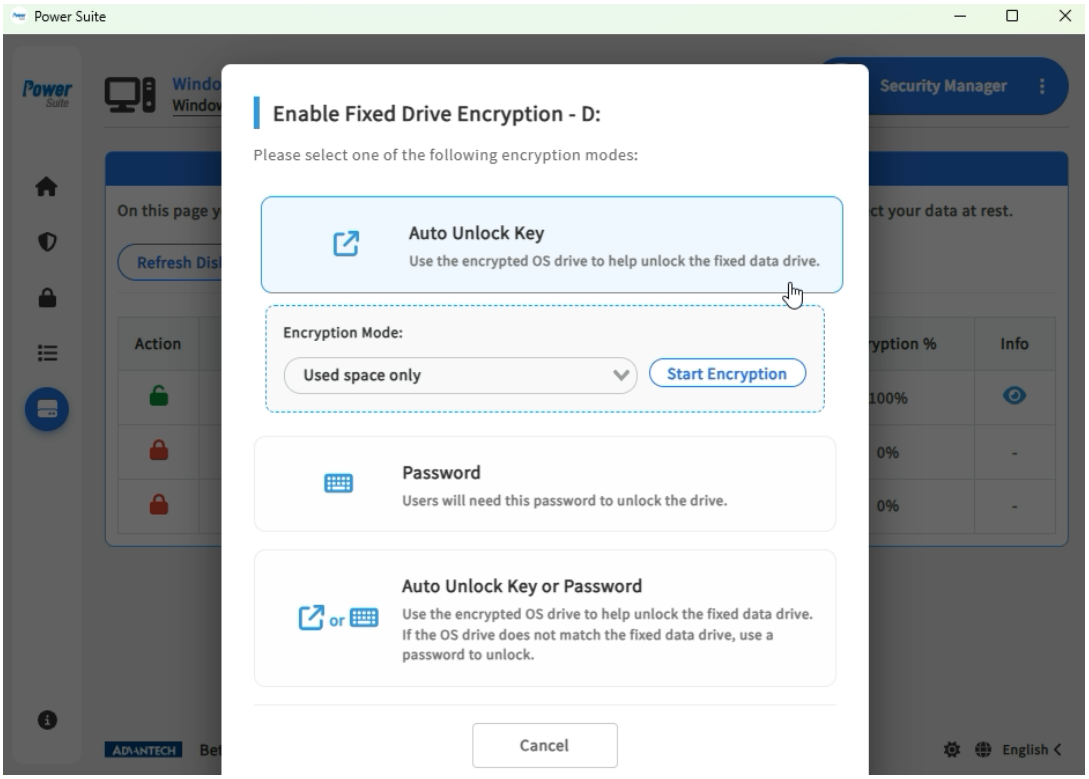


- Wait for the encryption process to complete.

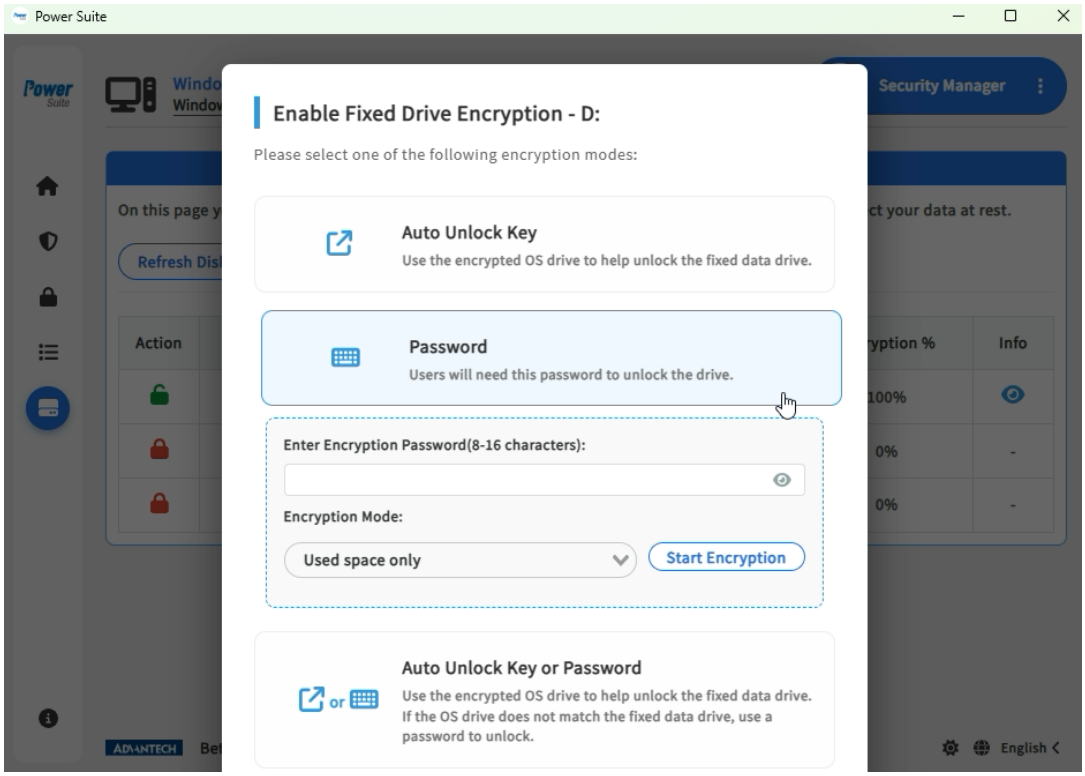


II. Encrypting Fixed Data Drives

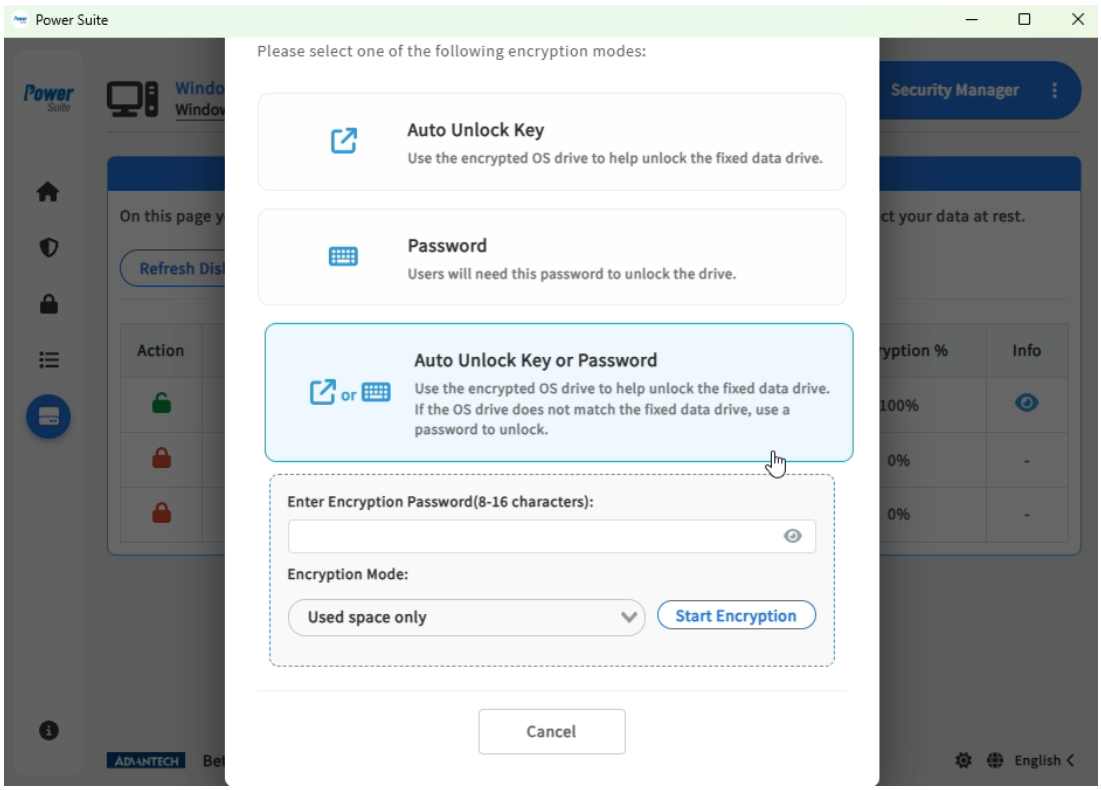
- Click the lock icon in the Action column for the D: drive (Fixed Data Drive).
  Auto-Unlock: If the OS drive is already encrypted, it can automatically unlock the fixed data drive. Select a mode and click Start Encryption.



Password: Uses a password for unlocking. Enter your password, select a mode, and click Start Encryption.

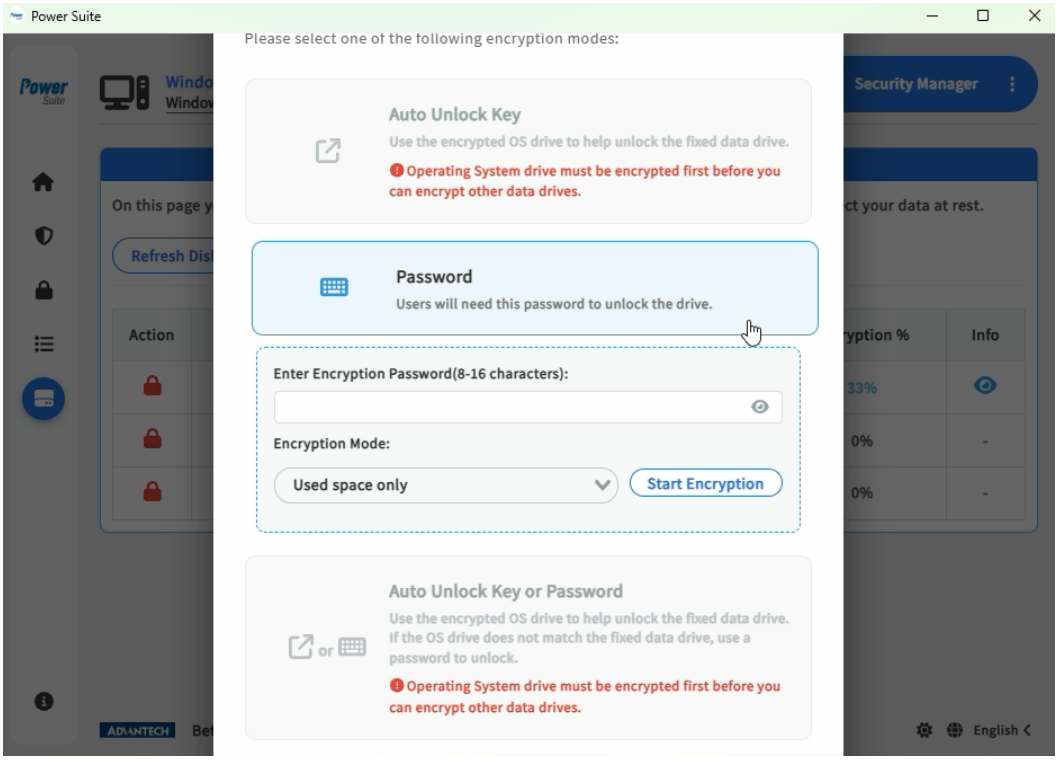


Auto-Unlock + Password: Combines both methods. If the OS drive fails to auto-unlock, a password will be required. Enter your password, select a mode, and click Start Encryption.

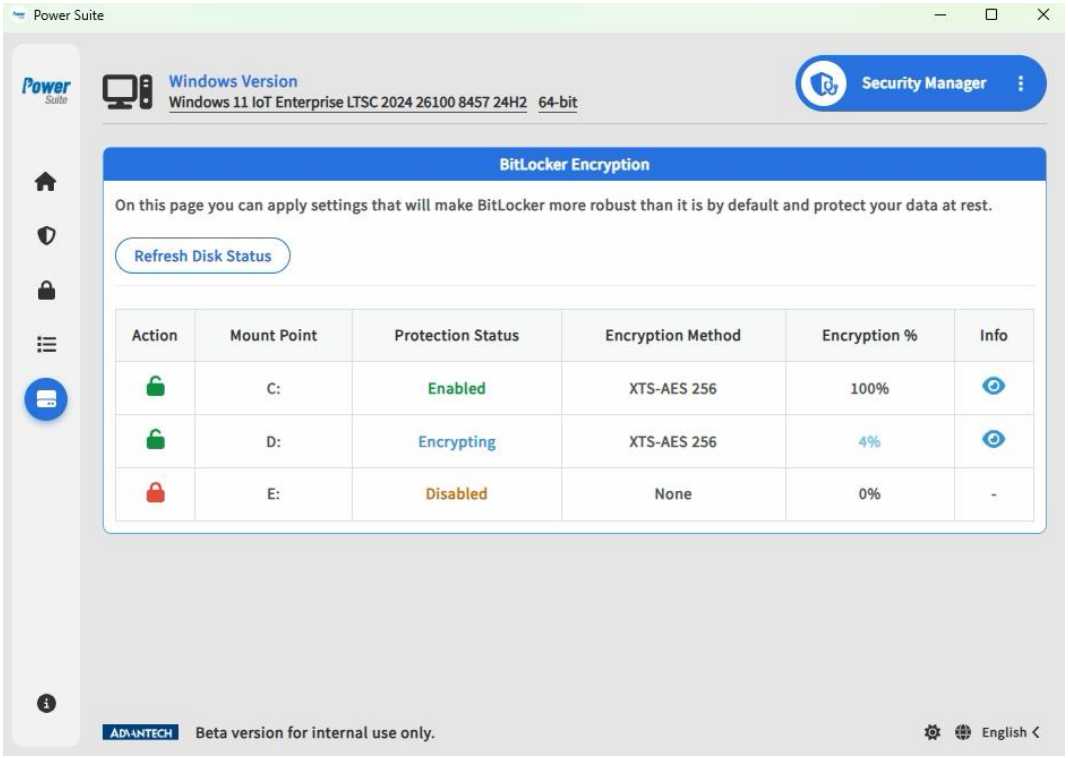


Password (OS Drive Unencrypted): If the OS drive is not encrypted, fixed data drives only

support password encryption. Enter your password, select a mode, and click Start Encryption.



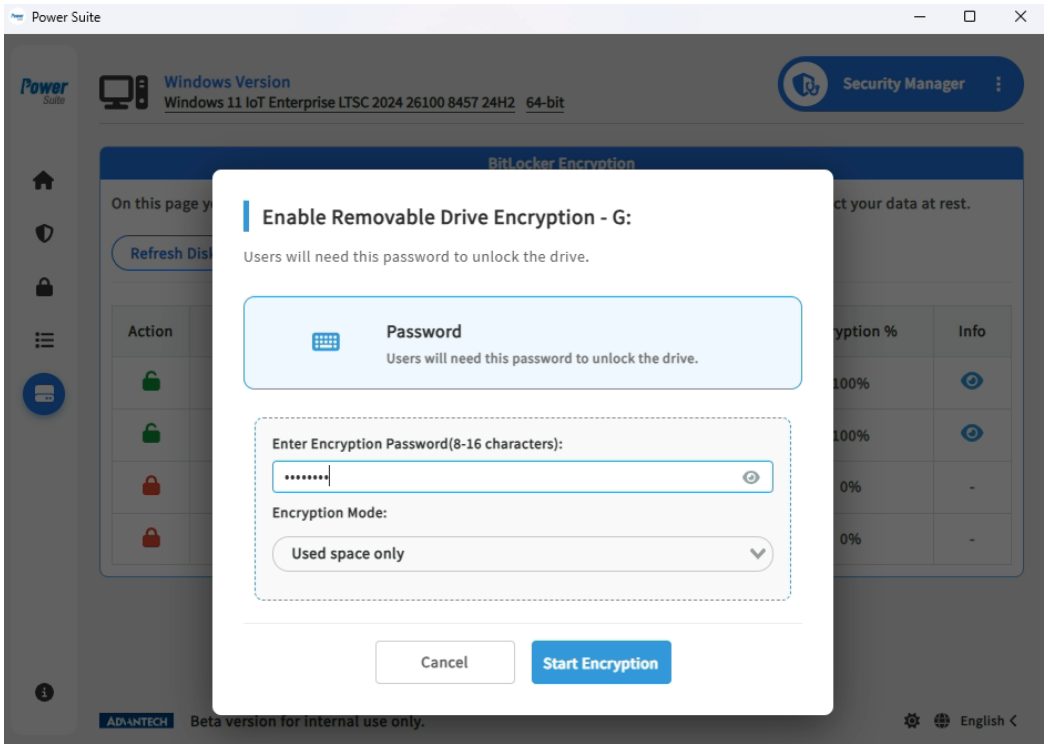
- Wait for the encryption process to complete.



III. Encrypting Removable Data Drives

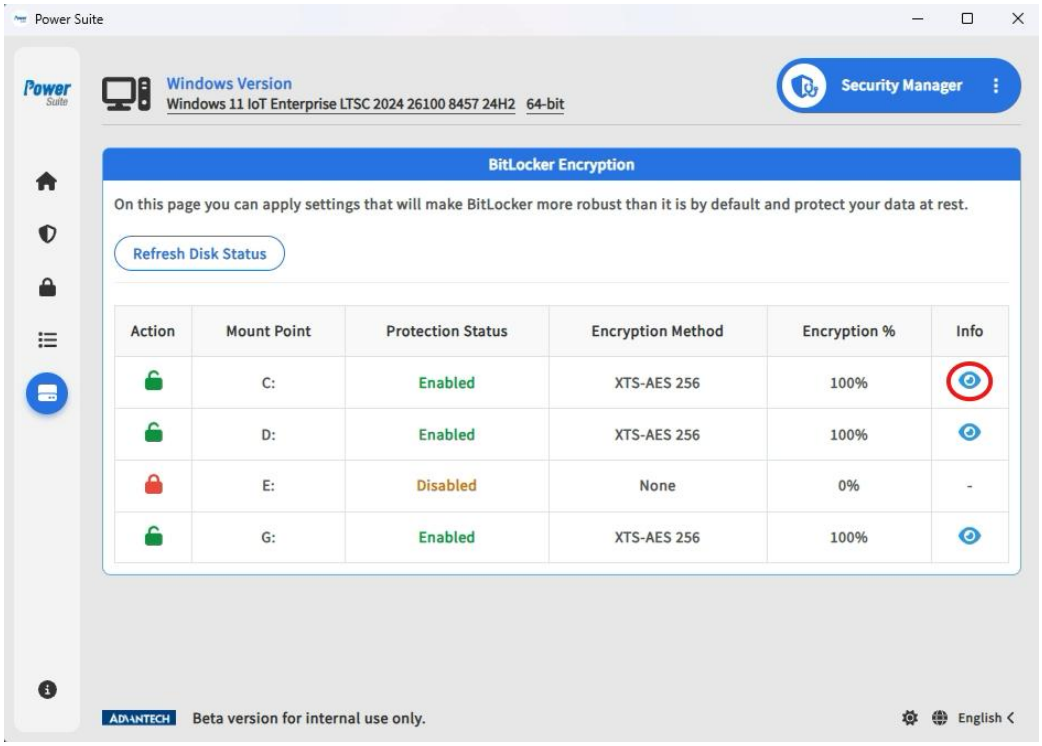
- Click the lock icon in the Action column for the E: drive (Removable Data Drive).
- Password: Uses a password for unlocking. Enter your password, select a mode, and click

Start Encryption.



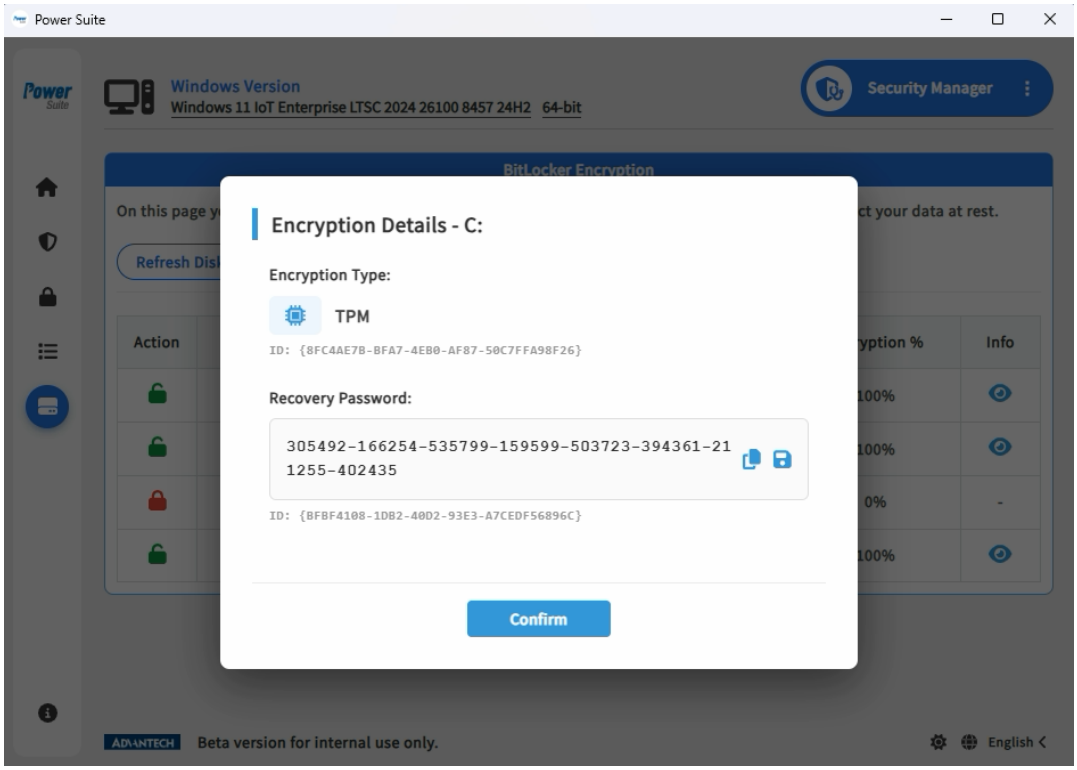
IV. Viewing Encryption Information

- Click the eye icon in the Info column to view the drive's encryption type and the Recovery Password.



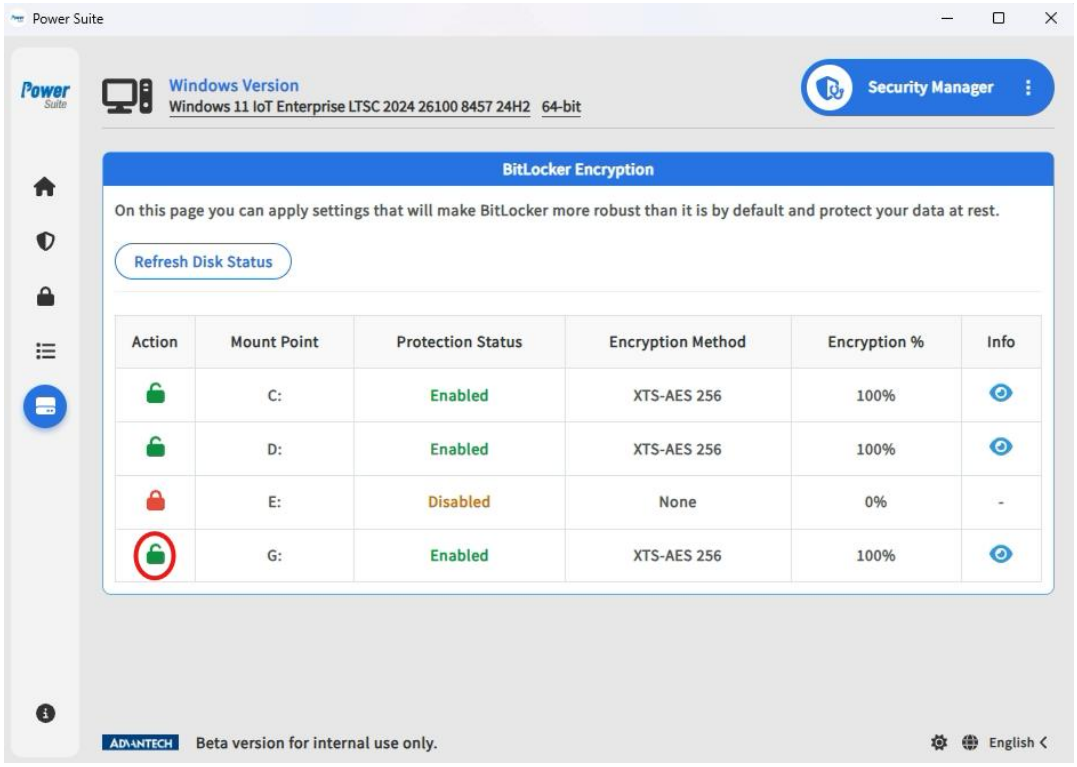
- Recovery Password: This is the final failsafe for restoring access to an encrypted drive. Click the Copy icon to copy the value to the system clipboard.

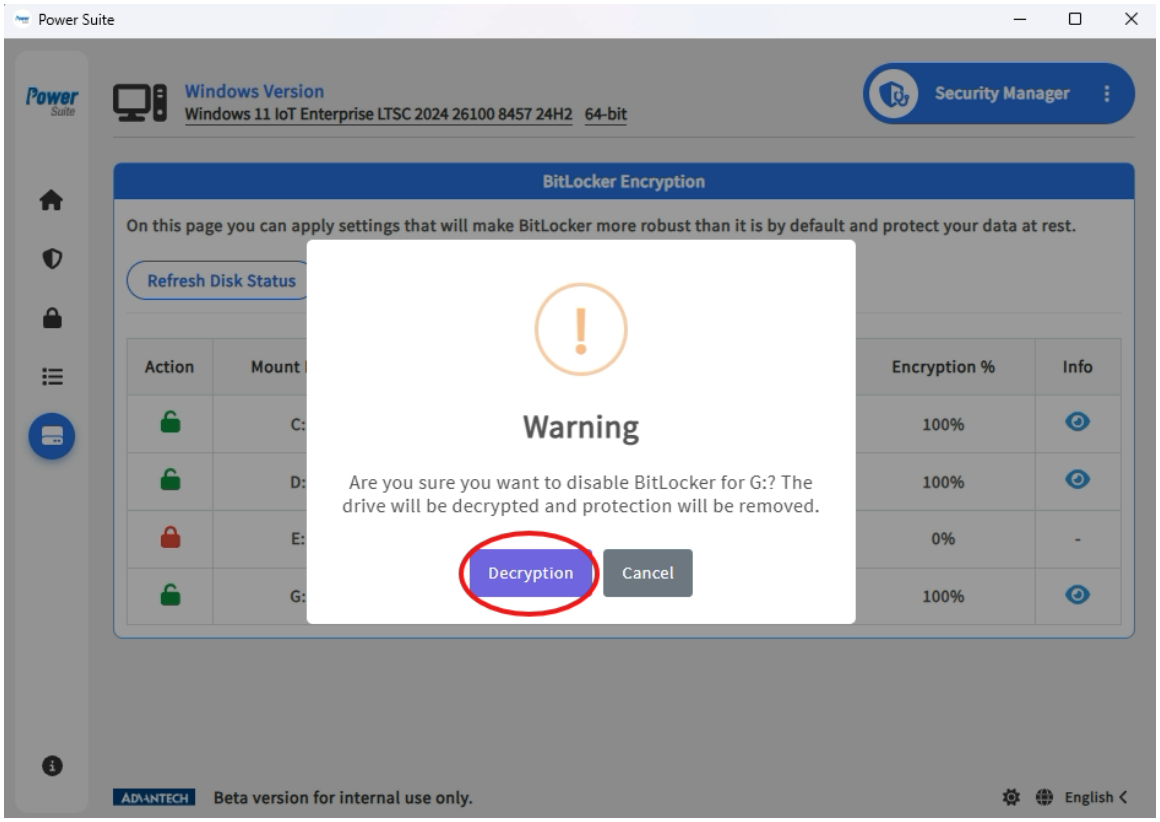
Click the Diskette/Save icon to save the value as a file (based on your browser's download settings).



V. Decryption

- Click the locked icon in the Action column of an encrypted drive.
- An unlock confirmation window will appear. Click Decryption to begin the process.




Power Suite
Windows Version
Windows 11 IoT Enterprise LTSC 2024 26100 8457 24H2 64-bit
Security Manager
BitLocker Encryption
On this page you can apply settings that will make BitLocker more robust than it is by default and protect your data at rest.
Refresh Disk Status
Action
Mount
Encryption %
Info
C:
100%
D:
100%
E:
0%
G:
100%
Warning
Are you sure you want to disable BitLocker for G:? The drive will be decrypted and protection will be removed.
Decryption
Cancel
Beta version for internal use only.
English

6. APPENDIX

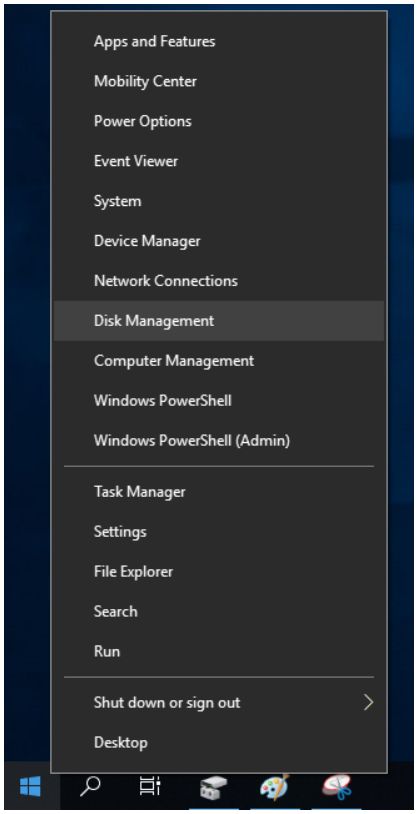
6.1 APPENDIX 1

6.1.1 Windows 10 IoT Enterprise LTSC 2019

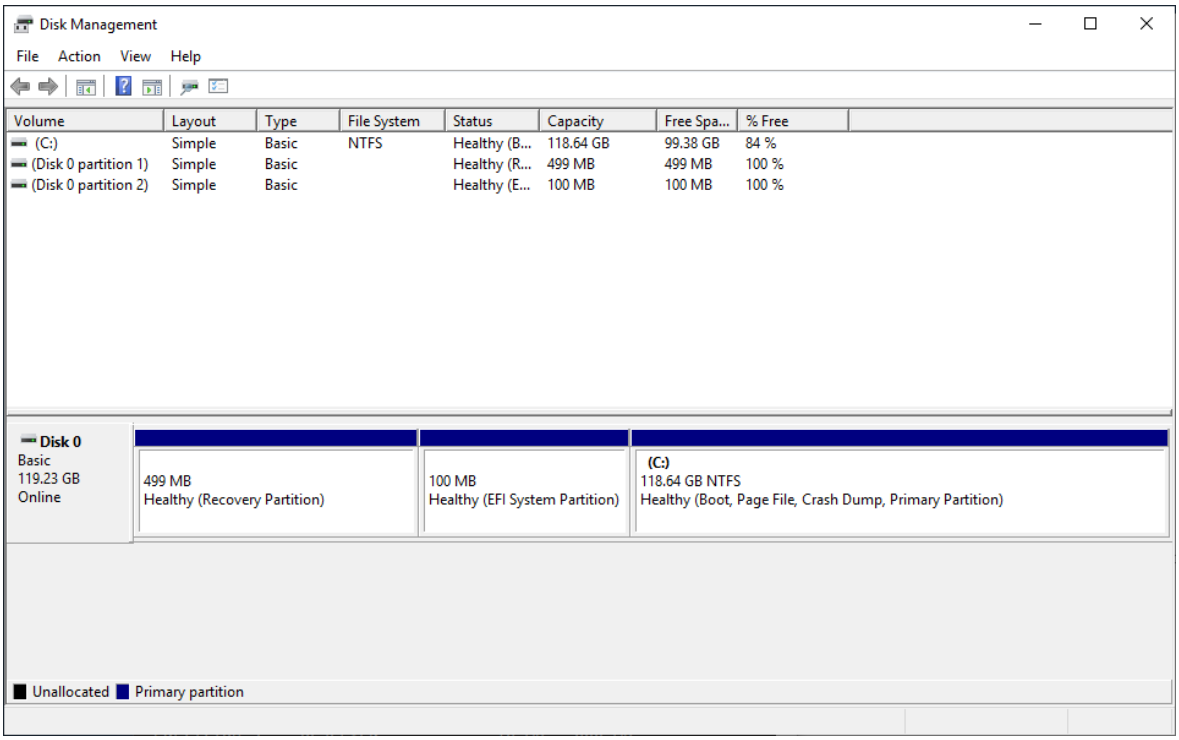
- First partition needs to be the “Recovery” partition.
- Second partition needs to be the “System” partition (EFI System Partition).
- Third partition needs to be the “Reserved” partition. This partition is not shown in Disk Management.
- The “Primary” partitions start at the fourth partition. “Primary” partitions are Windows partition and other data partitions.

The suggested partition layout schematic is as below.

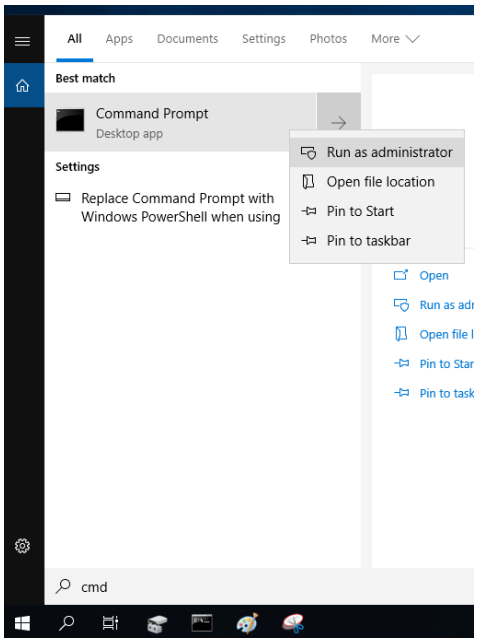
The partition status can be checked using Disk Management. Right-click on the start button, then click Disk Management.



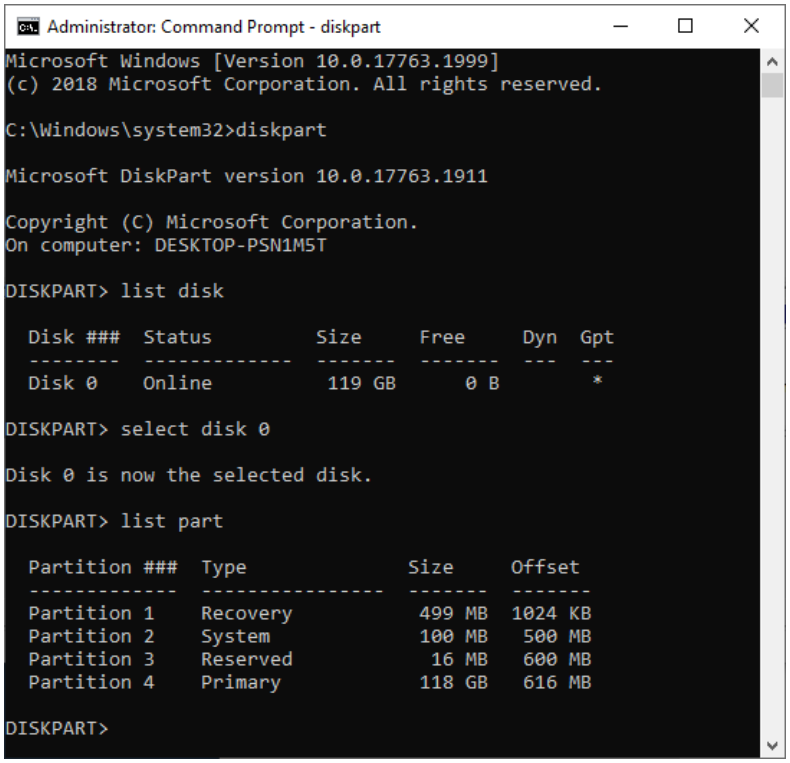
The suggested partition layout might appear as below.



The partition layout can also be checked using “diskpart” command. Search for “cmd” in the Start menu, then right-click “Command Prompt”. Left-click “**Run as administrator**”.



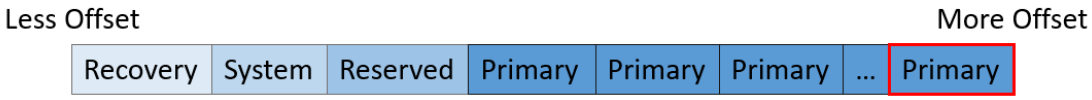
Enter “diskpart” and press Enter. At the DISKPART prompt, run “list disk”, “select disk”, and “list partition” to examine the partition layout.



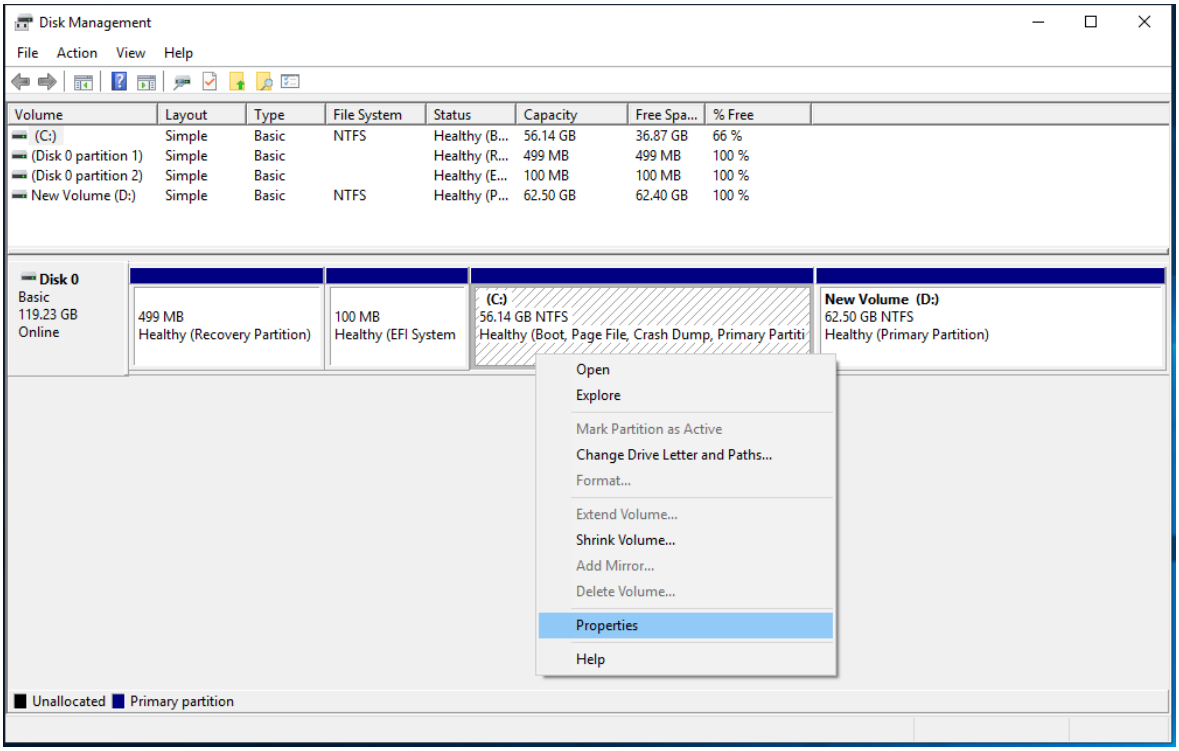
- The last partition needs enough free space to shrink.

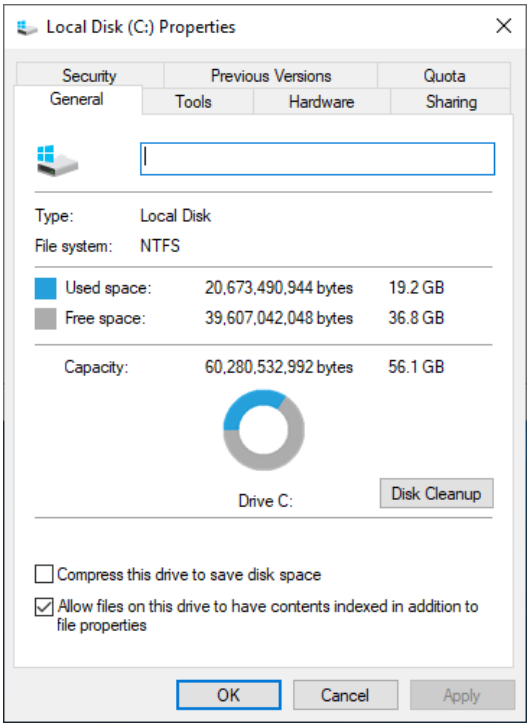
ADV Image Manager will use the last “Primary” partition to create the “ADV Backup” partition. Ensure that the last “Primary” partition can be shrunk to provide enough space greater than the used space on drive C.

The last “Primary” partition is shown below in the red frame.

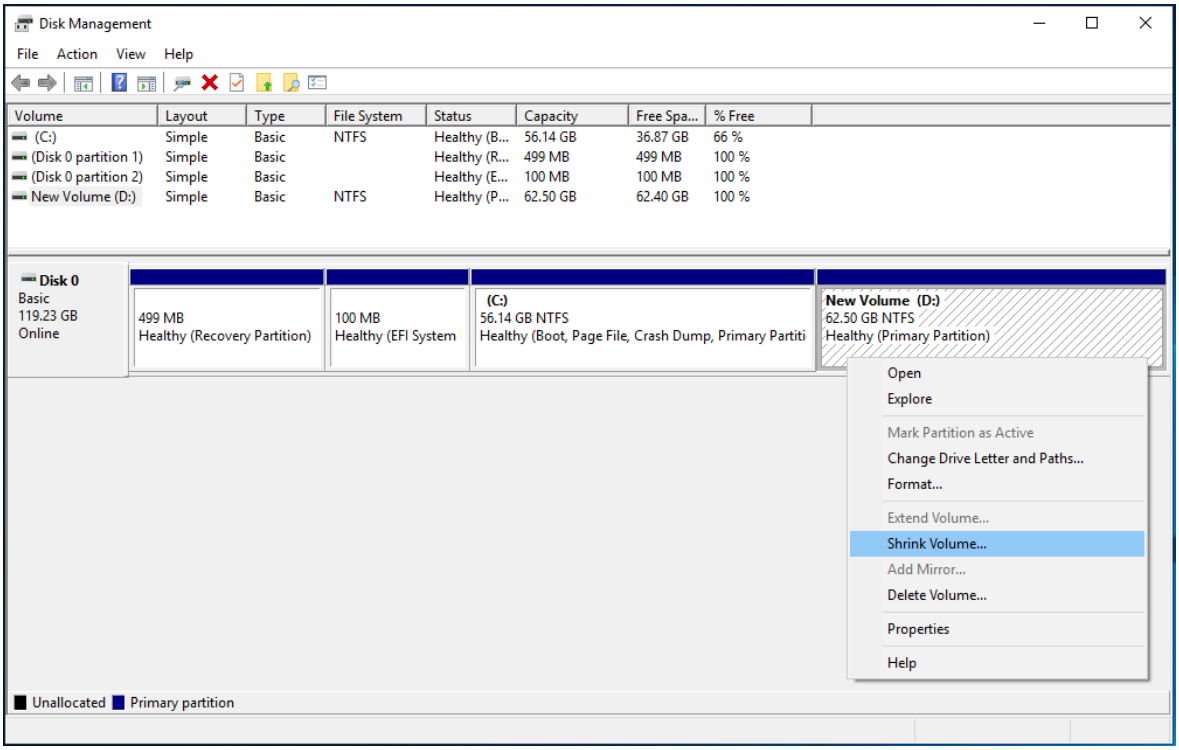


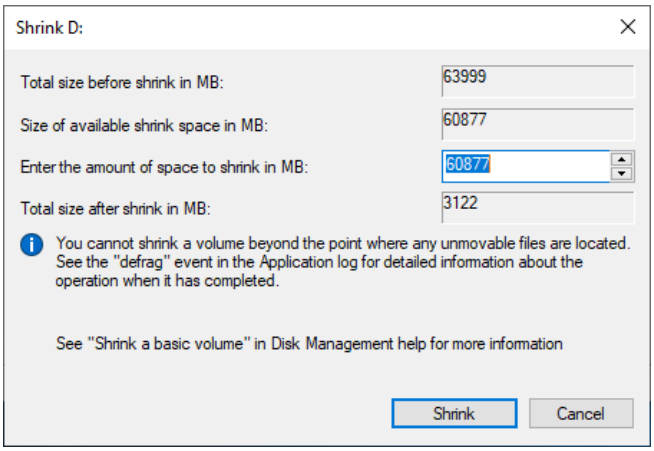
The used space on drive C can be checked by “**Properties**”. Right-click on the C:\ partition and select “**Properties**”.



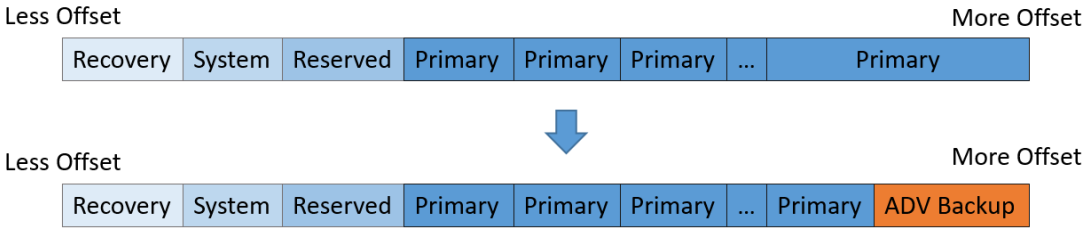


The maximum shrink space can be checked by "**Shrink Volume**". Right-click on the last partition and select "**Shrink Volume**".

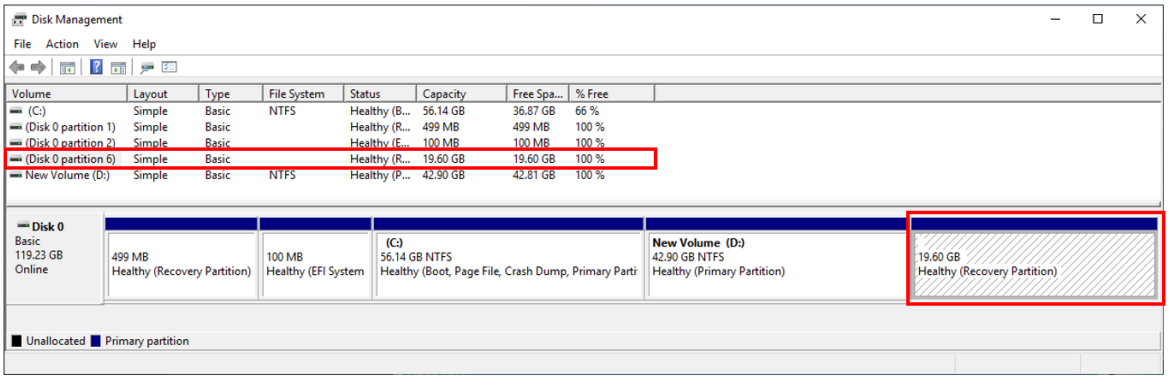




The “ADV Backup” partition will be created automatically through the ADV Image Manager environment settings, as shown in the schematic below.



For example, “ADV Backup” partition is shown below in the red frame. Please do not modify or delete this partition.

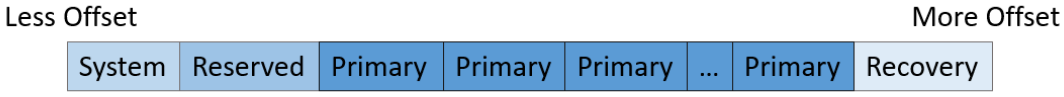


6.1.2 Windows 10 IoT Enterprise LTSC 2021 and Windows 11 IoT

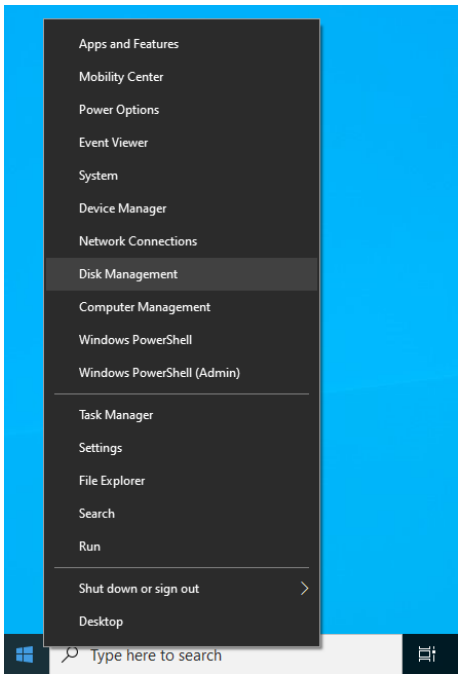
Enterprise LTSC 24H2

- This section applies to Windows 10 IoT Enterprise LTSC 2021 and Windows 11 IoT Enterprise LTSC 24H2 (x64). For Windows on ARM (WoA), refer to the next section.
- First partition needs to be the “System” partition (EFI System Partition).
- Second partition needs to be the “Reserved” partition. This partition is not shown in Disk Management.
- The “Primary” partitions are between the second partition and the last partition. “Primary” partitions are Windows partition and other data partitions.
- The last partition needs to be the “Recovery” partition.

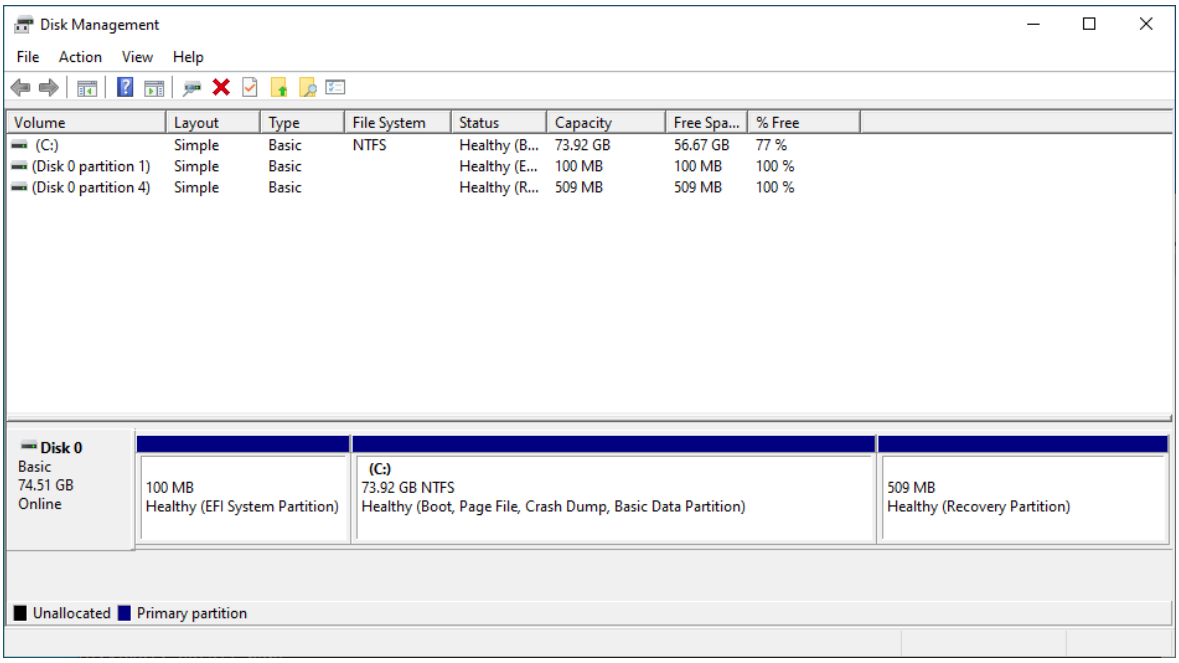
The suggestion partition layout schematic is as below.



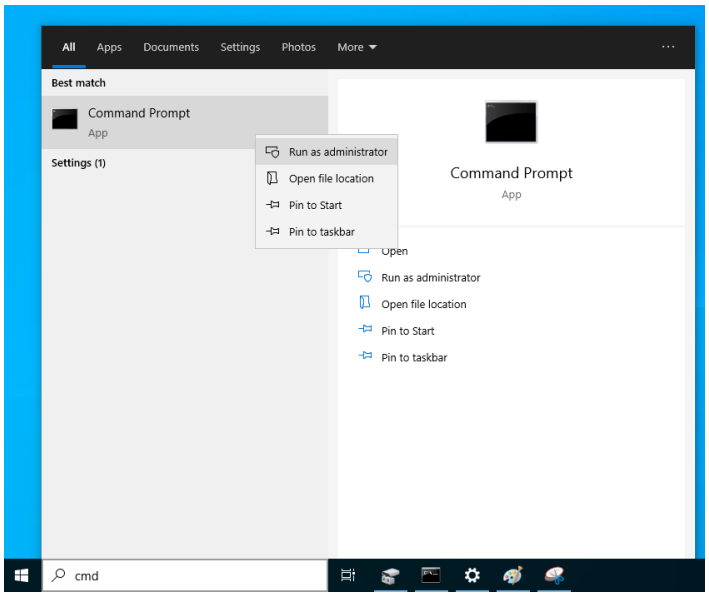
The partition status can be checked using Disk Management. Right-click on the Start button, then click Disk Management.



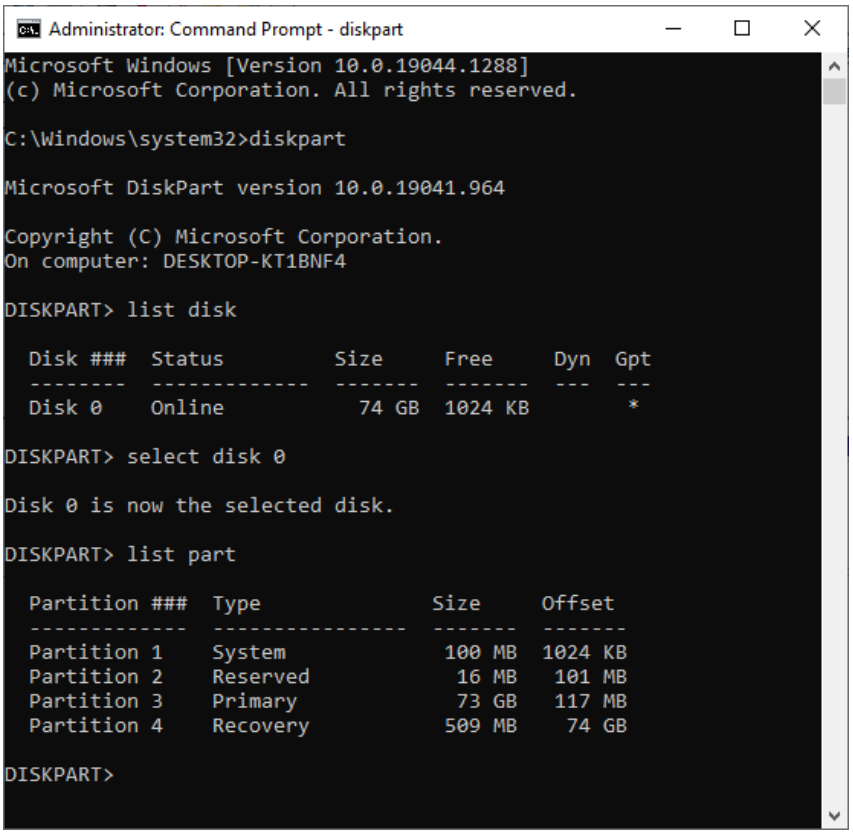
The suggested partition layout might appear as below.



The partition layout can also be checked using diskpart. Search the “cmd” in the Start menu, then right-click “Command Prompt”. Left-click “**Run as administrator**”.



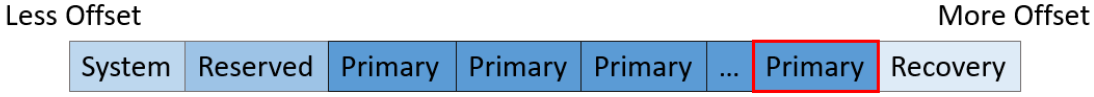
Type “diskpart” then press “Enter”. After starting diskpart, use the commands “list disk”, “select disk”, and “list part” to check the partition layout. The suggested partition layout might appear as below.



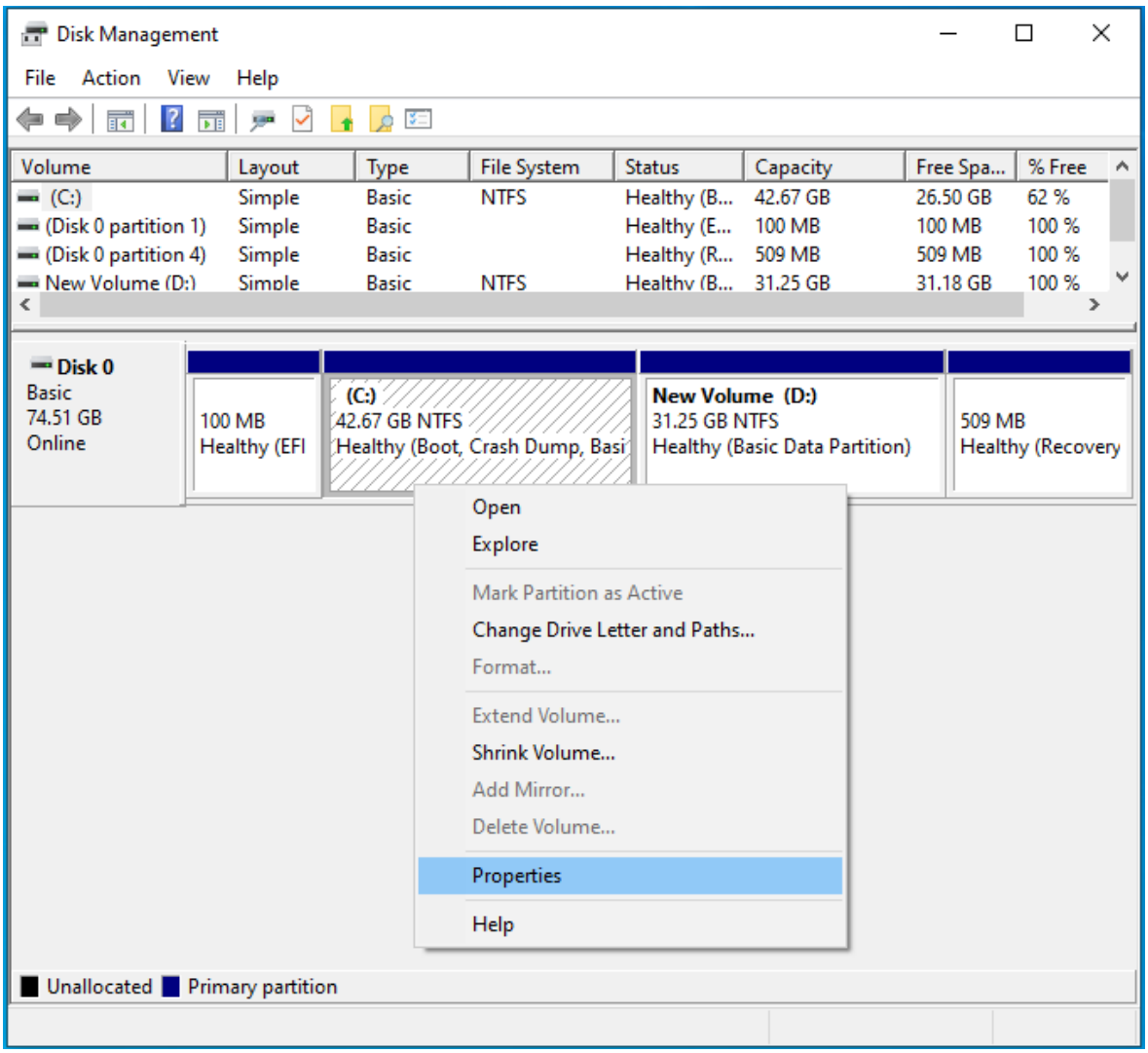
- The last “Primary” partition needs enough free space to shrink.

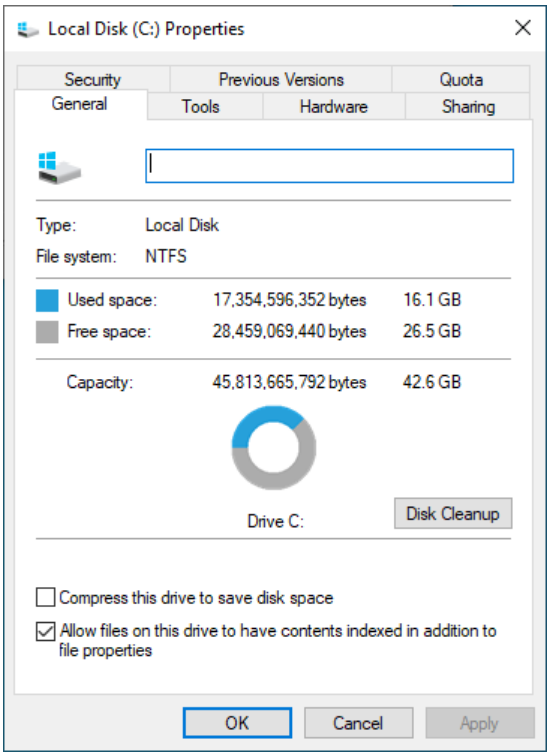
ADV Image Manager will use the last “Primary” partition to create the “ADV Backup” partition. Ensure that the last “Primary” partition can be shrunk to provide enough space greater than the used space on drive C:.

The last “Primary” partition is shown below in the red frame.

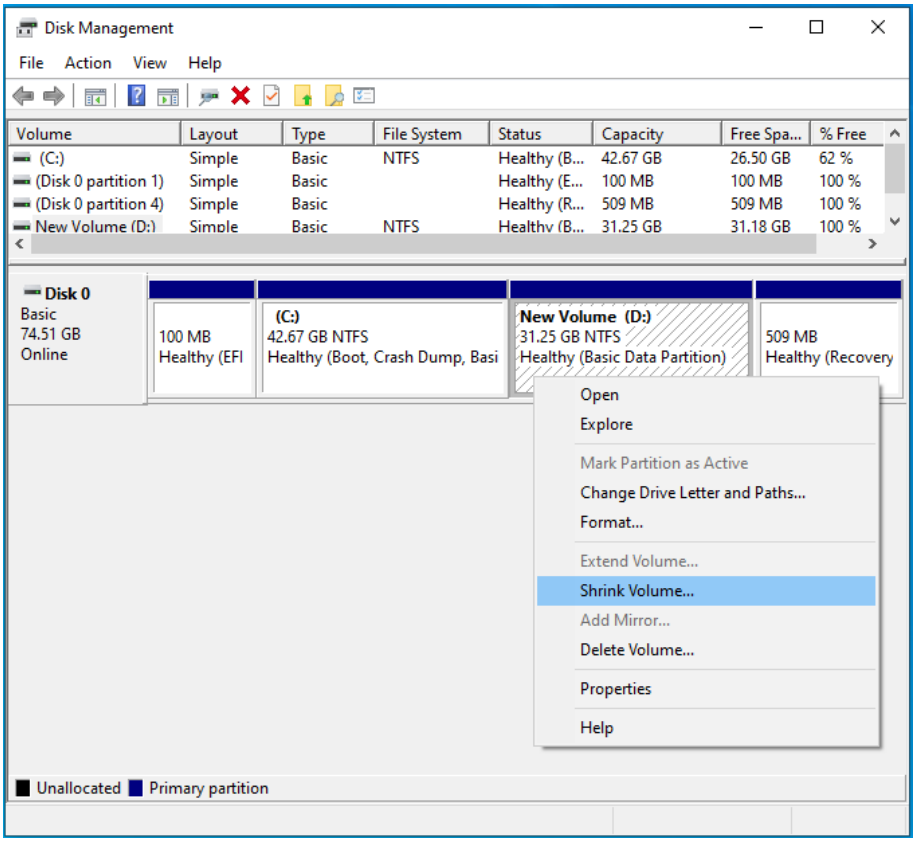


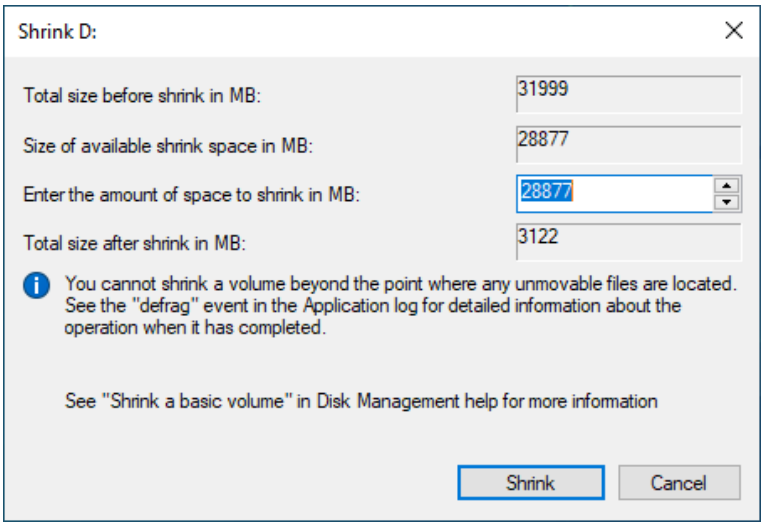
The used space on C: can be checked by “**Properties**”. Right-click on the C:\ partition and select “**Properties**”.



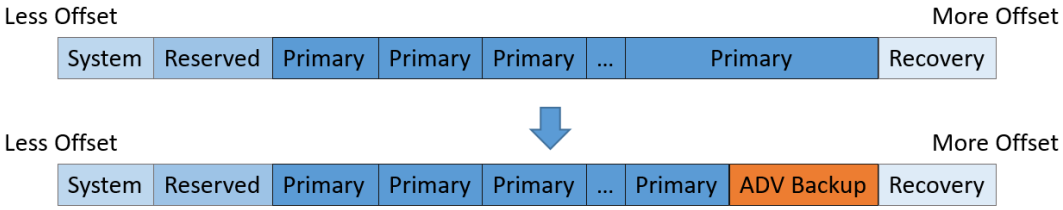


The maximum shrink space can be checked by "**Shrink Volume**". Right-click on the last "Primary" partition and select "**Shrink Volume**".

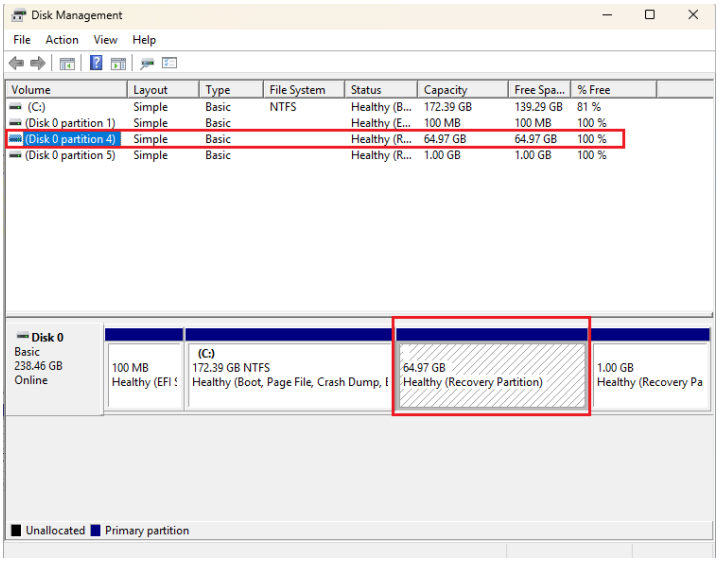




The “ADV Backup” partition will be created automatically through the ADV Image Manager environment settings, as shown in the schematic below.



For example, “ADV Backup” partition is shown below in the red frame. Please do not modify or delete this partition.



6.1.3 Windows 11 IoT Enterprise LTSC 24H2 (WoA)

- This section only applies to Windows 11 IoT Enterprise LTSC 24H2 Windows on ARM (WoA).
- The last partition must be either a “Primary” or “Recovery” partition.
- Under normal circumstances, the last partition will be “Primary”. However, if the system previously created an ADV Image Manager environment that is no longer present, the last partition will be “Recovery”.

The suggested partition layout under normal circumstances is shown below.

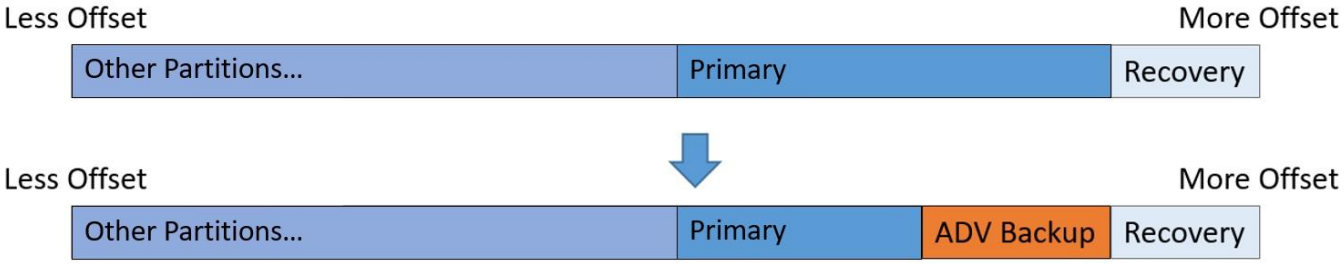
The suggested partition layout for a system that had previously created an ADV Image Manager environment, but which is no longer present, is shown below.

- The last “Primary” partition needs enough free space to shrink.

ADV Image Manager will use the last “Primary” partition to create the “ADV Backup” partition. Ensure that the last “Primary” partition can be shrunk to provide enough available space. For the first time, the available space must be greater than the total of the used space on drive C: plus an additional 1.5 GB. For subsequent times, the available space must be greater than the total of the used space on drive C:. Please refer to Section 6.1.2 for details on how to check the partition layout and verify the available shrink size.

When creating the ADV Image Manager environment for the first time, a recovery partition will be created at the end of the drive. This recovery partition is necessary for WinRE and will not be deleted when uninstalling the Advantech Power Suite. Please do not delete this recovery partition manually. The Recovery partition created by ADV Image Manager is shown below.

After that, the “ADV Backup” partition will also be created automatically through the ADV Image Manager environment settings, as shown in the schematic below. Please do not modify or delete this partition.

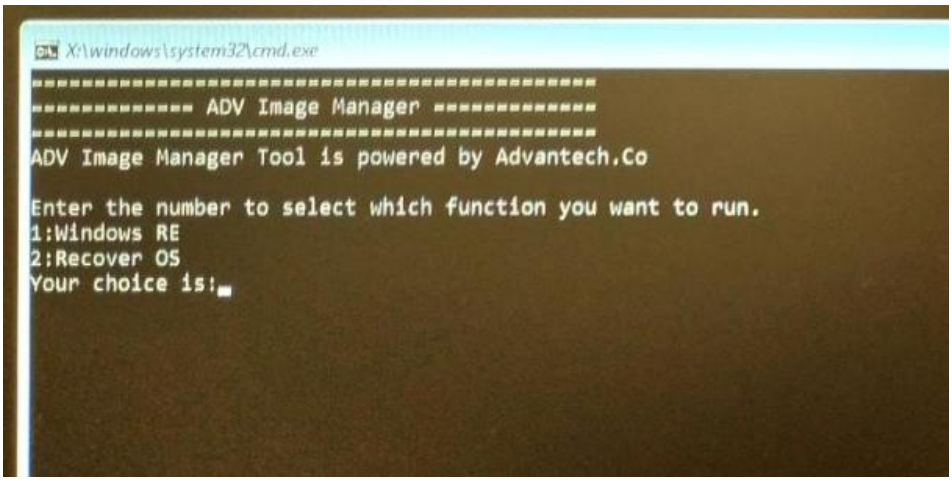


6.2 APPENDIX 2

Other WinRE Functions

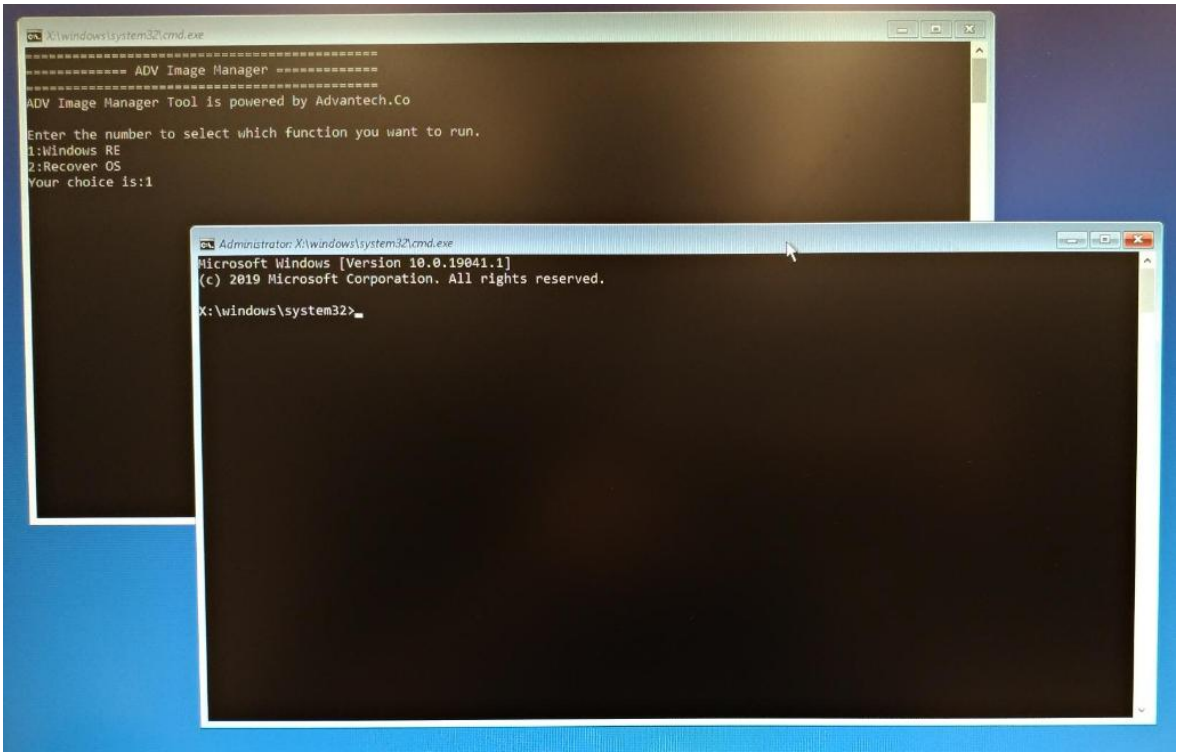
After entering WinRE, the command prompt shows function menu.

Type “1” then press “Enter” to select the Windows RE function.



After that, the WinRE function will start up as shown below.

Please keep the ADV Image Manager command prompt window running in the background and don’t close it.



6.3 APPENDIX 3

➢ BitLock

- Navigate to Control Panel > System and Security > BitLocker Drive Encryption.
- Select the C: drive and click 'Turn on BitLocker.' Follow the wizard to initialize the encryption process.
- Save the recovery key as prompted to a secure location. TLS Configuration for Data in Transit.

➢ Acronis

- To Back Up Partitions or Disks: Launch Acronis True Image OEM and select Backup from the sidebar, then click Add backup. Optionally rename the backup for easy identification. Choose Disks and partitions as the Backup source, selecting the desired partitions and disks. Select the Backup destination - Acronis Cloud, an external drive, NAS, or a specific folder. Optionally, configure backup options such as scheduling, scheme, and password protection. Initiate the backup immediately with Back up now or schedule it for later.
- To Recover Partitions or Disks: Open Acronis True Image OEM and ensure connection to Acronis Cloud if necessary. In the Backup section, choose the relevant backup and navigate to the Recovery tab to select Recover disks. Choose the backup version by date and time, then select disks or partitions for recovery. Choose the recovery destination, noting that all data on the destination will be replaced. Optionally, configure additional recovery parameters. Start the recovery process with Recover now.
- For more detailed instructions, please refer to the Acronis manual.

➢ Trellix

- Launch the Trellix Whitelisting Manager and enter the management password set during installation.
- Navigate to the 'whitelist' section and select 'Add All' to automatically include all relevant system files for protection Allow the program to complete the process of adding all files to the protection list.
- Open the Trellix Solidifier Command Line with Administrator privileges and execute the following command: 'sadmin features disable mp-casp'
- Return to the Trellix Whitelisting Manager and enable the System Protection switch to activate comprehensive security measures.
- For more detailed instructions, please refer to the Trellix manual.

6.4 APPENDIX 4

Change History

Version	Change content	Status
V2.0.8	Initial version	Released
V2.0.13	Add Security Diagnosis	Released
V2.0.15	OS Enhancement - General Settings - Energy - Wi-Fi Filter	Released
V2.0.18	ADV Image Manager - Support WoA	Released
V2.0.19	ADV Image Manager - Encrypt/Decrypt Backup Recovery System Information - Check for Updates OS Enhancement - WoA Firmware Update	Released
V2.1.0	ADV Image Manager - Multiple Backup Recovery - Bootable USB Media Security Manager - Rename “Security Diagnosis” to “Security Manager” - WDAC Allow Listing - Bitlocker Send Google Analytics Events	Released