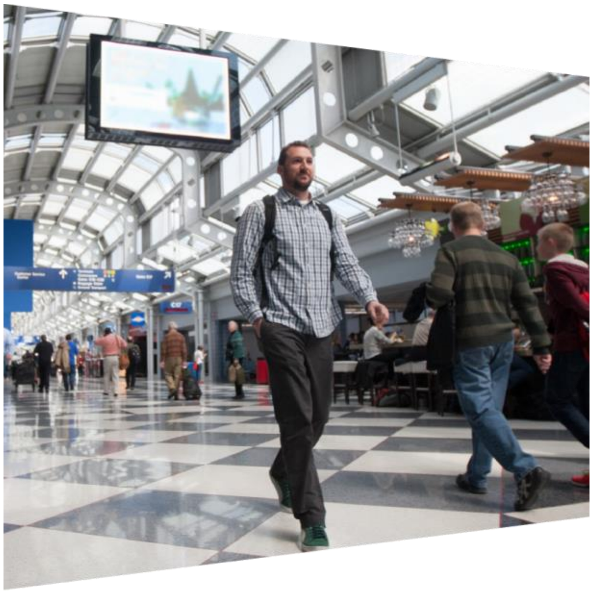


Windows

Version 1.0
Positioning White Paper

Guidelines for Designing Embedded Systems with Windows 10 IoT Enterprise

Contents

This white paper is not intended to provide any legal advice, or grant any legal rights or revise the terms of any Original Equipment Manufacturer (OEM) agreement. Compliance with the OEM agreement terms is the responsibility of the OEM.

Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Additionally, the techniques outlined in this paper are suggestions only and may or may not be fully supported by Microsoft.

Overview

Windows 10 IoT Enterprise for Embedded Systems gives you the full power of the Windows 10 Enterprise operating system for your embedded device, featuring the same security, productivity, reliability, and functionality as the binary-identical desktop version of Windows.

This white paper provides guidelines and suggestions for ways to satisfy certain requirements stated in the OEM agreement.

Building a task-specific experience

This paper will focus on the techniques for creating a task-specific or industry-specific experience for users of your device. If you are planning to deploy applications using the Win32 application programming interface on your device, the techniques you have used in the past are still supported and available for your use.

If you are planning to invest in building a Universal Windows Application (UWA), you can find useful development information at http://msdn.microsoft.com/en-us/windows/apps/

This paper will only address topics related to creating a task-specific experience. Other topics related to Windows 10 such as provisioning, deployment, and development, will be addressed in other papers.

There are a number of techniques you can use to help ensure the task-specific nature of your device. The scenarios to be reviewed in this paper include:

- Application control
- Customize the desktop
- Logon experience
- System control

Useful Links

Here are a couple of useful links for information:

Learn to build Universal Windows Apps

http://go.microsoft.com/fwlink/?LinkID=616850

Windows hardware development

http://go.microsoft.com/fwlink/?LinkID=616851

Getting started with Universal Windows Drivers

http://go.microsoft.com/fwlink/?LinkID=616852

How to setup a device for anyone to use

https://technet.microsoft.com/en-us/library/mt219050(v=vs.

General Group Policy settings

All settings outlined in this document are managed through the Local Group Policy Editor or the Registry Editor unless otherwise specified. In the tables below, the Policy Type will be either Computer Configuration or User Configuration. The Location defines the node where the specific policy can be found. For more information on implementing registry-based group policy for applications, please see the following article: http://go.microsoft.com/fwlink/?LinkID=616853

Policy Type	Location	Feature	Description
Computer Configuration	Administrative Templates\ System\Group Policy	Configure User Group Policy loopback processing mode	Setting to maintain computer's policy configuration no matter who logs on.

Application control

Embedded systems need to automatically run applications, prevent others from running and generally control what happens when they stop running for one reason or another. First let's look at the primarily two types of applications that can run on Windows 10 IoT Enterprise.

1. A Universal Windows app is a Windows experience that is built upon the Universal Windows Platform (UWP), which was first introduced in Windows 8 as the Windows Runtime. Universal Windows apps are most often distributed via the Windows Store (but can also be side-loaded), and are most often packaged and distributed using the .APPX packaging format.
2. A Classic Windows application is a Windows experience run that uses the Classic Windows Platform (e.g., .NET, COM, Win32, etc.) and is typically launched using an .EXE or .DLL file.

Application boot options

Depending on which application you have deployed there are several application boot options to help create a single purpose device experience.

Auto-boot Universal Windows apps

For Universal Windows apps use the Application Launcher to start an app automatically after a user signs in to a Windows 10 IoT Enterprise device and to restart the app when the app exits. You can configure the Application Launcher to launch different apps for different users. If the app is written specifically to work with the Application Launcher, you can configure the Application Launcher to perform a specified action based on an exit value returned by the app. For example, you could configure the Application Launcher to shut down or restart the device when the app exits.

Learn more at: http://go.microsoft.com/fwlink/?LinkID=616854

Auto-boot Classic Windows apps

For Classic Windows applications the Shell Launcher can be used to replace the Windows shell with a custom shell. You can use any executable as your customer shell to be a dedicated embedded application.

Use the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell**

Note: Unless you want the logon screen to appear prior to booting into your custom executable you will need to follow the instructions for setting an auto-logon experience or customizing the logon experience. Additionally, moving into an alternative shell directly will not allow you to access any of the Windows navigational elements on boot-up. This will take you directly to your predefined application and will not allow you to access the soft keyboard, charms bar, backlist, or applications bar. Additionally, if you want to launch into a modern application, you will need to do so programmatically and you cannot use the registry key above to do so. In order for a modern application to launch it needs to have the support of explorer.exe (modern shell). Modern applications will not run without explorer.exe initiated first. Scripts can be created that can chain the launch of Windows Explorer and the selected application and run on first boot.

Learn more at: http://go.microsoft.com/fwlink/?LinkID=616855

Additionally you can automatically run Classic Windows applications using the default desktop during the first boot of the image or after every logon. This is done by editing the following registry keys:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

It's also possible to make a Classic Window app run on logon by putting a shortcut for the app in **<C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup>**

Limit application access with AppLocker

Limiting the applications that the users can run is a common function in customizing a device. To accomplish this, use AppLocker. AppLocker is a simple and flexible mechanism that allows administrators to specify exactly what is allowed to run in their desktop environment. As a result, AppLocker provides operational and compliance benefits by allowing administrators to prevent unlicensed software from running in the desktop environment if the software is not on the allowed list, or to prevent vulnerable, unauthorized applications from running in the desktop environment, including malware.

Learn more at: http://go.microsoft.com/fwlink/?LinkID=616856

Note: These settings only disallow running the programs; they do not remove them from view.

Limit application visibility

Limiting the applications that the user can see is a common function in customizing a device. To accomplish this, use the following group policies:

Policy Type	Location	Feature	Description
User Configuration	Administrative Templates\ Control Panel	Remove common program groups from Start menu	Disables all Control Panel programs and the PC settings app.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Prevent users from uninstalling applications from Start	If you enable this setting, users cannot uninstall apps from Start or Apps bar.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not allow pinning programs to the Taskbar	This policy setting allows you to control pinning programs to the Taskbar.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove pinned programs list from the Start menu	If you enable this setting, the "Pinned Programs" list is removed from the Start menu. Users cannot pin programs to the Start menu.
User Configuration	Administrative Templates\ Windows Components\ App Runtime	Block launching desktop apps associated with a protocol	This policy setting allows you to minimize the risk involved when a packaged app launches the default app for a protocol.

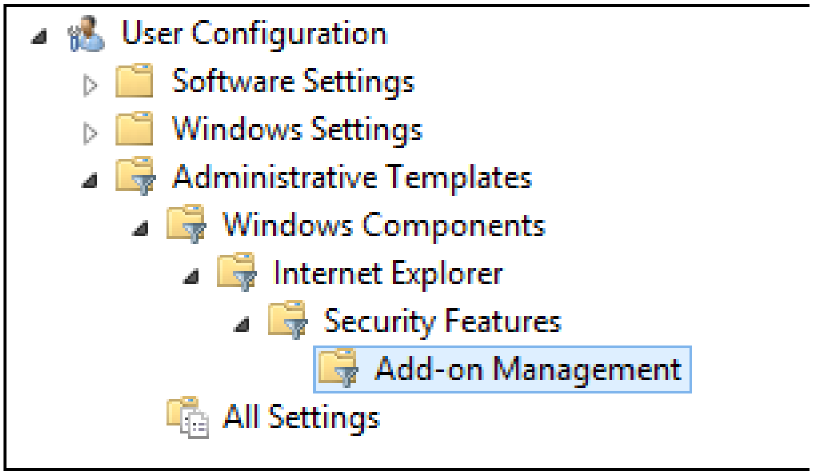
You can also limit the apps that run on the machine using AppLocker.

Disable Adobe Flash Player

In Internet Explorer

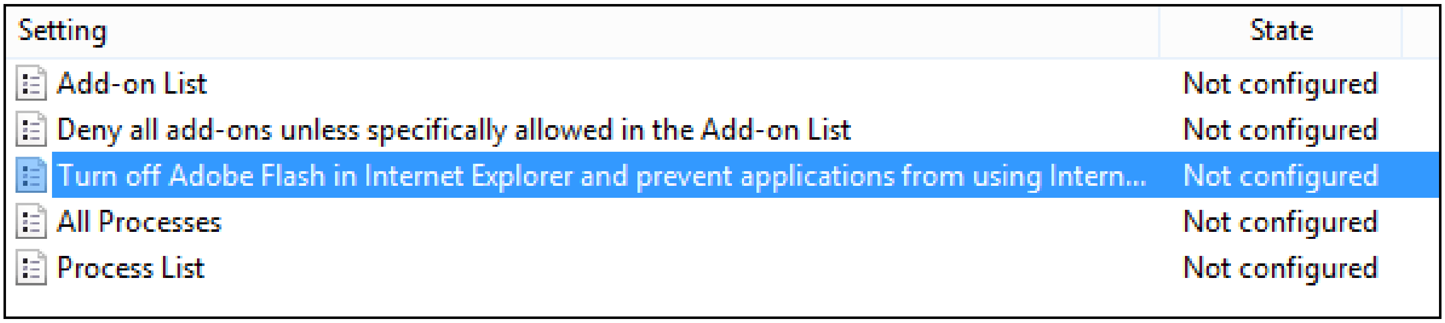
1. Go to the Windows Run command (Win+R) and type gpedit.msc to launch the Local Group Policy Editor

2. Select User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Add-on Management



- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Windows Components
      - Internet Explorer
        - Security Features
          - Add-on Management
    - All Settings

3. In the settings turn off Adobe Flash in Internet Explorer



Setting	State
Add-on List	Not configured
Deny all add-ons unless specifically allowed in the Add-on List	Not configured
Turn off Adobe Flash in Internet Explorer and prevent applications from using Intern...	Not configured
All Processes	Not configured
Process List	Not configured

Customize the desktop

It may be necessary to limit access to the desktop and customize the Start Menu and Taskbar as part of the overall device experience. There are numerous policy settings that can be applied to help customize the desktop. Below are some of the key policy for customizing the desktop experience for and embedded device.

Customize the Start Menu and Taskbar

You can limit access to the desktop with granular control over the Start Menu and Taskbar using the following policies. This may be necessary for devices that need to provide the end user with a number of applications with the familiar desktop experience, but without access to make changes. :

Policy Type	Location	Feature	Description
User Configuration	Administrative Templates\ Start Menu and Taskbar	Clear history of recently opened documents on exit	The system deletes shortcuts to recently used document files when the user logs off
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not allow pinning items in Jump Lists	Prevent users from pinning files, folders, websites, or other items to their jump lists in the Start Menu or Taskbar
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not display or track items in Jump Lists from remote locations	If enabled, files that the user opens over the network from remote computers are not tracked or shown in the jump list
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not keep history of recently opened documents	If enabled, the system empties the recent items menu on the Start Menu.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Prevent changes to Taskbar and Start Menu Settings	if enabled, the user will be prevented from opening the Taskbar properties dialog box
User Configuration	Administrative Templates\ Start Menu and Taskbar	Prevent users from customizing their Start Screen	Prevent users from selecting an app, resizing a tile, pinning/unpinning a tile or second tile, entering the customize mode and rearranging tiles within Start and Apps
User Configuration	Administrative Templates\ Start Menu and Taskbar	Prevent users from uninstalling applications from Start	Users cannot uninstall apps from Start
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove All Programs list from the Start menu	The "All Programs" item is removed from the simple Start Menu.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	The Power button and the Shut Down, Restart, Sleep and Hibernate commands are removed from the Start menu
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove common program groups from Start Menu	Only items in the users profile appear in the Programs menu
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove frequent programs list from the Start Menu	The frequently used programs list is removed from the Start Menu
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove Logoff on the Start Menu	The Log Off <username> does not appear in the Star Menu
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove pinned programs list from the Start Menu	"Pinned Programs" list is removed from the Start Menu
User Configuration	Administrative Templates\ Start Menu and Taskbar	Show "Run as different user" command on Start	If you disable this setting or do not configure it, users cannot access the "Run as different user" command from Start or any application.

Policy Type	Location	Feature	Description
User Configuration	Administrative Templates\ Start Menu and Taskbar	Prevent users from uninstalling applications from Start	If you enable this setting, users cannot uninstall apps from Start or Apps bar.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not allow pinning programs to the Taskbar	This policy setting allows you to control pinning programs to the Taskbar.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Remove pinned programs list from the Start menu	If you enable this setting, the "Pinned Programs" list is removed from the Start menu. Users cannot pin programs to the Start menu.

Note: Remove all tiles that you do not want your user to access; but if you are testing the behavior of Group Policy you many want to add CMD Shell to your start screen so that you can get to the necessary tools required for reconfiguring your settings.

To start, configure the Start Menu with the desired applications. Begin by installing all of the applications that are needed on the system. Then remove and lock down the applications that are not part of the final view required.

The remainder of these policies prevents the Classic Windows Platform from being exposed via messaging or features such as power management or file associations.

Policy Type	Location	Feature	Description
Computer Configuration	Administrative Templates\ Windows Components\ Windows Explorer	Configure Windows SmartScreen	This policy setting allows you to manage the behavior of Windows SmartScreen to help keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.
Computer Configuration	Administrative Templates\ Windows Components\ Windows Explorer	Show lock in the User Tile menu	Shows or hides lock from the User Title menu. If you enable this policy setting, the lock options will be shown in the User Tile menu.
Computer Configuration	Administrative Templates\ Windows Components\ Windows Explorer	Show sleep in the Power Options menu	Shows or hides sleep from the Power Options menu. If you enable this policy setting, the sleep option will be shown in the Power Options menu (as long as it is supported by the machine's hardware). If you disable this policy setting, the sleep option will never be shown in the Power Options menu.
Computer Configuration	Administrative Templates\ Windows Components\ Windows Explorer	Set a default associations configuration file	This policy specifies the path to a file (for example, either stored locally or on a network location) that contains file type and protocol default application associations. This file can be created using the DISM tool.

Custom layout

You can create custom layout using the PowerShell cmdlet Export-StartLayout then use the following policy to apply the layout to all users. Once enabled users will not be able to customize their start screen.

Policy Type	Location	Feature	Description
Computer Configuration Or User Configuration	Administrative Templates\Start Menu and Taskbar	Start Layout	This policy lets you specify the Start layout for users and prevents them from changing its configuration.

Disable recent items

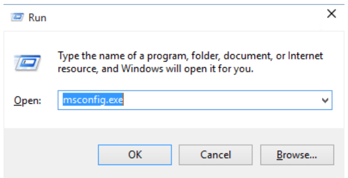
Disabling recent items can allow an enterprise more control over the device.

Policy Type	Location	Feature	Description
User Configuration	Administrative Templates\Windows Components\Edge UI	Turn off tracking of app usage	This policy setting prevents Windows from keeping track of the apps that are used and searched most frequently. If you enable this policy setting, apps will be sorted alphabetically in: - Search results - The Search and Share panes - The drop-down app list in the Picker Disabling or not enabling will allow Windows to keep track of the apps that are used and searched.

Disable access to Task Manager

To disable access to Task Manager and Control Panel:

- From the desktop, open the Run dialog box using the Windows logo + R keyboard shortcut.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: msconfig.exe

- In the “Run” dialog box, type **gpedit.msc** and then press **Enter**.

- In the Group Policy Editor window that opens, select **User Configuration\Administrative Templates\System\Ctrl+Alt+Del Options**.

- Select **Remove Task Manager**.
- Double-click or tap the **Remove Task Manager** option, then choose **Enable**.
- Repeat these actions for **Remove Logoff, Remove Lock Computer**, and **Remove Change Password**.

Note: To completely remove the Change Password option you will need to disable access to Control Panel. This can be done by setting the applicable Group Policy found in the following table:

Limit access to the search box / Cortana

You can limit access to the search box on the Taskbar by applying the following policy settings limiting it into a basic device side search only:

Policy Type	Location	Feature	Description
Computer Configuration	Administrative Templates\ Windows Components\ Search	Don’t search the web or display web results in Search	Queries won’t be performed on the web and web results won’t be displayed
Computer Configuration	Administrative Templates\ Windows Components\ Search	Set the SafeSearch setting for Search	Prevent uses from specifying the SafeSearch setting
User Configuration	Administrative Templates\ Windows Components\ File Explorer	Turn off display of recent search entries in the File Explorer search box	File explorer will not show suggestion pop-ups as users type into the search box
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not search programs and Control Panel items	if enabled, the Start Menu search box will not search for programs or Control Panel items
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not search for files	A "See more results" / "Search Everywhere" link will not be shown when the user performs a search in the start menu search box
User Configuration	Administrative Templates\ Start Menu and Taskbar	Do not search communication	if enabled, the Start Menu search box will not search communications

Policy Type	Location	Feature	Description
User Configuration	Administrative Templates\ Control Panel	Prohibit access to Control Panel and PC Settings	Disables all Control Panel programs and the PC settings app.
User Configuration	Administrative Templates\ System\Ctrl+Alt+Delete	Remove Task Manager	This policy setting prevents users from starting Task Manager.
User Configuration	Administrative Templates\ System\Ctrl+Alt+Delete	Remove Logoff	This policy setting disables or removes all menu items and buttons that log the user off the system.
User Configuration	Administrative Templates\ System\Ctrl+Alt+Delete	Remove Change Password	This policy setting prevents users from changing their Windows password on demand.
User Configuration	Administrative Templates\ System\Ctrl+Alt+Delete	Remove Lock Computer	This policy setting prevents users from locking the system.

Customize Windows start screen and available start-up functions

The start, lock, and account picture screens have limited customization ability.

START—You can change the start screen to present a solid background and choose from the color preference bar to set the background color. If you want a color that is not present in the color preference bar you will need to use sysprep.exe to configure the custom color.

LOCK—The lock screen can have an image selected for display through the personalization settings on the device. Any image can be displayed and will be optimized by Windows. Additionally, on the lock screen you can predetermine which apps you want to run in the background, show status, and display notifications. If you don't want to show this functionality then just remove the apps from this area.

ACCOUNT PICTURE—This is also referred to as the "user tile." It can be set in the personalization settings as well. This image will display on the logon screen when providing an upward swipe gesture on the lock screen. It also displays in the upper-right corner of the modern desktop.

Policy Type	Location	Feature	Description
Computer Configuration	Administrative Templates\ Control Panel\ Personalization	Prevent changing lock screen image	Prevents users from changing the background image shown when the machine is locked.
Computer Configuration	Administrative Templates\ Control Panel\ Personalization	Prevent changing Start menu background	Prevents users from changing the look of their Start menu background, such as its color or accent.
Computer Configuration	Administrative Templates\ Control Panel\ Personalization	Do not display the lock screen	This policy setting controls whether the lock screen appears for users.
Computer Configuration	Administrative Templates\ Windows Components\ Desktop Window Manager	Use solid color for Start background	This policy setting controls the Start background visuals. If you enable this policy setting, the Start background will use a solid color.

Policy Type	Location	Feature	Description
Computer Configuration	Administrative Templates\ Windows Components\ Portable Operating System	Windows To Go default startup options	This policy setting controls whether the PC will boot to Windows To Go if a USB device containing a Windows To Go workspace is connected, and controls whether users can make changes using the Windows To Go startup options Control Panel item.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Clear history of tile notifications on exit	If you enable this setting, the system deletes tile notifications when the user logs off. As a result, the tiles in the start view will always show their default content when the user logs on. In addition, any cached versions of these notifications will be cleared when the user logs off.
User Configuration	Administrative Templates\ Start Menu and Taskbar	Prevent users from uninstalling applications from Start	If you enable this setting, users cannot uninstall apps from Start.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Do not allow taskbars on more than one display	This policy setting allows you to prevent taskbars from being displayed on more than one monitor.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Do not search for files	If you enable this policy setting, the Start menu search box will not search for files.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Do not search programs and Control Panel items	If you enable this policy setting, the Start menu search box will not search for programs or Control Panel items.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Remove common program groups from Start menu	Removes items in the All Users profile from the Programs menu on the Start menu.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Remove Search link from Start menu	Removes the Search link from the Start menu, and disables some Windows Explorer search elements. Note that this does not remove the search box from the new style Start menu.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Prevent changes to Taskbar and Start menu settings	Removes the Taskbar and Start menu item from Settings on the Start menu. This setting also prevents the user from opening the Taskbar Properties dialog box.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Remove the networking icon	This policy setting allows you to remove the networking icon from the system control area.

Policy Type	Location	Feature	Description
User Configuration	Administrative Templates\ Start Menu and Task Bar	Remove the battery meter	This policy setting allows you to remove the battery meter from the system control area.
User Configuration	Administrative Templates\ Start Menu and Task Bar	Remove the volume control icon	This policy setting allows you to remove the volume control icon from the system control area.

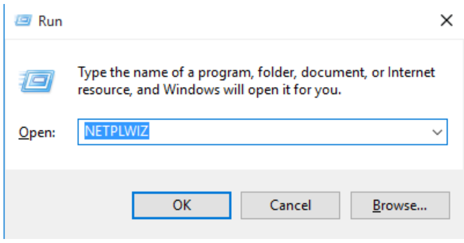
Logon experience

Set auto-logon to a specific account

In some enterprises there may be a desire to have devices auto-logon to a specific account, removing the need for a user to perform a logon action. This might be the case such as when the device is in use as a digital sign or a kiosk where, if there is a power outage, the device can reboot cleanly and directly into the experience desired.

To set auto-logon to a specific account:

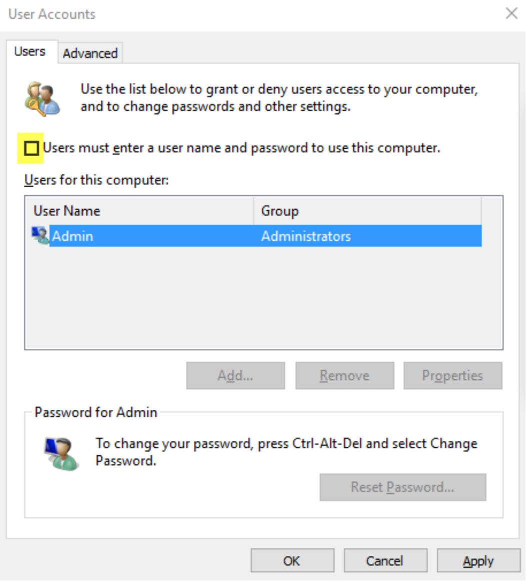
- From the desktop, open the Run dialog box using the Windows logo + R keyboard shortcut.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: NETPLWIZ

- In the “Run” dialog box, type NETPLWIZ**.exe** and then press **Enter**.
- In the dialog box that opens, clear the “Users must enter a username and password to use this computer” check box.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

□ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
Admin	Administrators

Password for Admin

To change your password, press Ctrl-Alt-Del and select Change Password.

- Click or tap **Apply**.

- A new dialog box will open. Enter the username and password that you want to use to log on automatically.
- Click **OK**.

Customize the logon experience

When devices are in use by a specific enterprise they may have guidelines for how they would like the logon experience to be presented. They may not want to allow the usage of a pin or picture as a credential. They may not want to allow app notifications on the logon screen. Choices like these allow the device experience to be better locked down for the individual IT department to manage. Below are some settings that might be used to customize a logon experience.

Policy Type	**Location**	**Feature**	**Description**
Computer Configuration	Administrative Templates\ System\Logon	Turn on PIN sign-in	This policy setting allows you to control whether a domain user can sign in using a PIN.
Computer Configuration	Administrative Templates\ System\Logon	Turn off app notifications on the lock screen	This policy setting allows you to prevent app notifications from appearing on the lock screen.
Computer Configuration	Administrative Templates\ System\Logon	Do not enumerate connected users on domain-joined computers	This policy setting prevents connected users from being enumerated on domain-joined computers.
Computer Configuration	Administrative Templates\ System\Logon	Enumerate local users on domain-joined computers	This policy allows local users to be enumerated on domain-joined computers.
Computer Configuration	Administrative Templates\ Windows Components\ Credential User Interface	Do not display the password reveal button	This policy setting allows you to configure the display of the password entry user experiences.
Computer Configuration	Administrative Templates\ System\User Profiles	Download roaming profiles on primary computers only	This policy setting controls on a per-computer basis whether roaming profiles are downloaded only on a user's primary computers. This policy setting is useful to improve logon performance and to increase security for user data on computers where the user might not want to download private data, such as on a meeting room computer or on a computer in a remote office.
Computer Configuration	Administrative Templates\ System\User Profiles	User management of sharing user name, account picture, and domain information with Windows 8 apps	This setting prevents users from managing the ability to allow apps to access the user name, account picture, and domain information.
Computer Configuration	Administrative Templates\ System\Logon	Always use custom logon background	This policy setting ignores Windows logon background.
Computer Configuration	Administrative Templates\ System\Logon	Do not process the legacy run list	This policy setting ignores the customized run list.

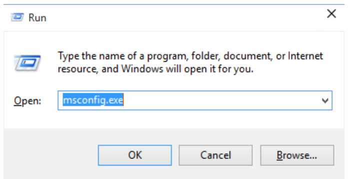
Computer Configuration	Administrative Templates\Control Panel\User Accounts	Apply the default account picture to all users	This policy setting allows an administrator to standardize the account pictures for all users on a system to the default account picture. One application for this policy setting is to standardize the account pictures to a company logo.

System control

Hide the Windows splash logo

The GUI boot can be disabled by:

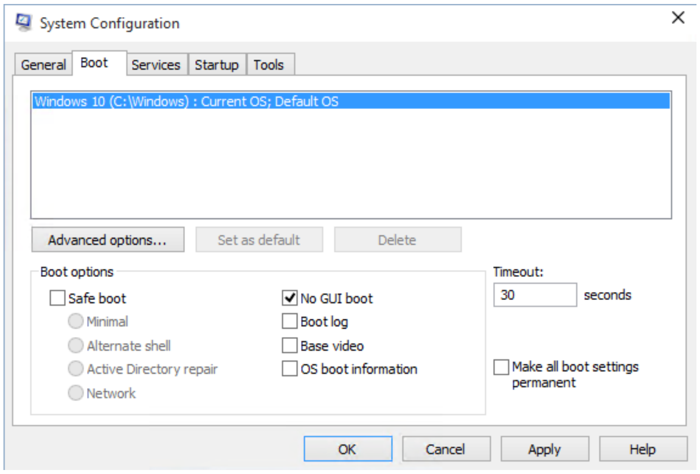
- From the desktop, open the Run dialog box using the Windows logo + R keyboard shortcut.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: msconfig.exe

- In the “Run” dialog box, type **msconfig.exe** and then press **Enter**.
- Click the **Boot** tab.
- Select the **No GUI boot** check box.
- Select the **Make all boot settings permanent** check box.



Windows 10 (C:\Windows) : Current OS; Default OS

Boot options

☐ Safe boot

○ Minimal

○ Alternate shell

○ Active Directory repair

○ Network

☑ No GUI boot

☐ Boot log

☐ Base video

☐ OS boot information

Timeout: 30 seconds

☐ Make all boot settings permanent

- Click **OK** or **Apply**.

Note: This does not remove the Windows trademark screen.

Suppress pop-up messages

Suppressing pop-up messages is a key concern for a device. For instance, if the operating system is being used for a digital sign or kiosk, allowing pop-ups would expose the user to the operating system and possibly the desktop. The following recommendations can help suppress pop-up windows:

Disable the Windows error reporting service on the device.

Disable Windows Error Reporting windows:

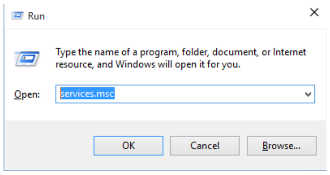
- Suppress pop-up error messaging using HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows\ErrorMode = 2

- Disable startup error messaging using HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\NoPopUpsOnBoot = 1 (You have to add the value name NoPopUpsOnBoot as a DWORD)

Disable Windows Error Reporting

Windows Error Reporting can be disabled to suppress pop-up messages.

- From the desktop, open the Run dialog box using the Windows logo + R keyboard shortcut.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

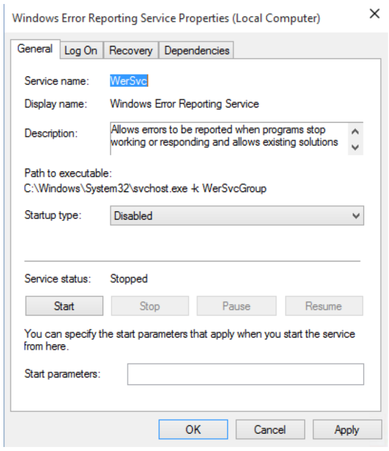
Open: services.msc

- In the “Run” dialog box, type **services.msc** and then press **Enter**.

- Search the list for Windows Error Reporting Services and press Enter.

- Change the Startup type to Disabled.

- Click **OK** or **Apply**.



Windows Error Reporting Service Properties (Local Computer)

Service name: WerSvc

Display name: Windows Error Reporting Service

Description: Allows errors to be reported when programs stop working or responding and allows existing solutions

Path to executable:
C:\Windows\System32\svchost.exe -k WerSvcGroup

Startup type: Disabled

Service status: Stopped

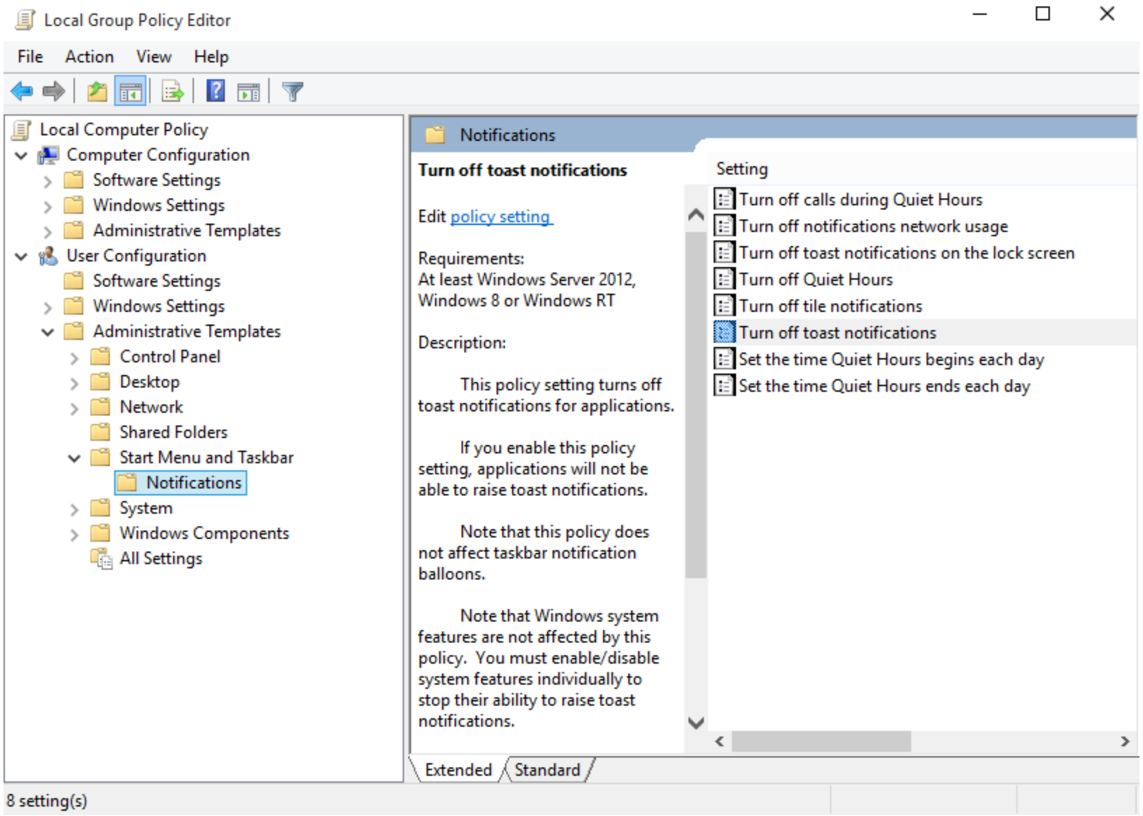
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Group Policies to suppress pop-up messages.

Additionally, on Windows 10 the following policies exist to help manage the toast and notification features:

Policy Type	Location	Feature	Description
User Configuration	Administrative Templates\ Start Menu and Taskbar\ Notifications	Turn off toast notifications	This policy setting turns off toast notifications.
User Configuration	Administrative Templates\ Start Menu and Taskbar\ Notifications	Turn off notifications network usage	This policy setting blocks application from using the network to send notifications to update tiles, tile badges, toast or raw notifications.
User Configuration	Administrative Templates\ Start Menu and Taskbar\ Notifications	Turn off toast notifications on the lock screen	This policy setting turns off toast notifications on the lock screen.
User Configuration	Administrative Templates\ Start Menu and Taskbar\ Push Notifications	Turn off tile notifications	This policy setting turns off tile notifications.



Turn off toast notifications

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:

This policy setting turns off toast notifications for applications.

If you enable this policy setting, applications will not be able to raise toast notifications.

Note that this policy does not affect taskbar notification balloons.

Note that Windows system features are not affected by this policy. You must enable/disable system features individually to stop their ability to raise toast notifications.

Setting
- Turn off calls during Quiet Hours
- Turn off notifications network usage
- Turn off toast notifications on the lock screen
- Turn off Quiet Hours
- Turn off tile notifications
- Turn off toast notifications
- Set the time Quiet Hours begins each day
- Set the time Quiet Hours ends each day

If it is not desired to turn off all notifications, the notifications can also be enabled/disabled at an application label via the "Notification" section of the Settings area. The settings available here are as follows:

- Show app notifications ON/OFF
- Show app notifications on the lock screen ON/OFF
- Play notification sounds ON/OFF
- Show notifications from these apps: There will be a listing of applications that have been installed on the system that provide notifications, each with a separate ON/OFF indicator.

Windows Diagnostic 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:

1. Start the Policy Editor by typing “GPEDIT” from “Search” in the charms bar.

2. Navigate to Local Computer Policy> Computer Configuration> Administrative Templates> System> Troubleshooting and Diagnostics> Diagnostics: Configure scenario execution level.

3. Enable the policy, set Scenario execution level to “Detection and Troubleshooting Only.”

Hide Windows fatal error messages

When a STOP message (a fatal system error message) displays in Windows, the computer enters debug mode for troubleshooting. The error message appears on 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 ntskrnl.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)

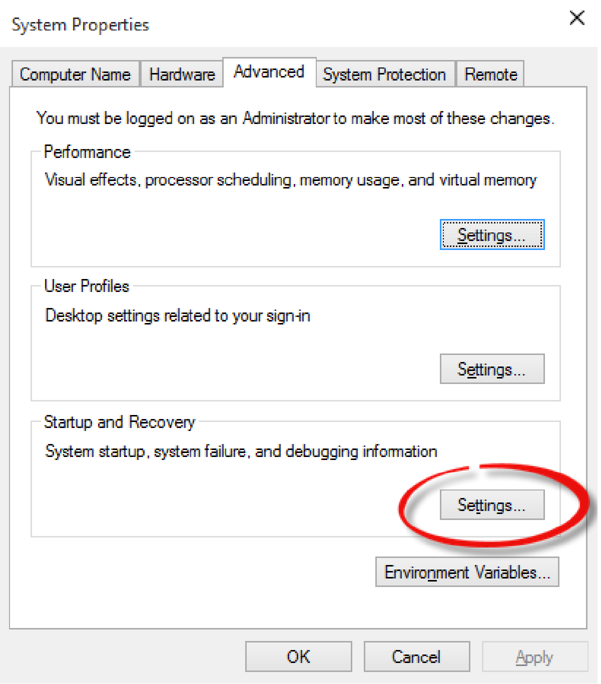
Additionally you can clear the flag “CrashDumpEnabled” in order to prevent the device from creating a crash dump file using:

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.

The same functionality can be enabled through the desktop UI.

- Go to Control Panel > System and Security > System
- Select Change Settings
- Select the Advanced tab
- Select Settings under Startup and Recovery

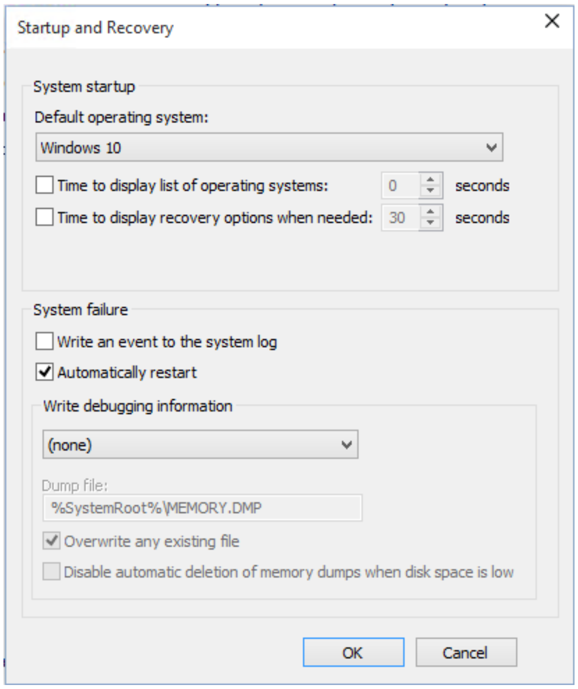


You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your sign-in

Startup and Recovery
System startup, system failure, and debugging information



System startup

Default operating system: Windows 10

□ Time to display list of operating systems: 0 seconds

□ Time to display recovery options when needed: 30 seconds

System failure

□ Write an event to the system log

☑ Automatically restart

Write debugging information: (none)

Dump file: %SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

□ Disable automatic deletion of memory dumps when disk space is low

Protect physical storage media with Unified Write Filter

You can use Unified Write Filter (UWF) in Windows 10 IoT Enterprise to help protect physical storage media, including most standard writable storage types that are supported by Windows 10, such as physical hard disks, solid-state drives, internal USB devices, external SATA devices, and so on. You can also use UWF to return the device to a known configuration on reboot by making read-only media appear to the OS as a writable volume. Additionally, you can exclude specific files, folders, or registry keys from being filtered by UWF and add them to an exclusion list.

Learn more at: http://go.microsoft.com/fwlink/?LinkID=616857

Tools

Microsoft provides a collection of tools that you can use to customize, assess, and deploy Windows operating systems to new devices. This collection of tools is called the Windows Assessment and Deployment Kit (Windows ADK).

Image Configuration Designer (ICD)

The Windows Imaging and Configuration Designer (ICD) tool streamlines the customizing and provisioning of a Windows image.

Learn more at: http://go.microsoft.com/fwlink/?LinkID=616858

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. This document is confidential and proprietary to Microsoft. It is disclosed and can be used only pursuant to a non-disclosure agreement.

Microsoft