UNIFIED CONFIGURATION TOOL GUIDE

INTRODUCTION

The Unified Configuration Tool (UCT) is a Microsoft Management Console (MMC) snap-in which enables local and remote management of Lockdown and Branding features installed on a Windows Embedded Standard 8 device. UCT supports configuring settings for Keyboard Filter, Dialog Filter, Unified Write Filter, and Custom Shell Launcher all from a single graphical interface making configuration of Windows Embedded devices more accessible to a wider audience spanning embedded developers to IT pros.

STEP 1: INSTALL UCT AND CONNECT TO YOUR DEVICE

You can either install UCT directly on your device, or you can install it on your computer and then connect remotely to your device. Your device must be connected to a network if you want to use UCT remotely to configure your device. If you install UCT on your computer, you also need to configure your device for remote management.

HARDWARE REQUIREMENTS

The computer or device must meet or exceed the following requirements:

- 1 GHz 32-bit or 64-bit processor
- 1 GB of operating system memory (32-bit system) or 2 GB of operating system memory (64-bit system)
- 2 GB of free hard drive space for complete installation

SOFTWARE REQUIREMENTS

The computer or device must meet or exceed the following requirements:

- It must be running one of the following operating systems:
  - Windows 7
  - Windows 8
  - Windows Embedded Standard 8
- It must have the following software installed:
  - .NET Framework 2.0 on Windows 7
  - .NET Framework 4.0 or higher on Windows 8 and Windows Embedded Standard 8
  - Microsoft Management Console (MMC)

To install UCT

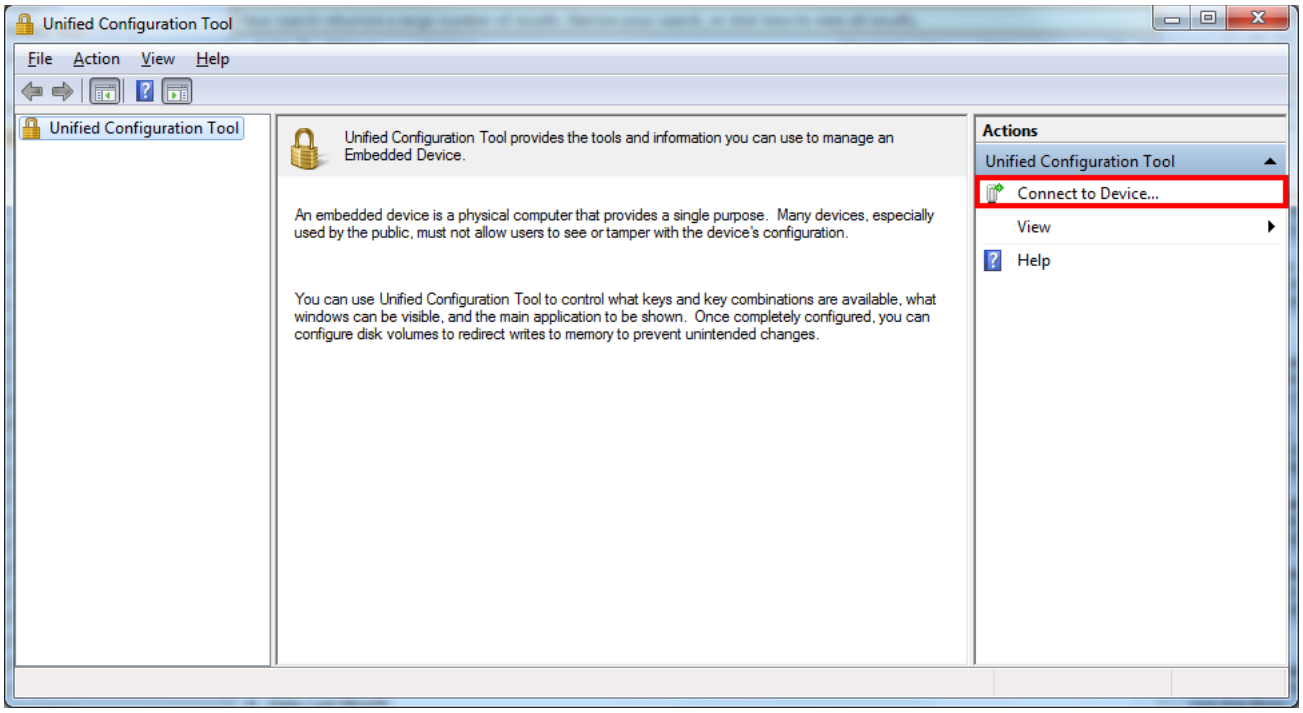
1. On the Windows Embedded Standard 8 Toolkit disk, run EmbLockSetup_x86.msi for 32-bit computers and devices, or EmbLockSetup_amd64.msi for 64-bit computers and devices.
2. In the installation wizard, follow the instructions.
3. Click **Start**, type **Unified**, and then under Programs, click **Unified Configuration Tool**.

To configure your device for remote management

1. In UCT, press F1 to open Help.
2. In the Help window, navigate to **Configure a Device for Remote Management**, and then follow the instructions.

To connect UCT to a Windows Embedded Standard 8 device

1. In UCT, on the **Actions** pane, select **Connect to Device**.



2. In the **Select Computer** dialog box, do one of the following:
   - If you installed UCT on your Standard 8 device, select **Local Computer**, and then click **OK**.
   - If you installed UCT on your computer, select **Another Computer**, and then do the following:
     - In the text box, enter the name of your Standard 8 device.
     - Click **Set User** and then enter the user name and password of the administrator account to use to connect to the device.

Important

You must use an administrator account to connect to a device. If you attempt to connect to a device by using a non-administrator account, Embedded Lockdown snap-in becomes unresponsive until the connection attempt times out.

STEP 2: USE UCT TO CONFIGURE YOUR DEVICE

This section walks through examples of configuring lockdown settings on your device. Each example is independent of the other examples, and you can follow them in any order.

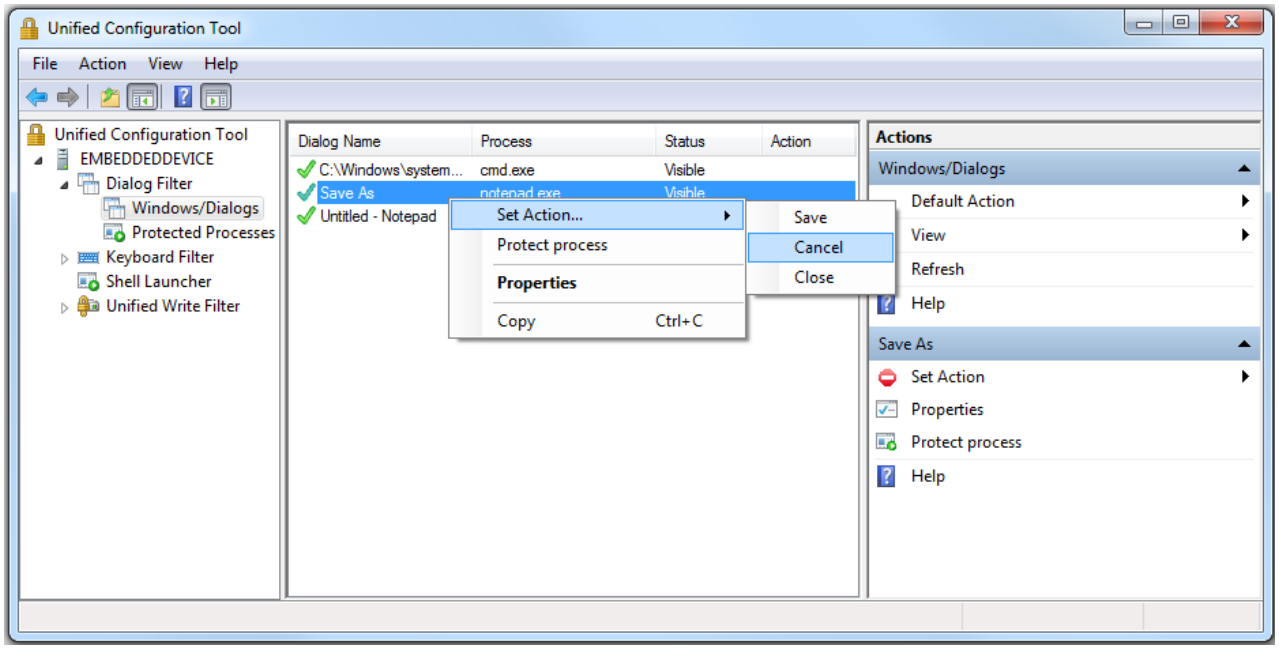
CONFIGURE DIALOG FILTER

You use Dialog Filter to control which pop-up windows and dialog boxes are displayed by the OS.

The easiest way to configure Dialog Filter is to use UCT to capture information about active windows and dialog boxes on your device.

To block the Save As dialog box in Notepad

1. On your device, open Notepad.exe.
2. In Notepad, on the **File** menu, click **Save As**, and leave the **Save As** dialog open.
3. In UCT, expand **Dialog Filter** and then select **Windows/Dialogs**.
4. In the **Actions** pane, click **Refresh** to make sure UCT reflects the current state of the device.
5. In the center pane, under **Dialog Name**, right-click **Save As**, point to **Set Action**, and then click **Cancel**.



6. On your device, in Notepad, verify that you cannot open the **Save As** dialog box.

ONLY SHOW DIALOG BOXES FROM SELECT PROCESSES

You can configure Dialog Filter to hide all non-administrator dialog boxes and windows except for those opened by selected processes. You do this by marking specific processes as protected and then setting the default action to close. Marking a process as protected means that the default action is not applied to any window or dialog that is created by that process.

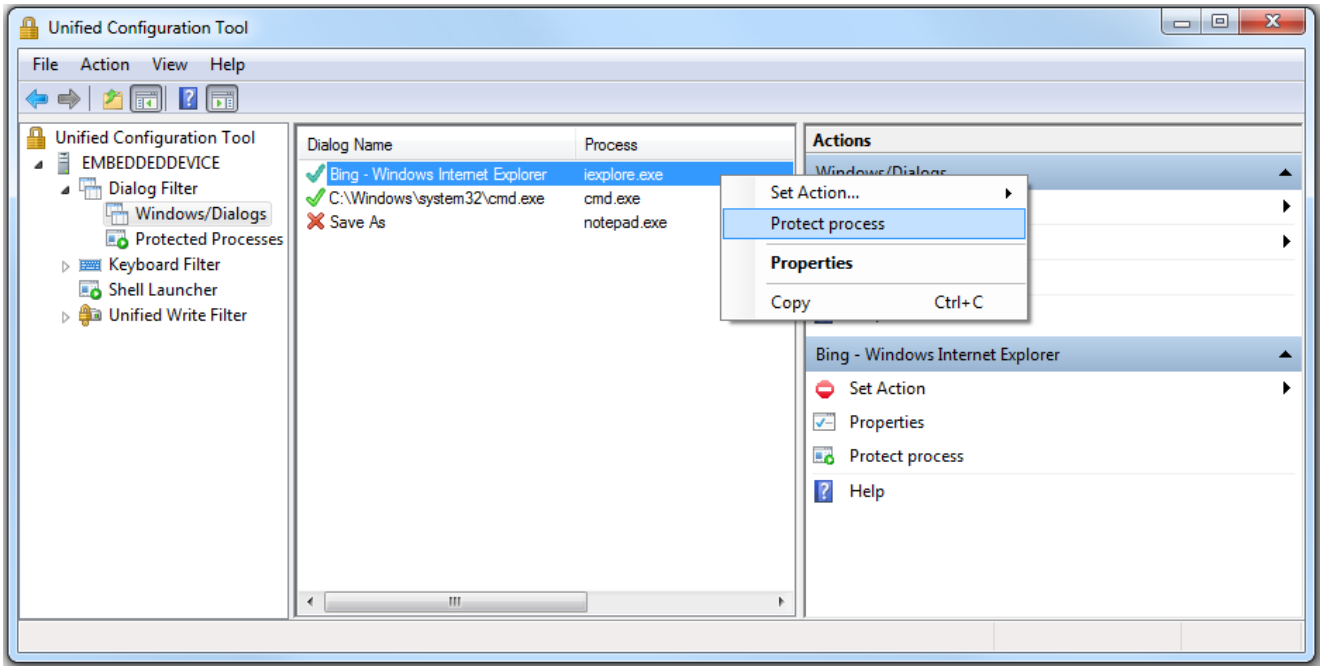
Before setting the dialog boxes or windows to close, be sure to view the processes running on your device and protect the critical processes in order to avoid unexpected behavior. For example, if you are using the Windows 8 Shell, you must add C:\windows\explorer.exe to the protected processes list to avoid loss of shell functionality, such as the Start menu and the charms bar.

Important:

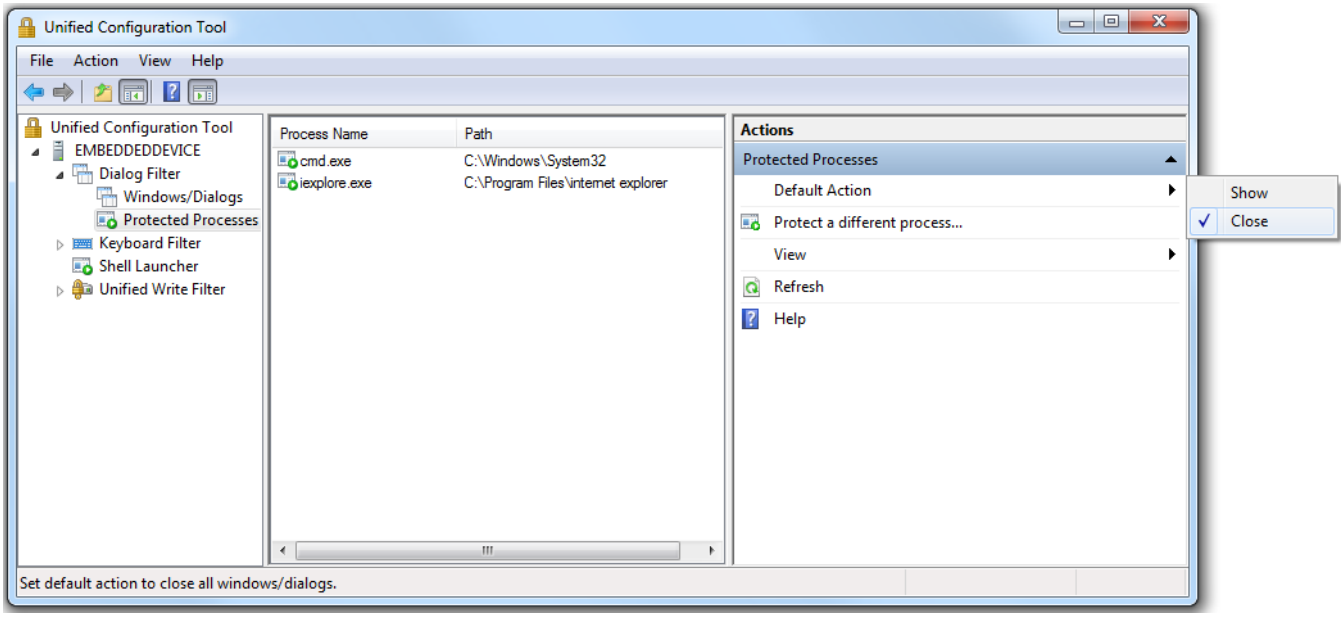
If you run UCT on your device, you must protect the mmc.exe process to allow UCT to continue to run.

To close all dialog boxes except those opened by Internet Explorer

1. On your device, start Internet Explorer.
2. In UCT, expand **Dialog Filter** and then select **Windows/Dialogs**.
3. In the **Actions** pane, click **Refresh** to make sure UCT reflects the current state of the device.
4. In the center pane, under **Process**, right-click **iexplore.exe** , and then click **Protect process**.



5. If Shell Launcher is installed on your device, under **Process**, right-click your shell, for example cmd.exe in the previous screenshot, and then click **Protect process**.
6. In the left pane, expand **Dialog Filter** and then click **Protected Processes**.
7. In the **Actions** pane, click **Default Action** and then click **Close.**



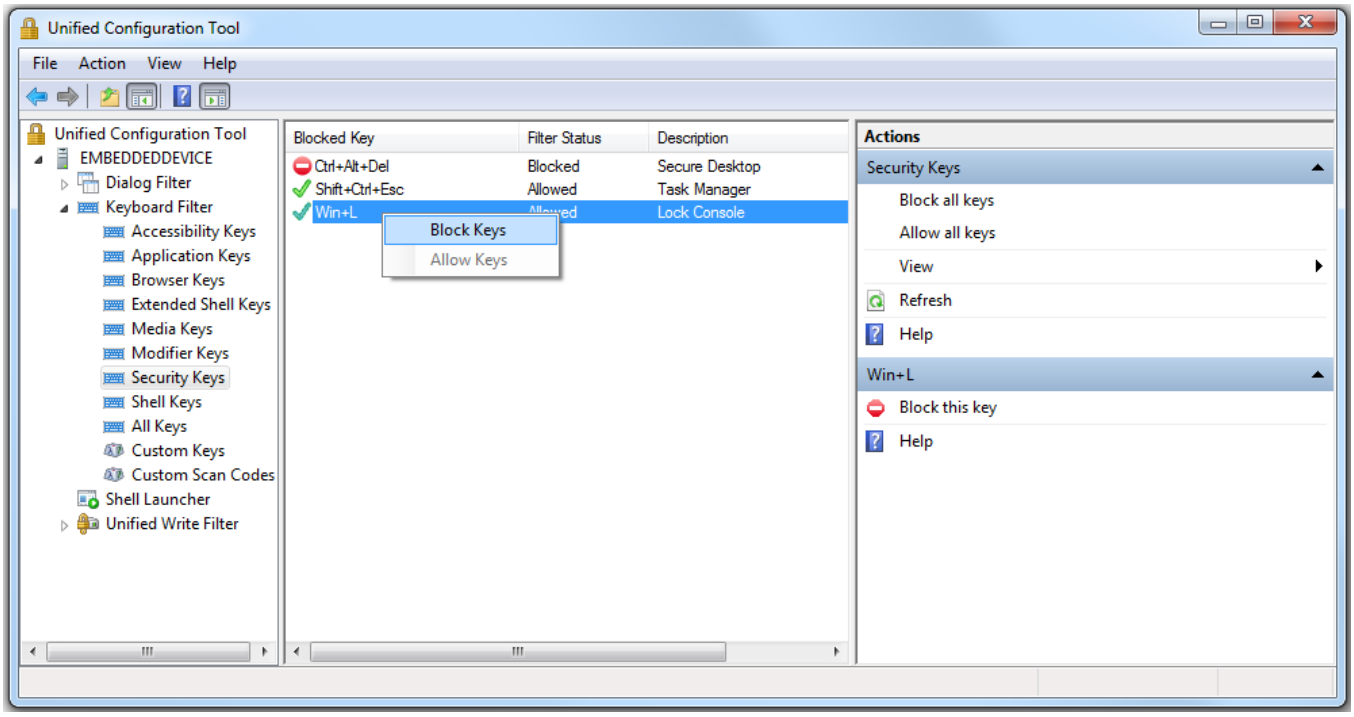
On your device, all non-administrator windows will automatically close when opened, except for windows opened by Internet Explorer. If you have marked other processes that you have marked as protected they will also automatically close.

CONFIGURE KEYBOARD FILTER TO PREVENT LOCKING THE DEVICE

You can use Keyboard Filter to lock down specific key combinations on your device, for example to block Ctrl+Alt+Del or Windows logo key+L so that users cannot lock the device.

To block key combinations that can lock the device

1. In UCT, expand **Keyboard Filter** and then select **Security Keys**.
2. In the center pane, under **Blocked Key**, right-click **Ctrl+Alt+Del**, and then click **Block Keys**.
3. In the center pane, under **Blocked Key**, right-click **Win+L**, and then click **Block Keys**.



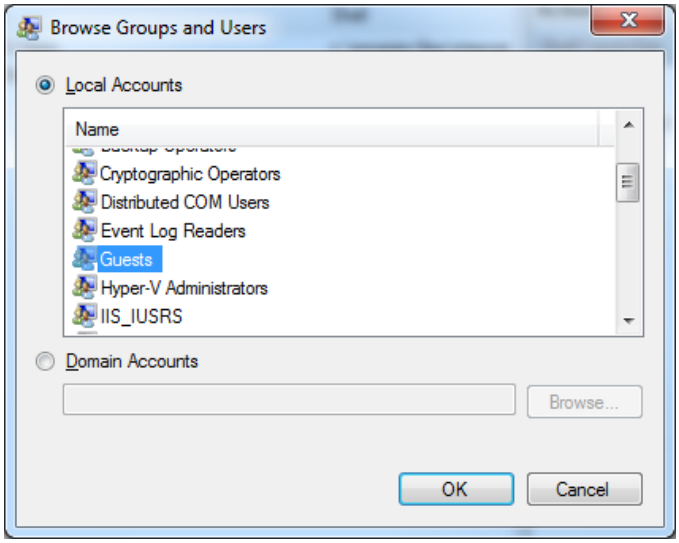
4. On your device, verify that you cannot lock the screen by pressing Win+L or Ctrl+Alt+Del.

CONFIGURE SHELL LAUNCHER TO LAUNCH INTERNET EXPLORER FOR GUESTS

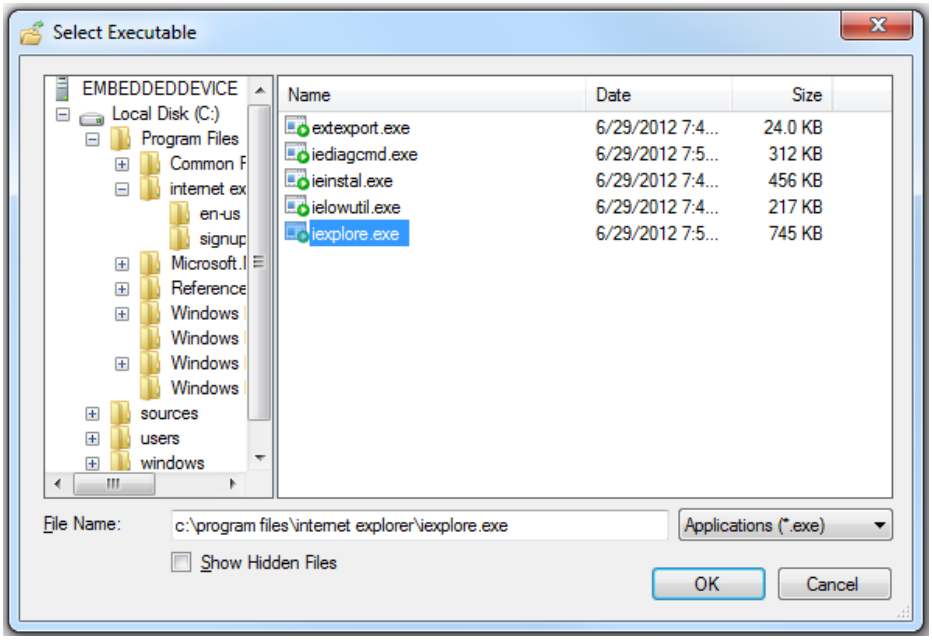
You can use Shell Launcher to launch a custom program as the shell instead of the standard Windows 8 shell. You can configure specific shells to be launched for specific users or for user groups.

To configure Shell Launcher to launch Internet Explorer as the shell for Guest accounts

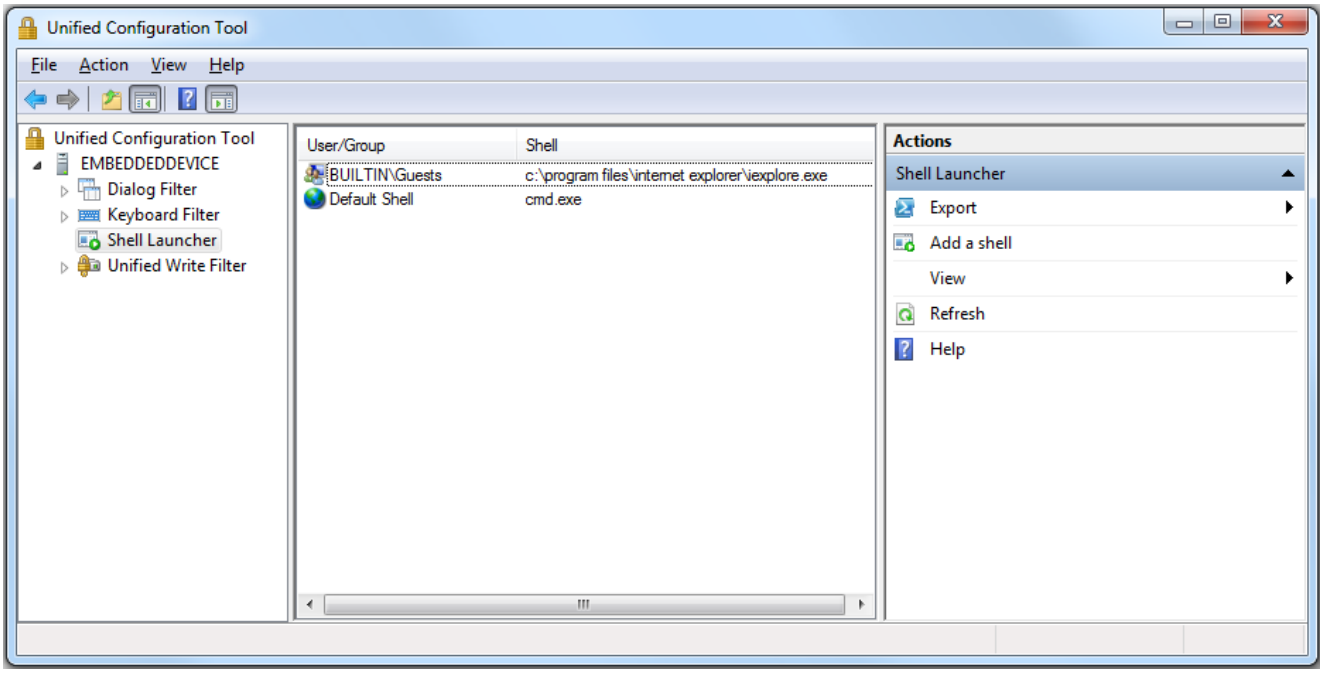
1. In UCT, navigate to **Shell Launcher**.
2. In the **Actions** pane, click **Add a shell**.
3. In the Shell Launcher dialog box, in **User or Group Name**, click **Edit**.
4. In the **Browse Groups and Users** dialog box, under **Local Accounts**, select **Guests**, and then click **OK**.



5. In the **Shell Launcher** dialog box, under **Shell Executable**, click **Browse**.
6. In the **Select Executable** dialog box, navigate to C:\Program Files\internet explorer, select **iexplore.exe**, and then click **OK**.



7. In the **Shell Launcher** dialog box, click **OK**.
   UCT now appears as shown in the following figure.



8. On your device, sign in as a guest, and then verify that Internet Explorer is launched as the shell.

CONFIGURE UNIFIED WRITE FILTER TO PROTECT YOUR DISK DRIVES FROM UNWANTED CHANGES

You can use Unified Write Filter (UWF) to protect your storage media, such as disk drives, from unwanted writes and changes. You can also add file and registry exclusions to allow specific files and registry entries to be updated

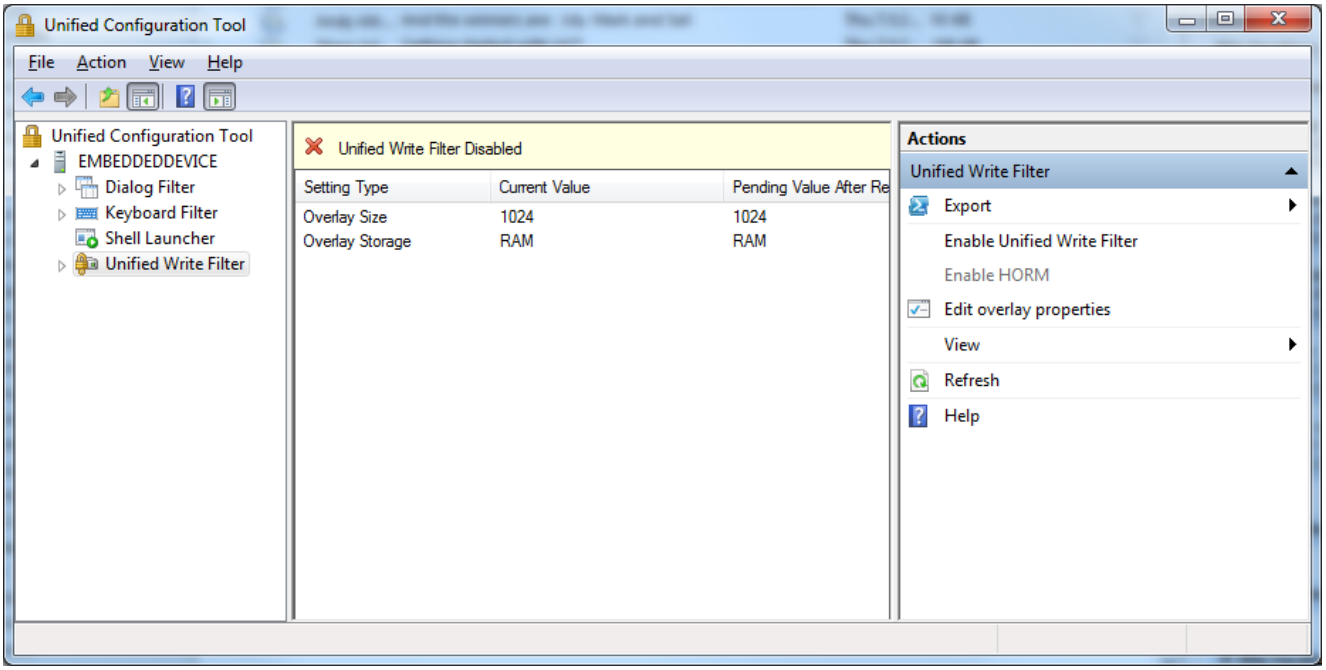
There are some files and folders that cannot be excluded. For more information, press F1 to open the help topic which contains the list of files and folders that cannot be excluded.
In the following example, you create three example text files on your device in order to demonstrate how to protect your disk while allowing specific files to be changed on the disk.

To enable UWF protection on the C: drive and allow changes to specific files to persist across device restarts

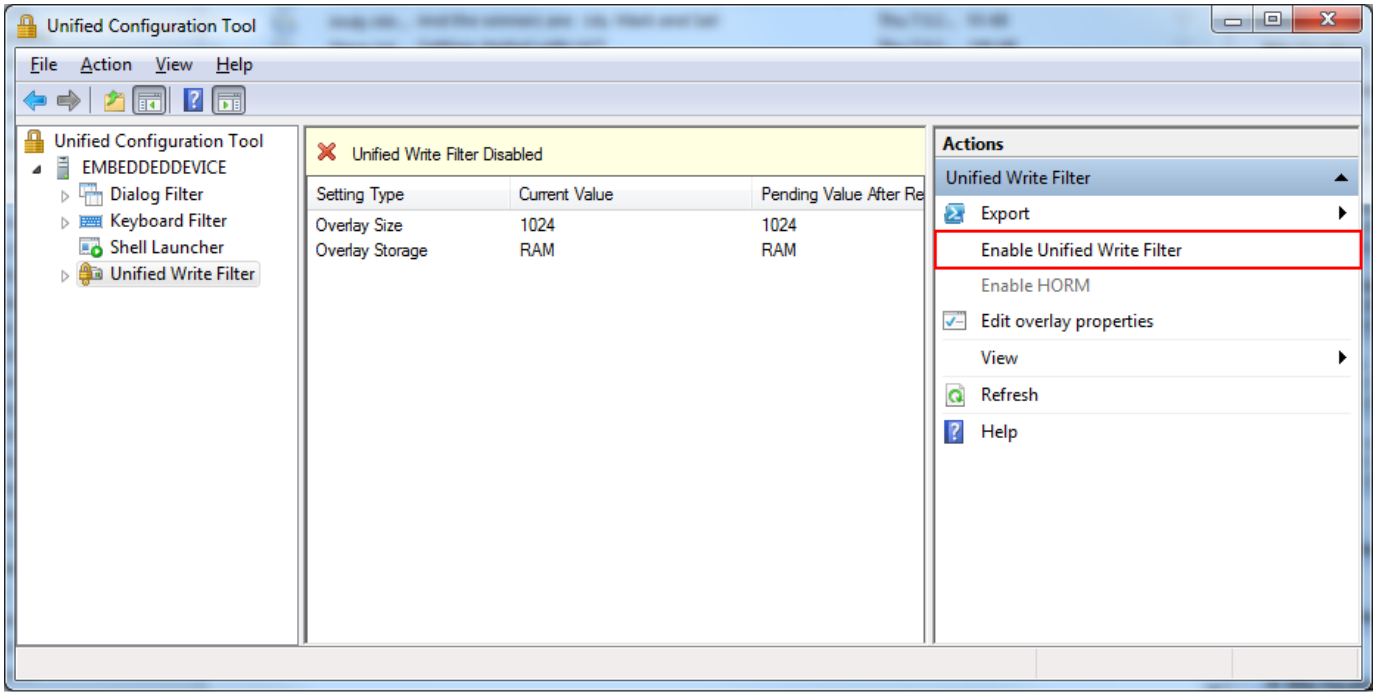
Important:

In this procedure, you use Notepad to modify files. Make sure that Dialog Filter has the default setting set to **Show**, and that no dialogs for notepad.exe are blocked. For more information, see CONFIGURE DIALOG FILTER and ONLY SHOW DIALOG BOXES FROM SELECT PROCESSES in this document.

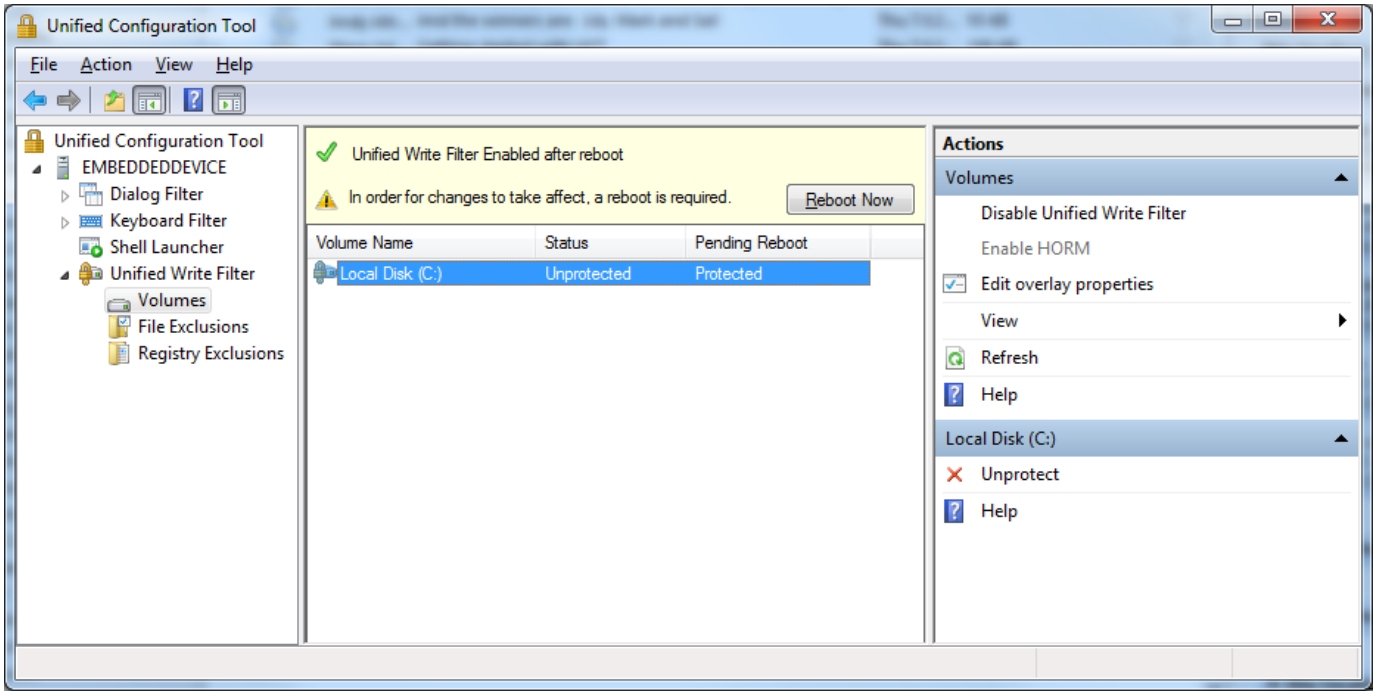
1. In UCT, navigate to **Unified Write Filter**.
2. In the center pane, make sure that UWF is disabled. If UWF is not currently disabled, click **Disable Unified Write Filter**, and then restart your device.



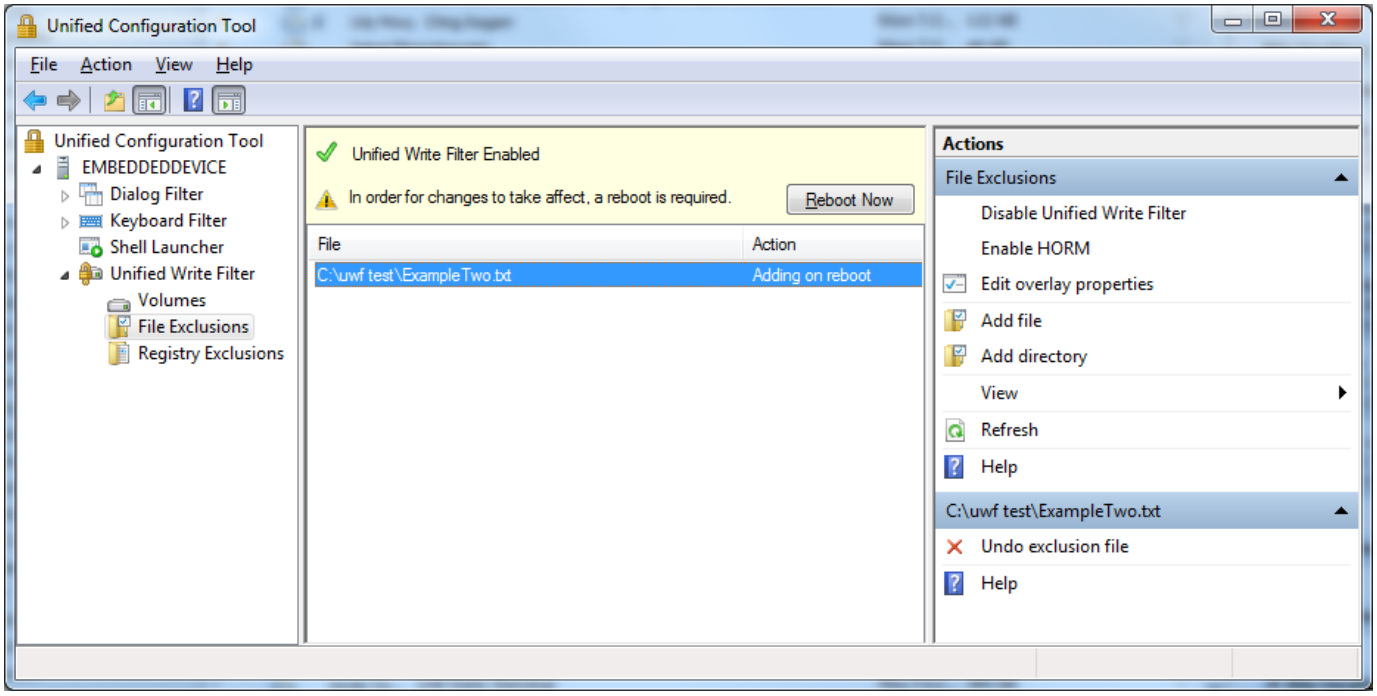
3. On your device, create a new folder **C:\UWF test**.
4. On your device, in the new folder C:\UWF test, create three new empty text files, **ExampleOne.txt**, **ExampleTwo.txt**, and **ExampleThree.txt**.
5. In UCT, in the **Actions** pane, click **Enable Unified Write Filter**.
   Do not restart your device yet.



6. In the left pane, navigate to **Volumes**.
7. In the center pane, right-click **Local Disk (C:)** and then click **Protect**.



8. In the center pane, click **Reboot Now** to restart your device.
   Wait for your device to restart, and for UCT to reload the configuration information.
9. In UCT, navigate to **File Exclusions**.
10. In the **Actions** pane, click **Add file**.
11. In the **Add file** dialog box, browse to C:\UWF test, select **ExampleTwo.txt**, and then click **OK**.



12. Click **Reboot Now** to restart your device.
13. On your device, open a new command prompt as an Administrator.
14. At the command prompt, type **cd "c:\UWF test"**
15. Type **dir** to see the three text files you created earlier.
16. Type **Erase ExampleOne.txt**
17. Type **dir** to verify that ExampleOne.txt no longer appears in the directory.
18. Type **notepad ExampleTwo.txt** to open the second example file in notepad.
19. In **Notepad**, enter some text, such as "This change should persist", save the file and close **Notepad**.
20. At the command prompt, type **notepad ExampleThree.txt**.
21. In **Notepad**, enter some text, such as "This change should not persist", save the file and close **Notepad**.
22. In **Notepad**, reopen **ExampleTwo.txt** and **ExampleThree.txt** to verify that the changes have been saved.
23. Restart your device.
24. In Notepad, open ExampleOne.txt, ExampleTwo.txt, and ExampleThree.txt again. Verify the following:
    - ExampleOne.txt is not deleted.
    - ExampleTwo.txt contains your text.
    - ExampleThree.txt does not contain any text.