How to Implement Windows 7 with Embedded Restrictions

Windows 7 for Embedded Systems

Introduction

Take advantage of the full power of Microsoft's premium operating system when footprint size is not an issue. Windows 7 for Embedded Systems features the same security, productivity and reliability features and functionality as Microsoft's powerful desktop operating system. In fact Windows 7 for Embedded systems is binary identical to the desktop version of Windows 7.

This white paper discusses techniques and provides guidance to help OEMs harden and customize their devices running Windows 7 with embedded restrictions.

Disclaimer

- This memo does not interpret any legal restrictions (ALP or CLA). **This is the responsibility of the OEM**.
- Many of the techniques discussed in this white paper are not supported by Microsoft.

During the operation of a device, all indication of the operating system should be suppressed. This end-to-end requirement covers all identifiable operating system display elements, from startup to shut down.

> **Note** Suppressing any other system messages that are not under control of the operating system but may reveal information about the device (such as the BIOS startup screen) is out of scope for this guidance.

Many of these settings could be deployed using Group Policy, although some of them would require a custom Group Policy Administrative Template ADM file to be created. Detailed information about how to create new ADM templates is provided in the article Using Administrative Template Files with Registry–Based Group Policy located at http://technet.microsoft.com/en-us/library/bb742499.aspx.

The download of the tools and templates required can be found here:

http://www.microsoft.com/downloads/details.aspx?familyid=e7d72fa1-62fe-4358-8360-8774ea8db847&displaylang=en

Note These settings are generally included as part of the base security builds for device applications provided by the vendor. For example, some settings that hide the operating system can be completed through the user profile that the autologon account uses. The profile provided for the device application frequently provides all these settings. We recommend copying this profile to the default user profile so that the settings from this profile will apply to all new user accounts and will therefore be applied to the domain autologon account.

To use the policy editor follow this simple procedure:

- Go to the start menu and type **"MMC"** in the search bar and hit enter
- Once you confirmed the UAC prompt to run the MMC, select **"File"** then **"Add or Remove Snap-ins"**
- In the upcoming dialog select **"Group Policy Object Editor"**
- This will prompt another dialog to select the **"Group Policy Object".** Check the box **"Allow the focus of the Group…".** This will allow us to save the MMS with the Snap-in for later use in this document.
- Close the Snap-ins dialog with OK.
- Now save this console with **"File/Save"** as the **"GPEdit.msc"**

Removal of Branding and Pop-Up Windows

Hide Windows Vista Startup Splash Logo

The GUI boot can be disabled by:

- Press **Start** and then **Run**.
- Type **Msconfig** then press enter.
- Click the **boot** tab.
- Check the **No Gui Boot** check box.
- Check the **Make all boot settings permanent** check box.
- Press OK or Apply.

Change Colors of Logon Screens

The logon screen background should be set to black by adding a value of **0 0 0** to the following registry values:

- **HKEY_USERS\.DEFAULT\Control Panel\Colors\Background**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Background**

Force Windows to Use an Alternative Shell

Ideally, the standard Windows Explorer shell would not be required for the autologon user at the device. Instead, the device application would run as the shell. This approach removes the need for many of the lockdown settings in Windows Explorer (for example, removal of the taskbar and removal of desktop and Start menu items) that are required if you start the device application from the Windows Explorer shell. The drawback is that if you do not run the Windows Explorer shell, the ability to start applications using the startup folder, the run key, or other functions of the Windows Explorer shell are lost, so the replacement shell must be able to launch all required executables to allow the device to function.

> **Note** For some device applications, the Windows shell is required to start the device application.

To replace the Windows shell, use the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

> **Note** For remote devices that use the Windows autodial function (the *rasauto* service), running Windows 7 with an alternative shell may create a situation where the autodialer fails to start a dial-up connection when it is required. This is because rasauto expects the entry in the *Winlogon\Shell* key to be a simple executable name, and not an executable with a full path associated. To work around this, make sure that the replacement shell application is in the autologon user's path and set the *Winlogon\Shell* value to just the simple name of the executable.

Hide Windows Fatal Error Messages

When a STOP message (a fatal system error message) displays in Windows Vista, the computer enters debug mode for troubleshooting. The error message appears on a Stop error, and the first few lines resemble the following sample error message:

Stop 0x0000001e (c000009a 80123f36 02000000 00000246)

Unhandled Kernel exception c000009a from 8123f26

Address has base at 80100000 ntoskrnl.exe

If such an event occurs, the computer can be configured to restart automatically through the Startup and Recovery options as shown in the following figure. This approach would effectively prevent the device from remaining on the Stop error (and the cryptic information it displays) until physical intervention is arranged.

The System Crash-Control setting can be configured through the following registry change:

- **System Key**: [**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl**]
- **Value Name**: AutoReboot
- **Data Type**: REG_DWORD (DWORD Value)
- **Value Data**: (0 = disabled, 1 = auto reboot)

Additionally you can clear the flag “CrashDumpEnabled” in order to prevent the device from creating a crash dump file using:

- **Value Name**: CrashDumpEnabled
- **Data Type**: REG_DWORD (DWORD Value)
- **Value Data**: (0 = disabled, 1 = enabled)

By configuring AutoReboot, it is possible that a hardware problem that surfaces early in the boot cycle of Windows may get the device into a cycle of continuous restarts. However, this situation would probably be no worse than having the computer stopped permanently with a Stop error until manual intervention occurs. It has the added advantage of being able to recover automatically from isolated occasional failures.

> **Note** Device applications usually include a feature that will prevent the device from continuously restarting.

Suppress Pop-up Messages

Suppressing pop-up messages is a key concern for a device. The following recommendations can help suppress pop-up windows:

Disable the Windows error reporting service on the device

- Disable Windows Error Reporting windows
  - Suppress pop-up error messages using **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows\ ErrorMode=2**
- Disable startup error messages using
  - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\**Windows\NoPopUpsOnBoot=1
  - (you have to add the value name NoPopUpsOnBoot as a dword).

Windows Diagnostics Resolvers: These show when Windows detects a hardware or software problem that requires the user to intervene. They can be suppressed by changing the Group policy as follows:

- Start the Policy Editor by typing “**Gpedit”** in the start searchbar
- Navigate to **Local Computer Policy->Computer Configuration->Administrative Templates->System->Troubleshooting and Diagnostics->Diagnostics: Configure scenario execution level**
- Enable the policy, set Scenario execution level to **Detection and Troubleshooting Only**.

Operating System Footprint Reduction

All nonessential applications and services not required on the device should not have their related application files that are included in the image. This approach is consistent with wanting to have the smallest surface area for attack on a device.

Individual operating system files should not be removed from the device image. Removal of such files would result in a build of Windows XP that would be unsupported by Microsoft.

> **Note** Any Windows component that can be removed through Add and Remove Windows Components item in Control Panel is acceptable to exclude from the device build. Other mechanisms for removing Windows components would be unsupported.

Command Prompt

By default, the copyright notices already appear when you open a command prompt. However you can add some custom information at the prompt (do not replace the copyright notice).

Open your registry and find the key below:

Registry Settings
System Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment] Value Name: PROMPT Data Type: REG_EXPAND_SZ (Expanded String Value) Value Data: Prompt Text (for example, PG)

Create or modify a REG_EXPAND_SZ string called "PROMPT" and set it to the required prompt format including any special codes or variables below.

Special Codes

- $A - & (Ampersand)
- $B - | (pipe)
- $C - ((Left parenthesis)
- $D - Current date
- $E - Escape code (ASCII code 27)
- $F -) (Right parenthesis)
- $G - > (greater-than sign)

- $H - Backspace (erases previous character)
- $L - < (less-than sign)
- $N - Current drive
- $P - Current drive and path
- $Q - = (equal sign)
- $S - (space)
- $T - Current time
- $V - Windows XP version number
- $_ - Carriage return and linefeed
- $$ - $ (dollar sign)

Variables

- %USERNAME% - Current Username
- %COMPUTERNAME% - Local computer name
- %USERDOMAIN% - Local domain name

The default prompt is "$P$G" (for example, "C :\>"), some alternatives include the following:

- [%ComputerName%] $S$P$G to show the computer, drive and path
- [%username%] $S$P$G to show the current user, drive and path

Restart or log-off Windows for the change to take effect.

Set AutoLogon to a Specific Account

To set **AutoLogon** to a specific account:

- Click **Start** and type **netplwiz**
- In the window that opens, clear the **Users must enter a username and password to use this computer** box.
- Click **Apply**
- A new dialog box will appear. Enter the user and password that you want to use to autologon.

- Click **OK**

Disable Access to Task Manager

To disable access to **Task Manager**:

1. Click **Start** and type gpedit.msc

2. In the **Group Policy** settings window:

   - Select **User Configuration**
   - Select **Administrative Templates**
   - Select **System**
   - Select **Ctrl+Alt+Delete options**
   - Select **Remove Task Manager**
   - Double-click the **Remove Task Manager** option, and then choose **Enable**
   - Do the same for **Remove Logoff**, **Remove Lock Computer**, and **Remove Change Password**.

You will find a couple further settings in this section that you might want to enable or disable, depending on the scenario of your embedded devices.

Using Virtual Windows XP Mode application as the shell

In order to use legacy application in Virtual Windows XP mode running on Windows 7 for Embedded Systems, OEMs have to comply with the licensing restrictions and make the legacy application the shell of the device.

This procedure explains how to do this:

First the Virtual XP Mode update files have to be downloaded an installed from http://www.microsoft.com/windows/virtual-pc/

Once installed you will find the “Windows XP Mode” in the “Windows Virtual PC” folder in the Start Menu.

Launch the “Windows XP Mode” link in the start menu

You will be asked a couple configuration questions. Once the Setup is done, Windows 7 and Windows Virtual PC will configure the “Windows XP Mode” and launch it.

Once the Windows XP Mode is showing, install your application inside the Virtual Machine.

In order to see the application in your Windows 7 host environment as a shortcut follow these steps:

- open the directory “C:\Documents and Settings\All Users\Start Menu\Programs” in the Windows Explorer
- Create a shortcut to your application in this folder
- Now shut down the virtual machine running Windows XP Mode

One the Virtual Machine was shut down, you will see in the start menu of Windows 7 in the directory “Window Virtual PC\Windows XP Mode Application” the shortcut to your application

If you select this shortcut, the Virtual PC will launch the Windows XP Mode and automatically start the application behind the shortcut without showing the Windows XP Desktop.

The last step you have to do to comply with the “Hide the shell” licensing restriction of Windows 7 for Embedded Systems is to make this application the “Shell” of your device.

- Navigate to the shortcut in the Start Menu of Windows 7 and right click the shortcut.
- Write down the link in the shortcut (starting with %SystemRoot%\system32\rundll32.exe %SystemRoot%\system32\VMCPropertyHandler.dll,LaunchVMSal "Windows XP Mode" …)
- Change the link to the shell in the registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

To further lock down your device, follow the procedures above in this whitepaper

> **Note** Windows XP mode requires VT extensions enabled for your motherboard and a CPU that supports these extensions. By default, Windows XP Mode does use 512MB of RAM, please refer to the XP Mode documentation if you need to change this or other defaults.

Summary

With a few easy steps you can comply with the rules of the Windows 7 for Embedded Systems license restriction.