Windows 10 IoT Lockdown Utility

User Manual

V1.7

Embedded IoT SW

Windows 10 IoT Lockdown Utility User Manual

Foreword

In Windows 10 IoT Enterprise, Microsoft removes Embedded Lockdown Manager which manages embedded lockdown features. Therefore, Advantech designs Windows 10 IoT Lockdown Utility to allow users to customize Win 10 IoT Enterprise OS image more quickly and intuitively.

Requirements

I.   Windows 10 IoT Enterprise LTSB&LTSC (included 2016 , 2019 , 2021).
II.   Corresponding to Win 10 lockdown utility v1.3.0.4
III. The user account must have administrator privileges
IV.   Before starting to experience this tool, please fill-in user information before start to use this tool.

Embedded IoT SW

Limitation

I.   After sysprep, the setup of below items would be removed:

Section

2.2 - Automatic Logon

5.1 - Advanced Boot Option: Loginscreen

5.2 - Ctrl+Alt+Del Screen Option: Lock/Sign out/change a Password/Task Manager

II.   If set shell launcher and automatic logon at the same time, after sysprep, the system will not be able to enter into OOBE normally. Do not sysprep after setting these 2 functions.

Embedded IoT SW

Introduction

1. Lockdown Settings
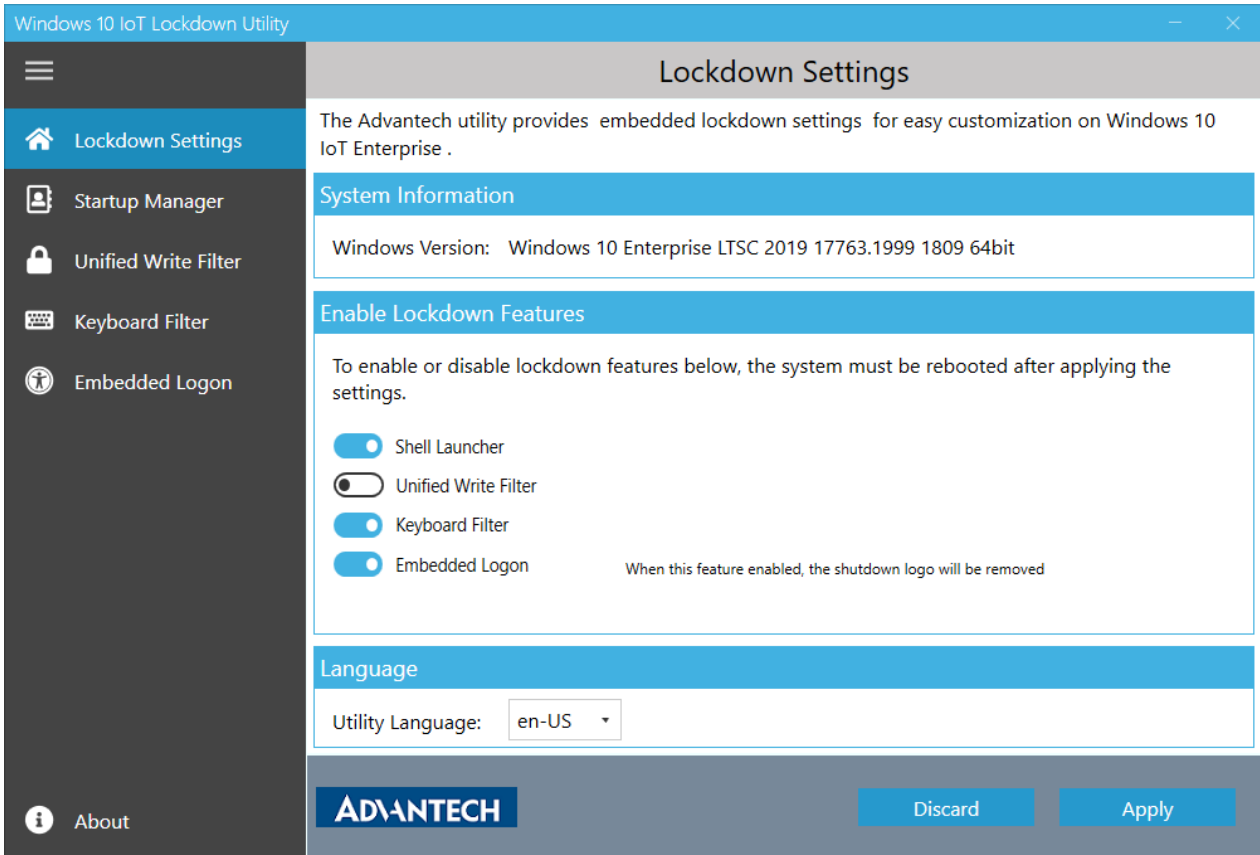
1.1 System Information

It shows Windows version and build numbers of your device. Windows 10 IoT Lockdown Utility only supports build version later than 10586(RTM).

1.2 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.
Please make sure toggle switches to be enabled before setting the functions from the menu on the left.
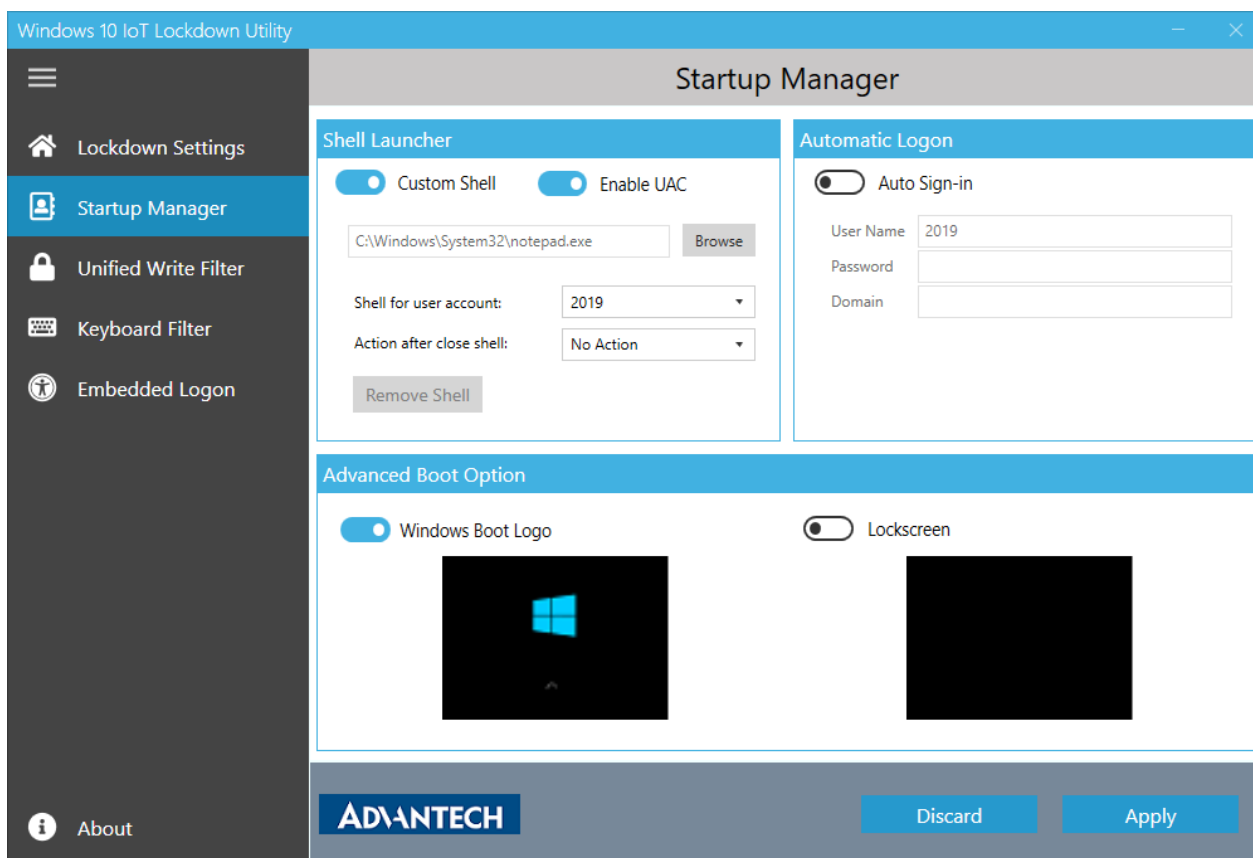
1.3 Language

Lockdown utility is multilingual, you could choose the desired language and restart the utility to see

Embedded IoT SW

it's changed to the selected language.

＊**Note:** Lockdown utility is currently available in English and traditional Chinese. Your language is not yet included? Please contact your local FAE to add your language.

2   Startup Manager

2.1   Shell Launcher

You can use Shell Launcher to replace the default Windows 10 shell with a custom shell (APP). When you enable "Custom Shell", you need to choose a custom shell which will be executed automatically after system boot up.

If custom shell needs to be run with administrator privileges, you need to disable User Account Control (UAC). Otherwise custom shell won't be executed.

＊**Note:** the UAC in User Account Control Settings is for user to enable/disable the notice message sending to remind user the items to be setting requires account control authorization. This is different with the UAC function in Lockdown Utility.

2.1.1 Shell for user account: You may assign different shells for different user accounts. The default user account would follow the Windows user account.

2.1.2 Action after close shell: Action Under the custom shell environment, you may decide the action of the system when the shell to be forced closed. Options including: **No Action**, **Shutdown Computer**, **Reboot Computer** and **Restart Shell**. When you close shell (APP), the

6

chosen action will be run.

2.1.3 Remove shell: Click this button to remove the assigned shell from device.

2.2   Automatic Logon

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

＊**Note:** After sysprep, the setup of automatic logon would be removed.

2.3   Advanced Boot Option

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

3   Unified Write Filter

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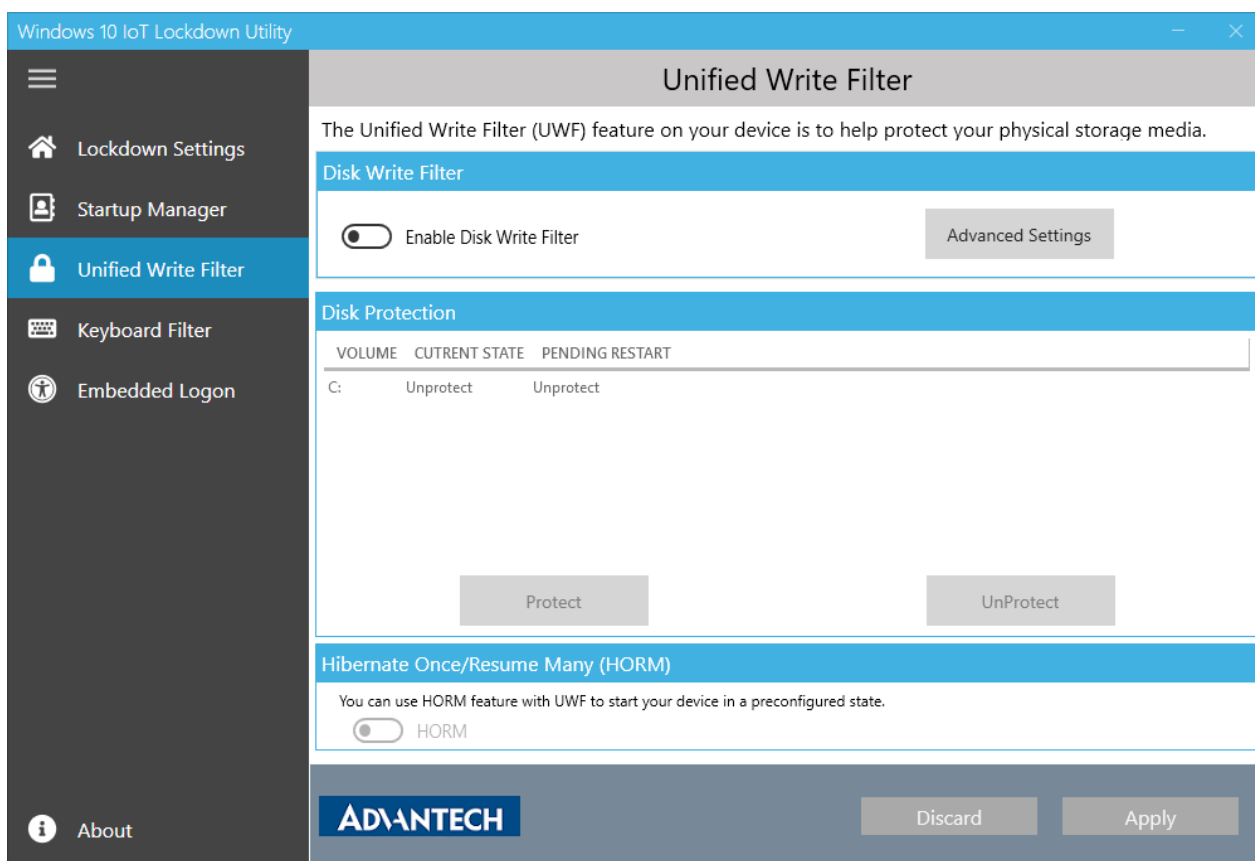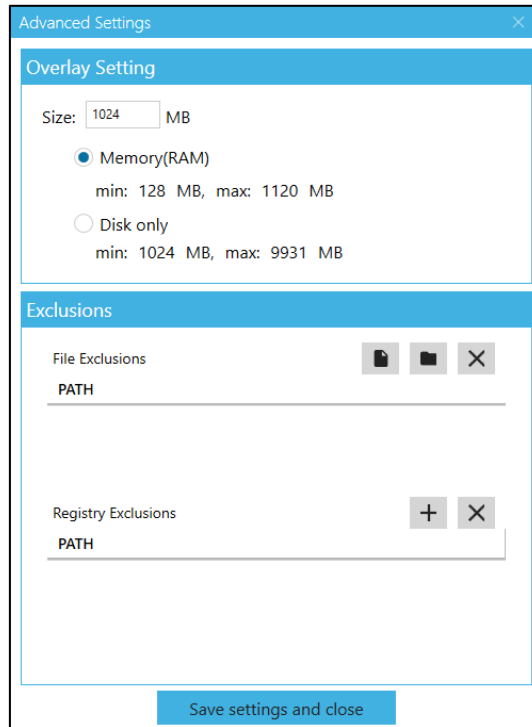

3.1   Disk Write Filter

After enabling Disk Write Filter, you **cannot modify advanced settings** because of dependency.

Embedded IoT SW

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 become read-only, 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.

＊**Note**: Please enable "Disk Write Filter" before go to next action, "Disk Protection".

3.2 Disk Protection

This area lists all volumes on the device. If you want to use Disk Write Filter, It's necessary to indicate how many volume you would to protect.

<u>You cannot use UWF to protect external removable Medias.</u>

＊**Note**: If you already protect disk and then you would like to disable "Disk Write Filter", please unprotect disk first.

3.3 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 or disable HORM. UWF must be configured in the

Embedded IoT SW

following ways to protect the hibernation file from becoming invalid:

I.   All fixed volumes mounted on the system must be protected by UWF.

II.   Your system must not contain any file, folder, or registry exclusions configured for UWF.

III.   The UWF overlay must be configured to use RAM mode. HORM does not support disk-backed overlays.

https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/hibernate-once-resume-many-horm-

＊**Note1**: 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.

＊**Note2**: Once the system enter into Hibernate once with HORM enable, the next HORM enable action will resume from the previous Hibernate status.

In Win 10 IoT Ent 2021 LTSC, since the enablement of read only media is a required condition. We will try to help you to open read only media in advanced if the use of HORM is confirmed (see below UI).
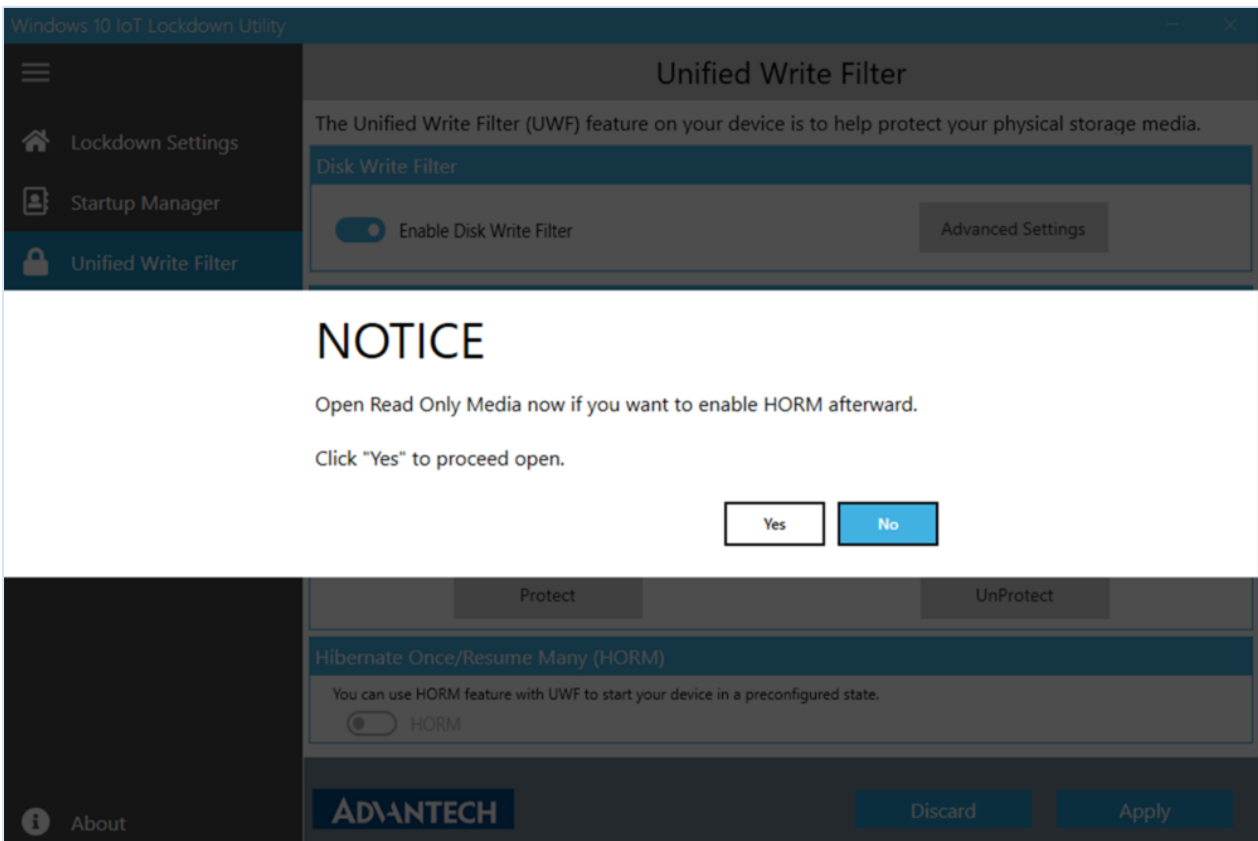
However, if you would like to enable HORM under the condition of UWF is enable and read only media is disabled. Then please disable UWF first to enable read only media and HORM afterward. Otherwise the settings under UWF is enabled would be invalid.

4   Keyboard Filter

Embedded IoT SW
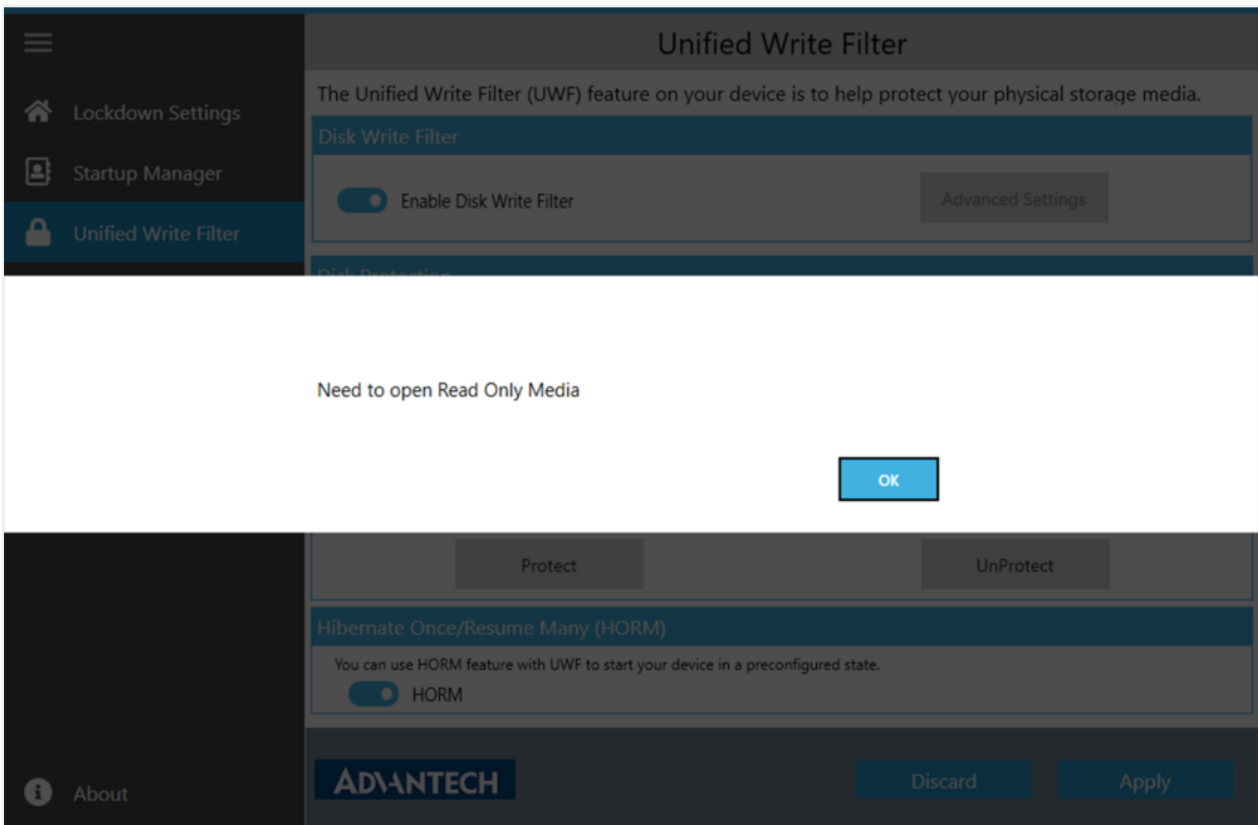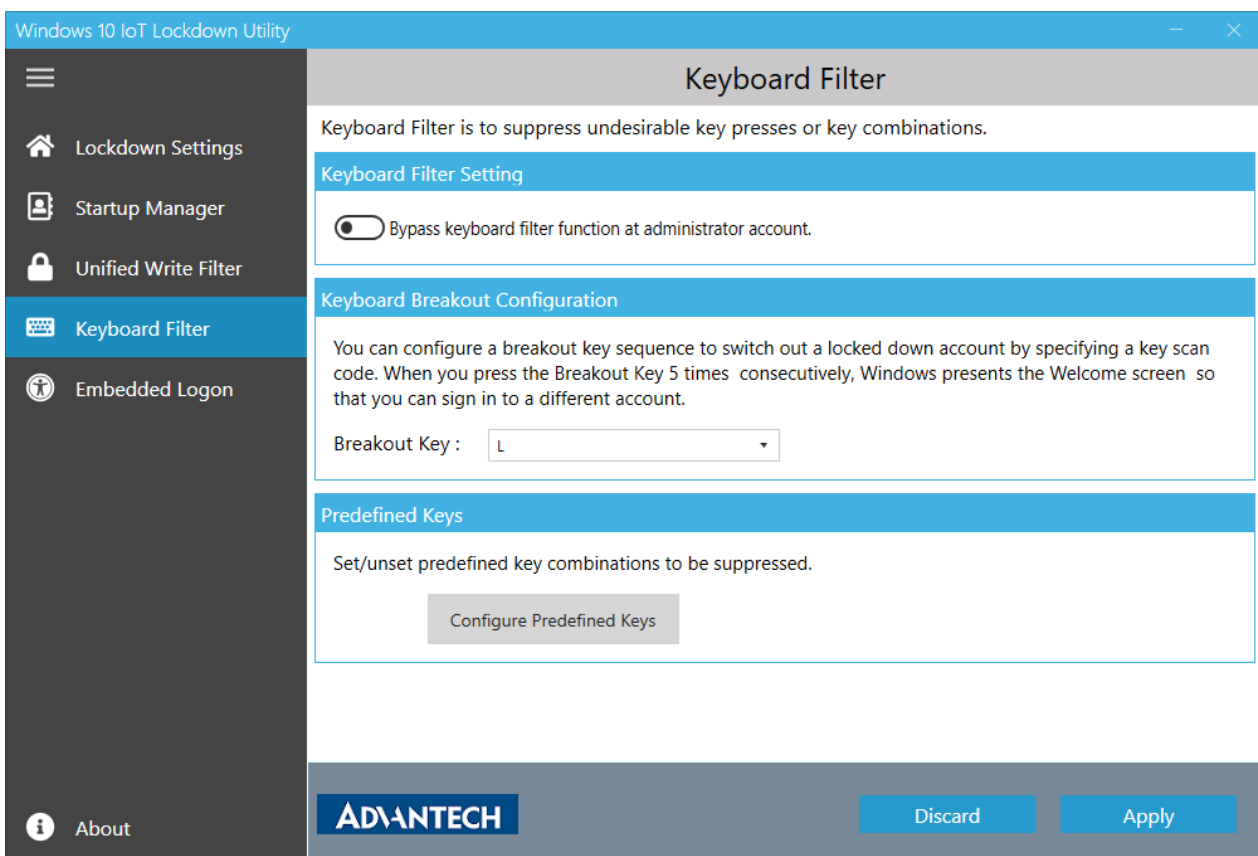
4.1   Keyboard Filter Setting

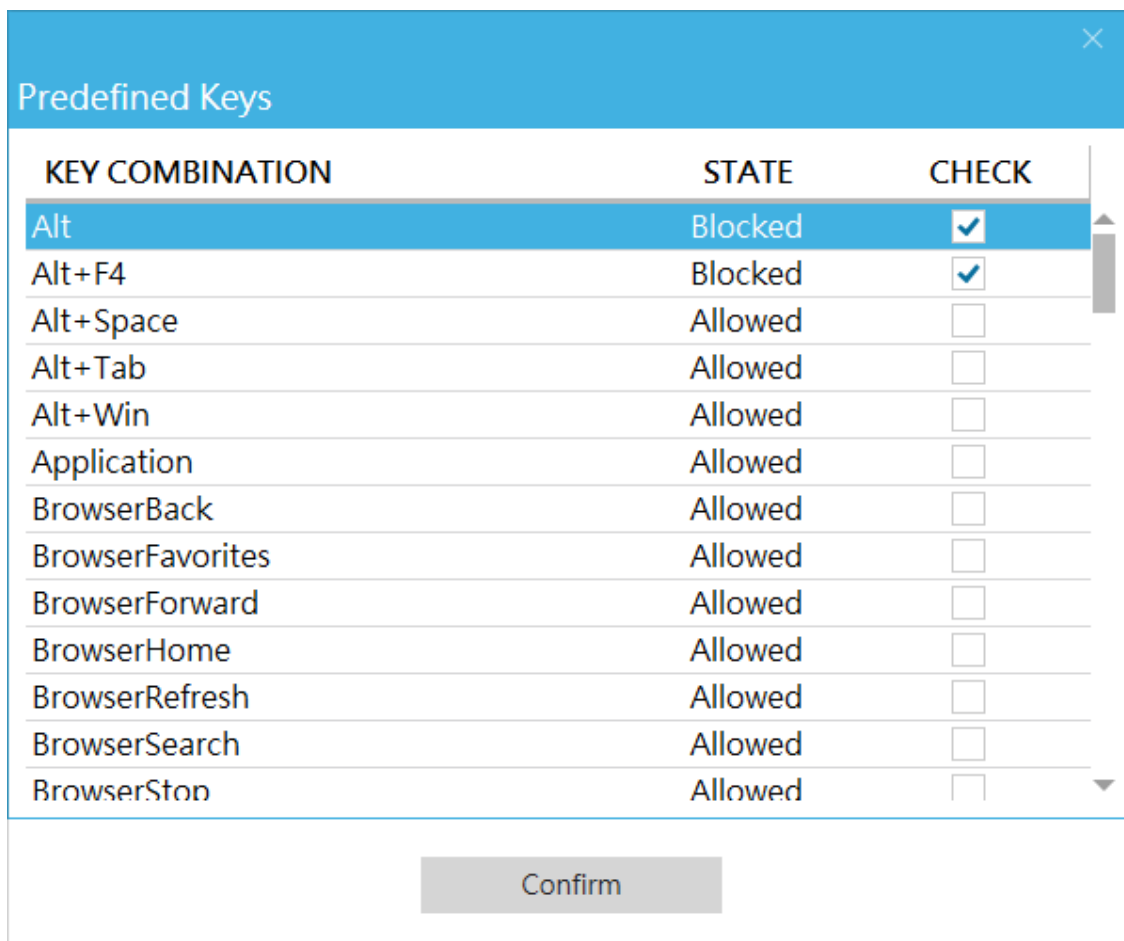You have to enable the setting to avoid being restricted keyboard use under administrator account.

4.2   Keyboard Breakout Configuration

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.

4.3   Predefined Keys

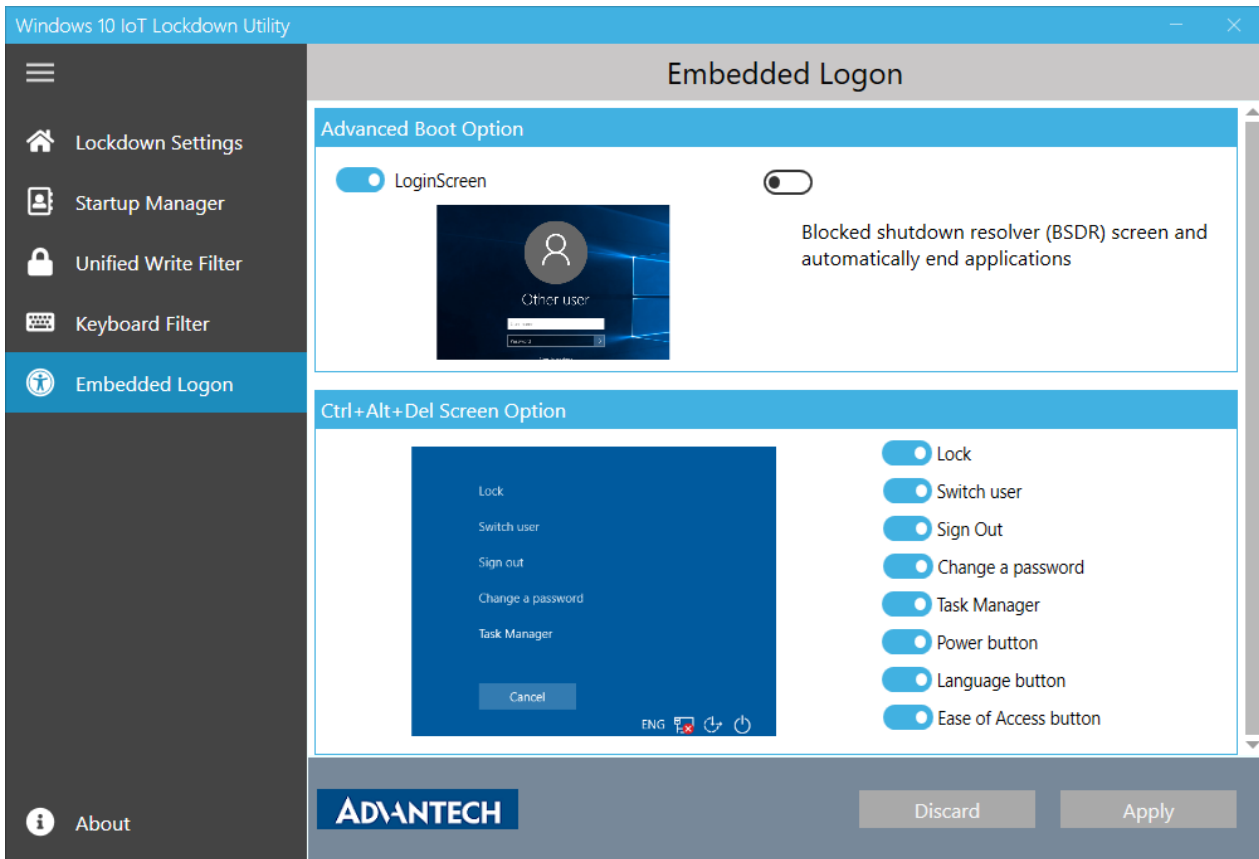We provide predefined keys which are defined by Microsoft.
The default setting is to allow all of the predefine keys. If you want to block keys for your users, check the items that you want to block, and click "Confirm". This key combination will be blocked.

11

Embedded IoT SW

5   Embedded Logon

5.1   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 "Startup Manager" 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.

＊**Note:** After system prepare, the setup of Loginscreen would be removed.

5.2   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.

＊**Note:** After system prepare, the setup of Ctrl+Alt+Del (Lock/Sign out/change a Password/Task Manager) would be removed.

Embedded IoT SW

Through the configuring on the utility, you can efficiently customize and build up your Windows 10 IoT Enterprise image. Should you have any suggestion, please feel free to feedback to us Suggestion Link.

APPENDIX

Change History

Version	Change content	Status
V1.1		Released
V1.2	Add P3-Limitations	Released

V1.3	Add
	    P3-Requirement: 2019 LTSC
	    P6-3.1 Note
	    P7-3.1 Note
	Update
	    P11-Windows Update
		Released

V1.5	Add
	P3-Requirement
	P4-Limitation
	P6-2.1.1:Shell for user account
	P7-2.1.3: Remove Shell
	P9-Notice for HORM
	P13- Note for disable Automatic Windows update
	        6.4.3:Hibernate
	        6.4.4_Microsoft defender
	        6.5.1:Black screen when BSOD
	        6.5.2:Action center
	        6.7:Device Control
		Released

V1.6	Add P4-Requirement P5-Limitation P10-HORM P15-6.4.2:Windows setting	Released
V1.7	Add P5-Language	Released