Windows 10 IoT Enterprise

Lockdown Features

Microsoft

Windows 10 IoT Enterprise

The full version of Windows 10 Enterprise with advanced lockdown capabilities

Classic Windows applications and Universal Windows apps for mission critical industry devices

Features Highlight for Windows 10 IoT Enterprise

Feature	Benefit
Mobile Device Management (MDM)	Consistent management framework across devices (1st or 3rd party)
Granular UX Control and Lockdown	Provide a predicable and consistent device experience
Machine login with Azure AD Join and Azure State	Simplify device access to cloud resources
Device Guard*	Protect operating system from running unwanted apps and increase security on mission critical devices.
Credential Guard*	Protect device credentials from pass the hash attacks
Custom Branding (logon and boot)	Helps create a custom device experience
AppLocker	Prevent users from installing and using unauthorized applications.
Next Generation Credentials	Reducing reliance on passwords, increasing resistance to theft and phishing
Image Configuration Designer (ICD)	Easily customize the device experience/image

* Requires UEFI 2.3.1 or greater; Virtualization Extensions such as Intel VT-x, AMD-V, and SLAT must be enabled; x64 version of Windows; IOMMU, such as Intel VT-d, AMD-Vi; TPM 2.0; BIOS Lockdown;

Feature Comparisons

of Windows 10 based products

Core Features

Familiar, and better than ever	Windows 10 Pro	Windows 10 Enterprise	Windows 10 IoT Enterprise
Customizable Start Menu	√	√	√
Windows Defender & Windows firewall	√	√	√
Fast start up with Hiberboot and InstantGo[1]	√	√	√
TPM support[2]	√	√	√
Battery Saver	√	√	√
Windows Update	√	√	√
Cortana[5]			
Talk or type naturally	√	√	√
Personal and proactive suggestions	√	√	√
Reminders	√	√	√
Search web, device, and cloud	√	√	√
“Hey Cortana” hands-free activation	√	√	√
Windows Hello			
Native fingerprint recognition	√	√	√
Native facial and iris recognition	√	√	√
Enterprise level security	√	√	√
Multi-doing			
Virtual desktops	√	√	√
Snap assist (up to 4 apps on one screen)	√	√	√
Snap apps across screens on different monitors	√	√	√
Continuum[4]			
Switch from PC to tablet mode	√	√	√
Microsoft Edge			
Reading view	√	√	
Built-in ink support	√	√	
Cortana integration[5]	√	√	
Universal Windows Platform			
Universal Windows apps	√	√	√
Classic Desktop applications	√	√	√
Microsoft Universal Windows apps included	√	√	
Microsoft Store Client	√	√	

3DBuilder
AppConnector
Bing Finance
Bing News
Bing Sports
BingWeather
Getstarted
MicrosoftSolitaireCollection
Office Hub
Office.OneNote
People
Phone Companion App
SkypeApp
WindowsAlarms
WindowsCalculator
WindowsCamera
WindowsCommunicationsApps
WindowsMaps
WindowsPhotos
WindowsSound Recorder
WindowsStore
XboxApp
ZuneMusic
ZuneVideo

Business Features

	Windows 10 Pro	Windows 10 Enterprise	Windows 10 IoT Enterprise
Existing fundamentals			
Device Encryption[6]	√	√	√
Domain Join	√	√	√
Group Policy Management	√	√	√
BitLocker2	√	√	√
Enterprise Mode Internet Explorer (EMIE)	√	√	√
Assigned Access 8.1	√	√	√
Remote Desktop	√	√	√
Direct Access		√	√
Windows To Go Creator	√	√	√
AppLocker		√	√
BranchCache		√	√
Start Screen Control with Group Policy		√	√
Management and deployment			
Side-loading of line of business apps	√	√	√
Mobile device management	√	√	√
Ability to join Azure Active Directory, with single sign-on to cloud-hosted apps[7]	√	√	√
Business Store for Windows 10[8]		√	
Granular UX Control		√	√
Easy Upgrade from Pro to Enterprise Edition	√	√	√
Easy Upgrade from Home to Education Edition			
Security			
Microsoft Passport	√	√	√
Enterprise Data Protection[8]	√	√	√
Credential Guard[9]		√	√
Device Guard[9]		√	√
Delivering Windows as a service			
Windows Update	√	√	√
Windows Update for Business	√	√	
Current Branch for Business	√	√	
Long Term Servicing Branch		√	√

Not allowed with current licensing terms

Name for grouping of features for creating a targeted device experience

Granular UX Control

Granular UX Control	Windows 10 Pro	Windows 10 Enterprise	Windows 10 IoT Enterprise
Unified Write Filter		√	√
Embedded Logon		√	√
Assigned Access		√	√
Shell Launcher		√	√
Embedded Boot Expereince		√	√
Unbranded Screens		√	√
AppLocker		√	√
MDM & Group Policies		√	√

Lockdown Features

of Windows 10 IoT Enterprise

Lockdown Feature Comparisons

	Windows Embedded 8.1 Industry Pro		Windows 10 IoT Enterprise
Capability	**Feature Mapping**		
Protect devices physical storage media	Unified Write Filter	----->	Unified Write Filter
Boot fast to a know state on the device	HORM	X	
Suppress Windows UI elements displayed during Windows logon and shutdown	Embedded Logon	----->	Embedded Logon
Block edge gestures	Gesture Filter	----->	Assigned Access
Block hotkeys and other key combinations	Keyboard Filter	----->	Assigned Access / Shell Launcher
Launch a desktop app on login	Shell Launcher	----->	Shell Launcher
Launch a Universal Windows app on login	Application Launcher	----->	Assigned Access
Suppress system dialogs & control processes that can run	Dialog Filter	----->	AppLocker & MDM policies
Suppress toast notifications	Toast Filter	----->	MDM & Group policies
Configure lockdown features	Embedded Lockdown Manager	----->	ICD / Provisioning package(s)
Restrict USB devices / peripherals on system	USB Filter	----->	MDM & Group policies
Launch a Universal Windows app on login plus lock access to system	Assigned Access	----->	Assigned Access
Custom brand a device by removing and/or replace Windows UI boot elements	Embedded Boot Experience / Unbranded Screens	----->	Embedded Boot Experience / Unbranded Screens
Suppress Windows UI elements displayed during logon and logoff	Embedded Logon	----->	Embedded Logon

Lockdown of Windows 10 IoT Enterprise

Consistent and predictable device lockdown across form factors

Unified Write Filter

Easily create read only devices
Improve system uptime

USB Access

Only allow approved USB devices

Layout Control

Customize the Start Menu layout for special purpose devices

AppLocker

Control which apps are visible and can run

Shell Launcher

Enable a single Win32 app experience

Assigned Access

Enable a single Universal Windows app experience

Unified Write Filter (UWF)

Sector Based Protection

Registry Exclusion

File & Folder Exclusion

Windows 10 Enterprise / IoT Enterprise

Create read only devices

Protect system against write operations

Improve system up-time

Reduce IT support & improve compliance

Unified Write Filter (UWF)

Not support Fast Startup function of Windows 10

Control Panel > System and Security > Power Options > Choose what he power button does > Turn on fast startup

Support all fixed volume type (except for external USB volume), master boot record (MBR) volume, GUID partition table (GPT) volume.

HDD, SSD, Internal USB device, External SATA device

Exclusion of UWF

Not support exclusions as following items (File and Folder)

\Windows\System32\DEFAULT

\Windows\System32\SAM

\Windows\System32\SECURITY

\Windows\System32\SOFTWARE

\Windows\System32\SYSTEM

\Users\<User Name>\NTUSER.DAT

The volume root. For example, C: or D:.

The \Windows folder on the system volume.

The \Windows\System32 folder on the system volume.

The \Windows\System32\Drivers folder on the system volume.

Paging files.

Exclusion of UWF

Only support exclusions as following items (Registry Key)

HKEY_LOCAL_MACHINE\BCD00000000

HKEY_LOCAL_MACHINE\SYSTEM

HKEY_LOCAL_MACHINE\SOFTWARE

HKEY_LOCAL_MACHINE\SAM

HKEY_LOCAL_MACHINE\SECURITY

HKEY_LOCAL_MACHINE\COMPONENTS

UWF servicing mode

Windows updates, antimalware signature file update, Custom software or third-party software update

Turn on / off UWF

To turn UWF on or off by using Control Panel

Control Panel > Program > Programs and Features > Turn Windows features on or off >

Windows Features > Unified Write Filter

To turn UWF on or off by using DISM

Command prompt with administrator rights.

```
dism /online /Enable-Feature /FeatureName:Client-UnifiedWriteFilter
```

```
dism /online /Disable-Feature /FeatureName:Client-UnifiedWriteFilter
```

To turn UWF on or off by using ICD

Build a provisioning package in Windows ICD

Available customizations page > Runtime settings > UnifiedWriteFilter

Restart device for turning on or off UWF

Enable / Disable UWF

Enable or disable UWF

- Windows Management Instrumentation (WMI) class UWF_Filter
- Command line tool uwfmgr.exe

Improve the performance of UWF

- Paging files are disabled.
- System restore is disabled.
- SuperFetch is disabled.
- File indexing service is turned off.
- Fast boot is disabled.
- Defragmentation service is turned off.
- BCD setting bootstatuspolicy is set to ignoreallfailures.

Configure UWF

Configure UWF

Use the WMI providers directly in a Windows PowerShell script

Use the WMI providers directly in an application

https://msdn.microsoft.com/en-us/library/windows/hardware/mt571998(v=vs.85).aspx

User the command line tool, uwfmgr.exe

https://msdn.microsoft.com/en-us/library/windows/hardware/mt572002(v=vs.85).aspx

Custom Logon

Suppress Windows 10 UI element

Welcome screen, shutdown screen, Blocked Shutdown Resolver (BSDR) screen, automatically end application

https://msdn.microsoft.com/en-us/library/windows/hardware/mt571990(v=vs.85).aspx

Turn on Custom Logon

Turn on Custom Logon using Unattend

Use Windows System Image Manager(Windows SIM)

Microsoft-Windows-Embedded-EmbeddedLogon component

Turn on Custom Logon using Windows Imaging and Configuration Designer

Build a provisioning package in Windows ICD

Available customizations page > Runtime settings > SMISettings

BrandingNeutral = TRUE
AnimationDisabled = TRUE
NoLockScreen = TRUE
UIVerbosityLevel = 0 | 1
HideAutoLogonUI = TRUE

Turn on Custom Logon

Turn on Custom Logon using DISM

Command prompt with administrator rights

```
Dism /online /Enable-Feature /FeatureName:Client-EmbeddedLogon
```

```
Dism /online /Disable-Feature /FeatureName:Client-EmbeddedLogon
```

Turn on Custom Logon in Control Panel

Control Panel > Programs and Features > Turn Windows features on or off >

Windows Features on or off > Embedded Logon.

Complementary features to Custom Logon

Power button

To remove the power button from the Welcome screen

1. Sign in with an administrator account.
2. From a command prompt, run gpedit.msc to open the Local Group Policy Editor.
3. Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
4. Double-tap or click 'Shutdown: Allow system to be shut down without having to log on'.
5. In the 'Shutdown: Allow system to be shut down without...' dialog box, select Disabled, and then tap or click OK.

Complementary features to Custom Logon

Welcome screen

To remove buttons from the Welcome screen

HKLM\Software\Microsoft\Windows Embedded\EmbeddedLogon - BrandingNeutral

Action	Registry value
Disable all Welcome screen UI elements	static const DWORD EMBEDDED_DISABLE_LOGON_ANCHOR_ALL = 0x1
Disable the Power button	static const DWORD EMBEDDED_DISABLE_LOGON_ANCHOR_SHUTDOWN = 0x2
Disable the Language button	static const DWORD EMBEDDED_DISABLE_LOGON_ANCHOR_LANGUAGE = 0x4
Disable the Ease of Access button	static const DWORD EMBEDDED_DISABLE_LOGON_ANCHOR_EASEOFACCESS = 0x8
Disable the Switch user button.	static const DWORD EMBEDDED_DISABLE_BACK_BUTTON = 0x10
Disable the Blocked Shutdown Resolver (BSDR) screen so that restarting or shutting down the system causes the OS to immediately force close any open applications that are blocking system shut down. No UI is displayed, and users are not given a chance to cancel the shutdown process	static const DWORD EMBEDDED_DISABLE_BSDR= 0x20

Complementary features to Custom Logon

Welcome screen

To remove Wireless UI from the Welcome screen

1. From a command prompt, run gpedit.msc to open the Local Group Policy Editor.
2. Computer Configuration > Administrative Templates > System > logon
3. Double-tap or click 'Do not display network selection UI'.
4. In the 'Do not display network selection UI ' dialog box, select Enabled, and then tap or click OK

Unbranded Boot

Suppress Windows 10 start, resume, crash screen

https://msdn.microsoft.com/en-us/library/windows/hardware/mt571997(v=vs.85).aspx

Unbranded Boot

Configure Unbranded Boot using Unattend

Windows SIM

Microsoft-Windows-Embedded-BootExp component

Configure Unbranded Boot using Windows ICD

Build a provisioning package in Windows ICD

Available customizations page > Runtime setings > SMISettings > Unbranded Boot

Unbranded Boot

Configure Unbranded Boot using BCDEdit

To configure Unbranded Boot settings at runtime using BCDEdit

1. Open a command prompt as an administrator.
2. To disable the F8 key during startup to prevent access to the Advanced startup options menu, type the following:

   ```
   bcdedit.exe -set {globalsettings} advancedoptions false
   ```

3. To disable the F10 key during startup to prevent access to the Advanced startup options menu, type the following:

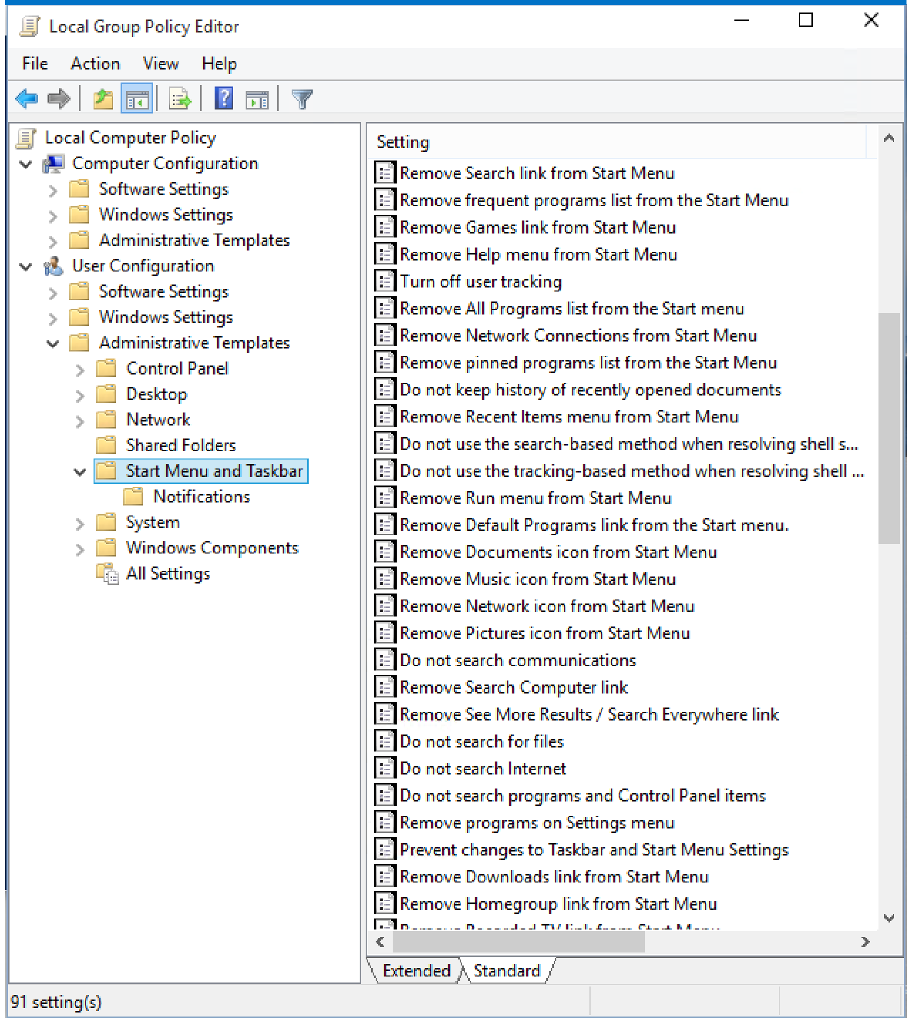
   ```
   bcdedit.exe -set {globalsettings} optionsedit false
   ```

4. To suppress all Windows UI elements (logo, status indicator, and status message) during startup, type the following:

   ```
   bcdedit.exe -set {globalsettings} bootuxdisabled on
   ```

Granular UX Control | Group Policy or ICD

Fully customize the Start Menu, Start Screen taskbar to a desired layout



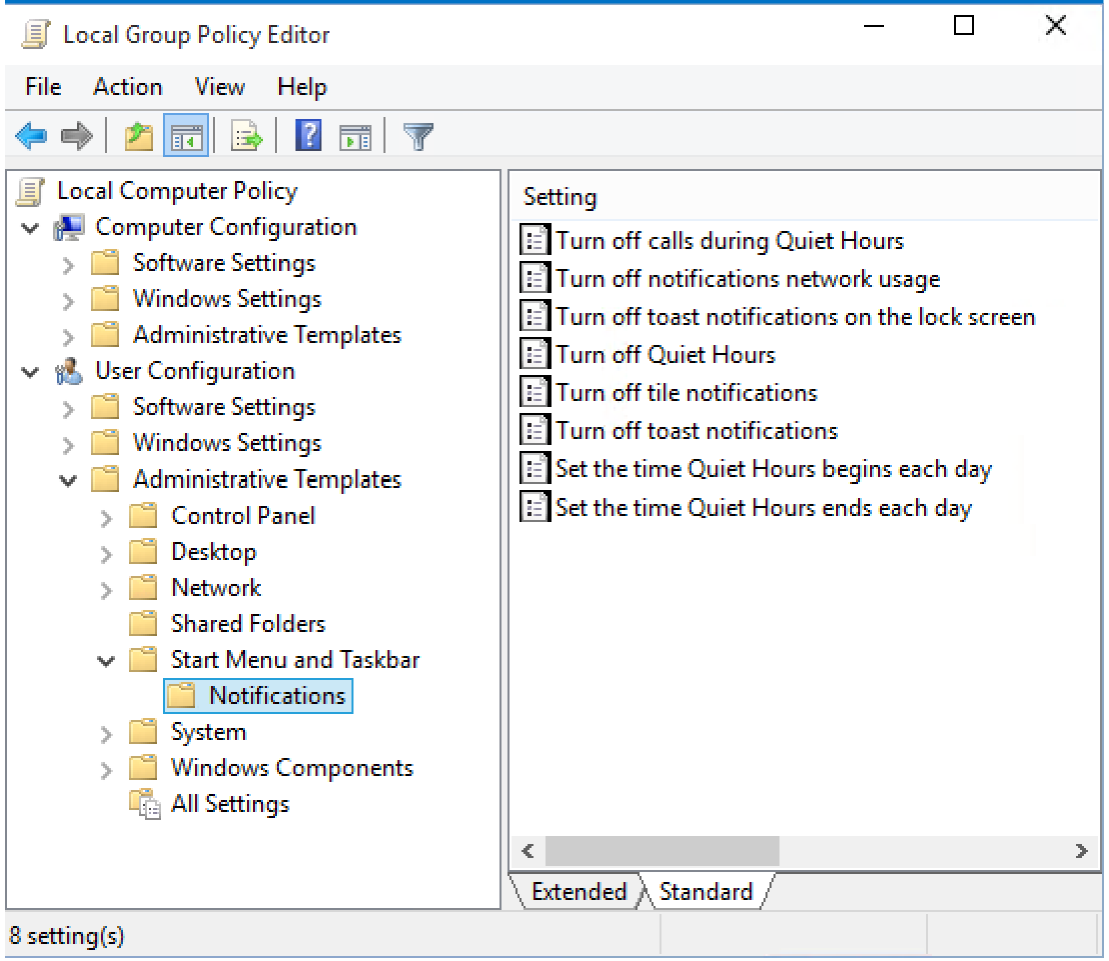
- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Desktop
      - Network
      - Shared Folders
      - Start Menu and Taskbar
        - Notifications
      - System
      - Windows Components
      - All Settings

Setting

- Remove Search link from Start Menu
- Remove frequent programs list from the Start Menu
- Remove Games link from Start Menu
- Remove Help menu from Start Menu
- Turn off user tracking
- Remove All Programs list from the Start menu
- Remove Network Connections from Start Menu
- Remove pinned programs list from the Start Menu
- Do not keep history of recently opened documents
- Remove Recent Items menu from Start Menu
- Do not use the search-based method when resolving shell s...
- Do not use the tracking-based method when resolving shell ...
- Remove Run menu from Start Menu
- Remove Default Programs link from the Start menu.
- Remove Documents icon from Start Menu
- Remove Music icon from Start Menu
- Remove Network icon from Start Menu
- Remove Pictures icon from Start Menu
- Do not search communications
- Remove Search Computer link
- Remove See More Results / Search Everywhere link
- Do not search for files
- Do not search Internet
- Do not search programs and Control Panel items
- Remove programs on Settings menu
- Prevent changes to Taskbar and Start Menu Settings
- Remove Downloads link from Start Menu
- Remove Homegroup link from Start Menu
- Remove Recorded TV link from Start Menu

91 setting(s)

Suppress toast notifications



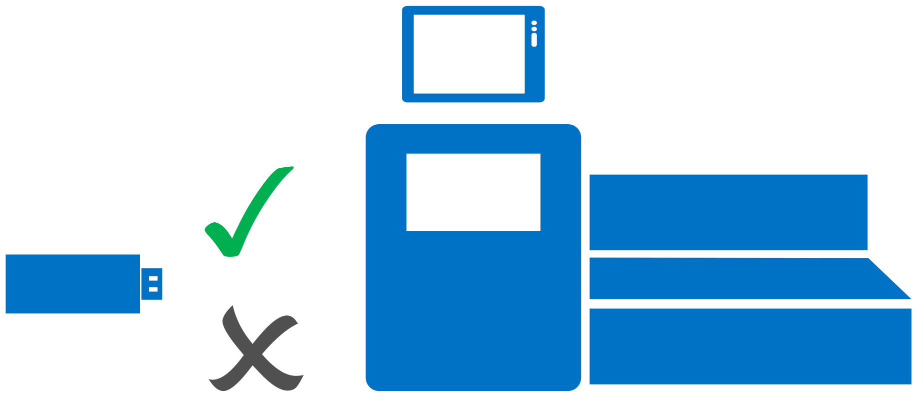
- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Desktop
      - Network
      - Shared Folders
      - Start Menu and Taskbar
        - Notifications
      - System
      - Windows Components
      - All Settings

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

8 setting(s)

Restrict Access to USB Devices | Group Policy or ICD



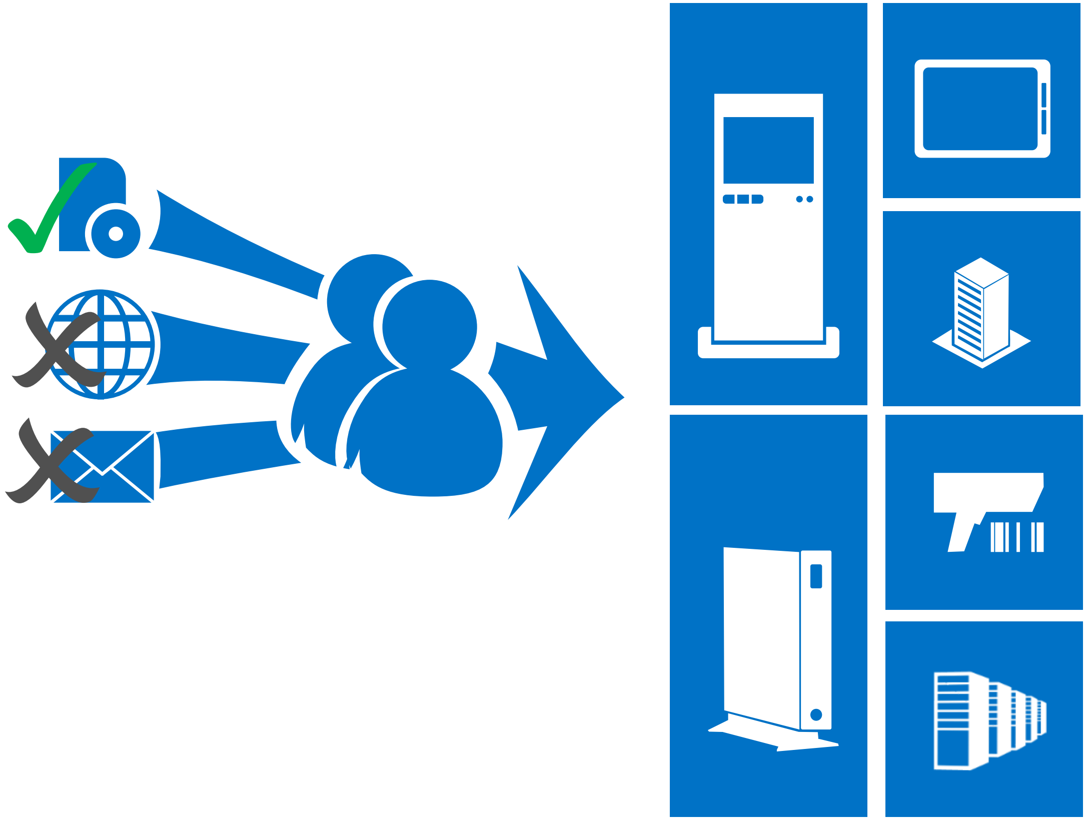
Prevent installation of all devices

Allow users to install only authorized devices

Prevent installation of prohibited devices

Control read and write permissions on removable media

AppLocker



Eliminate unwanted/unknown applications in your network

Enforce application standardization within your organization

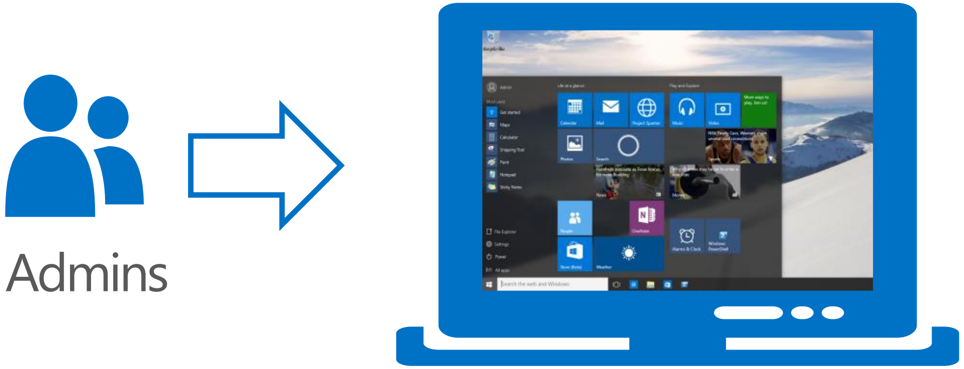
Easily create and manage flexible rules using Group Policy

Shell Launcher

Users
Classic Windows apps

Launch Classic Windows apps as a custom shell

Dedicated device & app experience



Different shells for different user groups

Admins can still have access to the Universal Windows Platform

Shell Launcher

Features on/off
To turn Shell Launcher on or off by using Control Panel
To turn Shell Launcher on or off by using DISM in PS

Functions
Enable or disable Shell Launcher.
Specify a shell configuration for a specific user or group.
Remove a shell configuration for a specific user or group.
Change the default shell configuration.
Get information on a shell configuration for a specific user or group.

Only one **WESL_UserSetting** instance exists on a device with Shell Launcher

Warning If your shell application requires administrator rights and needs to be elevated, and User Account Control (UAC) is present on your device, you must disable UAC in order for Shell Launcher to launch the shell application.

P.s> alternate method (Not recommended)
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKLM\Software\Microsoft\Windows Embedded\EmbeddedLogon

Shell Launcher

To turn Shell Launcher on or off by using Control Panel

1.In Control Panel, click Programs and Features.

2.In the Programs and Features window, click Turn Windows features on or off.

3.In the Windows Features window, expand the Embedded Features node, and check or clear the checkbox for Shell Launcher

To turn Shell Launcher on or off by using DISM

1.Open a command prompt with administrator rights.

2.At the command prompt, type the following command to turn on / off Shell Launcher:

```
Dism /online /Enable-Feature /FeatureName:Client-EmbeddedShellLauncher

Dism /online /Disable-Feature /FeatureName:Client-EmbeddedShellLauncher
```

Shell Launcher

Enable or disable Shell Launcher

By default, Shell Launcher is not enabled. You can enable or disable Shell Launcher by calling the WESL_UserSetting.SetEnabled function in the Windows Management Instrumentation (WMI) class WESL_UserSetting. If you enable or disable Shell Launcher, the changes do not affect any sessions that are currently signed in; you must sign out and sign back in.

Launch different shells for different user accounts

The default shell is set to cmd.exe

If you use the WMI providers to configure Shell Launcher for a user or group at run time, you must use the security identifier (SID) for that user or group; you cannot use the user name or group name.

Perform an action when the shell exits

Return code 0 (Restart the shell), 1(Restart the device), 2(Shut down the device), 3(Do nothing)

Shell Launcher

Custom shell launches with the same level of user rights as the account that signed in. This means that a user with administrator rights can perform any system action that requires administrator rights, including launching other applications with administrator rights. A user without administrator rights cannot perform any system action that requires administrator rights.

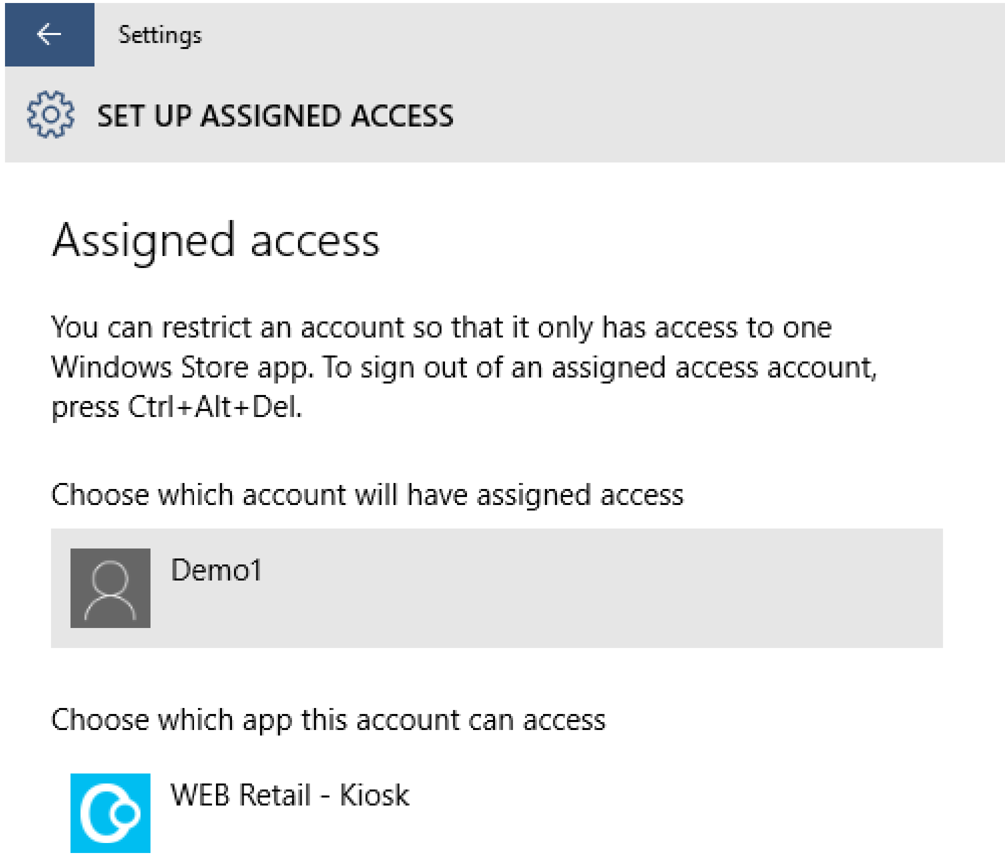
Configure Shell Launcher

WESL_UserSetting

Find the SID for a user and any groups : whoami command-line tool

https://technet.microsoft.com/en-us/library/cc771299(WS.10).aspx

Assigned Access



Settings

SET UP ASSIGNED ACCESS

Assigned access

You can restrict an account so that it only has access to one Windows Store app. To sign out of an assigned access account, press Ctrl+Alt+Del.

Choose which account will have assigned access

Demo1

Choose which app this account can access

WEB Retail - Kiosk

Easily create a single Universal Windows application experience

Assigned Access

In Windows 10, initially enabled

Steps
Log in as administrator.
Create the user account.
Log in as an user account
Install the application that follows the assigned access/above the lock guidelines.
Log out as user account
Log in as administrator
Configure assigned access.
Log out as administrator.
Log in as the user.

Way to configure
Configure assigned access by using Windows PowerShell (WE8.1 LBT & CM)
Configure assigned access by using the UI
Assigned access Windows PowerShell reference
WEDL_AssignedAccess

Only one user Can be set with One UWP app

Assigned access caution

Accessibility - Assigned access does not change **Ease of Access settings**. → You can block to using Keyboard Filter
Left Alt+Left Shift+Print Screen : Open High Contrast dialog box.
Left Alt+Left Shift+Num Lock :Open Mouse Keys dialog box.
Windows logo key+U : Open Ease of Access Center.

Key sequences blocked by assigned access
Alt+Spacebar :Open the shortcut menu for the active window.
Ctrl+Alt+Esc : Cycle through items in the reverse order from which they were opened.
Ctrl+Esc : Open the Start screen, Ctrl+F4Close the window ,Ctrl+Shift+EscOpen Task Manager.
Ctrl+Tab : Switch windows within the application currently open.
LaunchApp1 : Open the app that is assigned to this key.
LaunchApp2 : Open the app that is assigned to this key, which on many Microsoft keyboards is Calculator..
LaunchMail : Open the default mail client.
Windows logo key : Open the Start screen.

Not blocked → Keyboard Filter
Alt+F4, Alt+Shift+TaB, Alt+Tab
Ctrl+Alt+Delete is the key to break out of Assigned Access

Keyboard Filter settings apply to other standard accounts
UWFsettings apply to all users, including those with assigned access.

Assigned Access

Configure assigned access by using Windows PowerShell

LBT(Lockdown Baseline Tool (LBT) and Configuration Manager (CM)

Configure assigned access by using the UI

LB

Assigned access Windows PowerShell reference

LB

WEDL_AssignedAccess

LB

Summary

Windows 10 has No embedded features Nor embedded lockdown manager
Moreover no plan to release these UIs
So use WICD or Group policy editor etc…

Custom Logon
https://msdn.microsoft.com/en-us/library/windows/hardware/mt571990(v=vs.85).aspx

Unbranded Boot
https://msdn.microsoft.com/en-us/library/windows/hardware/mt571997(v=vs.85).aspx

Unified Write Filter
https://msdn.microsoft.com/en-us/library/windows/hardware/mt572001(v=vs.85).aspx
Important : You cannot use UWF to protect external removable drives, USB devices or flash drives.
Read more other notes!

Other good tips/clarification
https://msdn.microsoft.com/en-us/library/dn449303(v=winembedded.82).aspx#BKMK_AssignedAccess

Online Resources

Customize
https://msdn.microsoft.com/en-us/library/windows/hardware/mt269765(v=vs.85).aspx

Setup a device for anyone to use (Kiosk mode)
https://technet.microsoft.com/en-us/library/mt219050(v=vs.85).aspx

Find the application user model id of an installed app
https://msdn.microsoft.com/ko-kr/library/dn449300(v=winembedded.82).aspx

Security Identifier (SID) : GetSID of a user, object using registry, WMIC, Powershell
http://blogs.msdn.com/b/gaurav/archive/2014/06/03/get-sid-of-the-object-registry-wmic-powershell.aspx

Microsoft