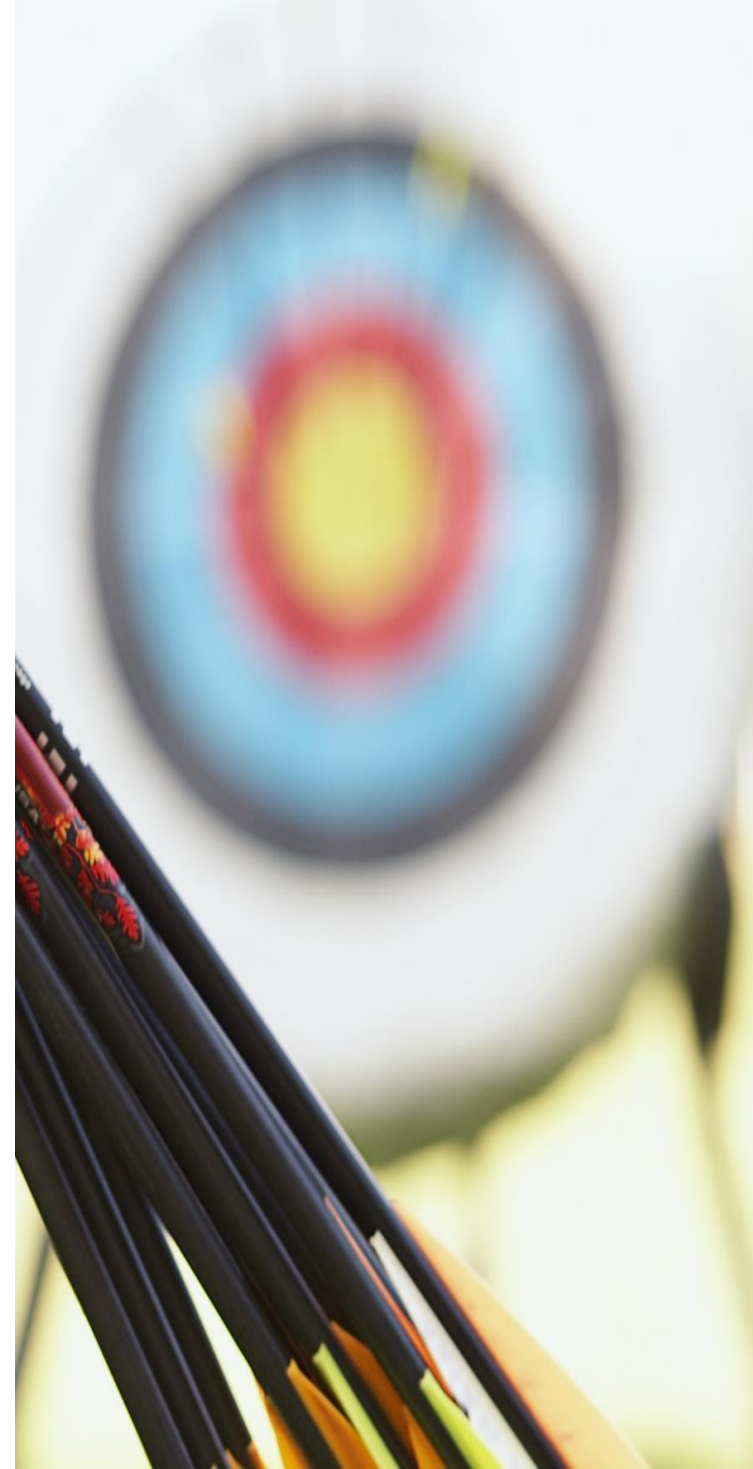


Windows Tech Series

Securing Windows IoT Devices and Solutions

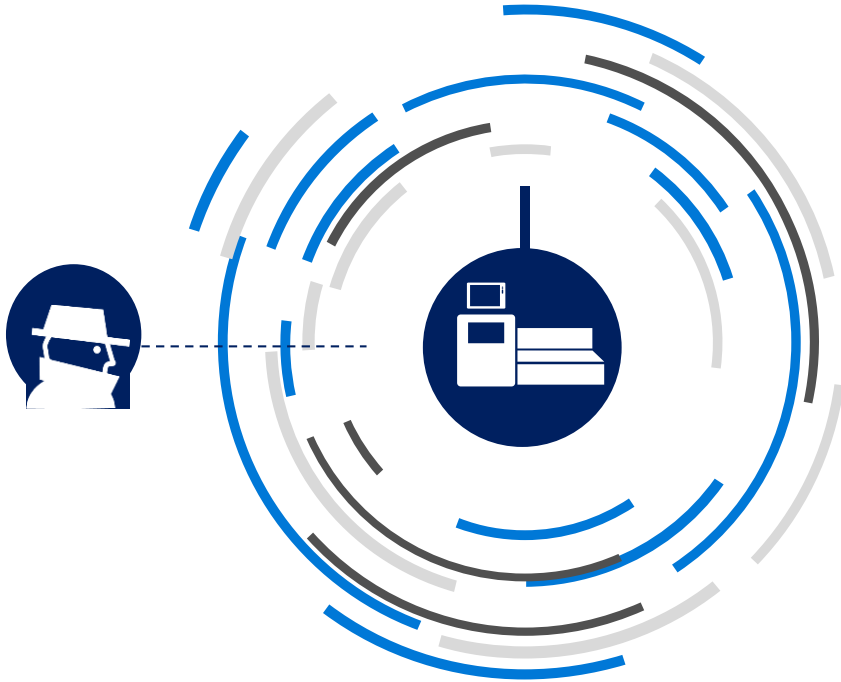
Objectives

- Review Windows 10 IoT security features
- Describe Windows 10 IoT lockdown technologies
- Describe Windows 10 IoT Device Guard



Introduction to Windows IoT Security

Securing IoT devices



- Next Generation Credentials
 - Two-factor authentication and SSO
- BitLocker
 - Device encryption and secure key storage
- Lockdown
 - Security layers and predictable device experiences
- Device Guard
 - Only run trusted apps
- TPM and Malware Protection
 - Including "Secure Boot", "Measured Boot", and Authenticity protection

Next Generation Credentials

- Easy to deploy two-factor password alternative
- Breach, theft, and phish resistant credentials
- Single sign-on experience
- Convenience, with security

Windows 10 IoT Enterprise only

BitLocker

- Protects data when a device is lost or stolen using full disk encryption
- Provides single sign-on and protection from cold boot attacks
- Easy to deploy and manageable at scale
- Offers market-leading integration, performance, and reliability
- Compliance for Common Criteria, FIPS 140-2, HIPPA, PCI DSS and more

Available for ***all*** Windows 10 IoT editions

Lockdown

- Lockdown capabilities across all Windows 10 IoT editions
 - Specific capabilities for each edition
- Provide extra layers of security
 - For example, block specific keys to prevent system access
- Provide predictable device experiences for LoB device scenarios
 - For example, default apps

Device Guard

- Only trusted apps will run, just like many mobile OS's (for example, Windows Phone)
- Untrusted apps and executables, such as malware, cannot run
- Works with Universal and Win32 apps

Supported on Windows 10 IoT Enterprise only

Securing IoT devices with TPM

Protect from malware

"Secure Boot" and enable remote attestation with "Measured Boot"

Enabling TPM Protection:

- On-chip
- Firmware
- Discrete (I2C or SPI)
- TPM Simulator-dev tool

Protect customer data

Enterprise grade device encryption and secure key storage

Resist tampering

Authenticity with a strong, hardware-bound device identity using Trusted Platform Modules (TPMs)

Windows 10 IoT Lockdown

Lockdown

Windows IoT Enterprise and IoT Core



Unified Write Filter

Easily create read only devices
Improve system uptime



USB Access

Only allow approved USB devices

Windows IoT Enterprise and Mobile Enterprise



AppLocker

Control which apps are visible and can run



Assigned Access

Enable a single (desktop) or multiple (mobile) UWP experience

Windows IoT Mobile Enterprise Only



Layout Control

Customize the Start Menu layout for special purpose devices

Windows IoT Enterprise Only



Shell Launcher

Enable a single Win32 app experience

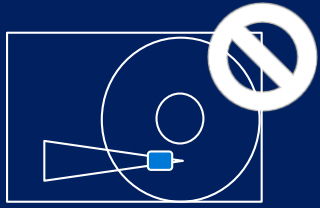


Block keyboard shortcuts/filter keys

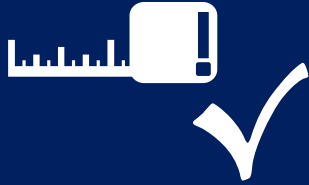
Block keyboard shortcuts and other keys to prevent system access

Consistent and predictable device lockdown across form factors

Unified Write Filter (UWF)



Sector Based Protection



Registry Exclusion



File and Folder Exclusion

- Create read-only devices
 - Protect system against write operations
 - Improve system uptime and reduce IT support
- Protect system against write operations
- Improve system uptime
 - Reduce IT support and improve compliance

Available for Windows 10 IoT Enterprise
and Windows 10 IoT Core

Restrict access to USB devices

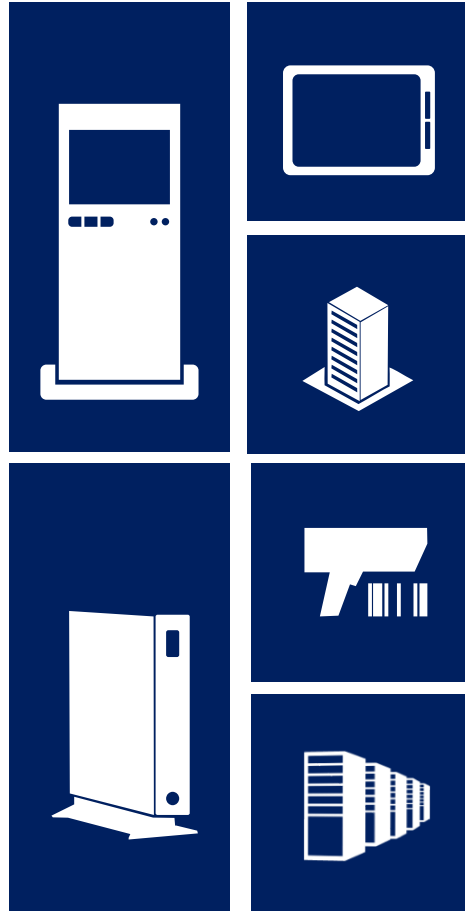
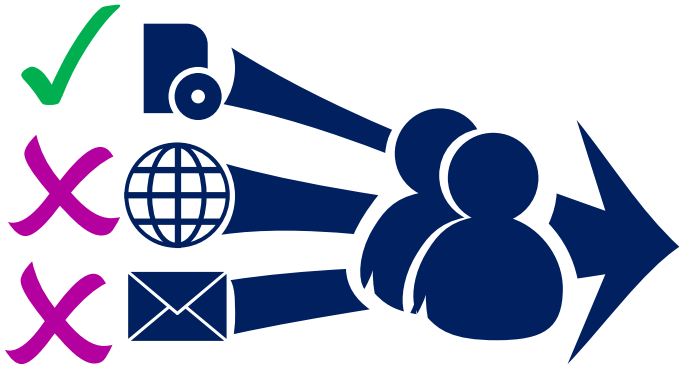


Group Policy or ICD

- 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

Available for Windows 10 IoT Enterprise and Windows 10 IoT Core

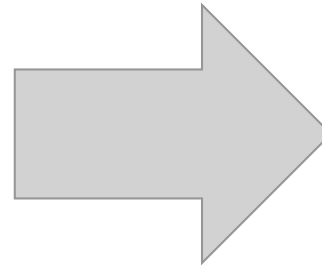
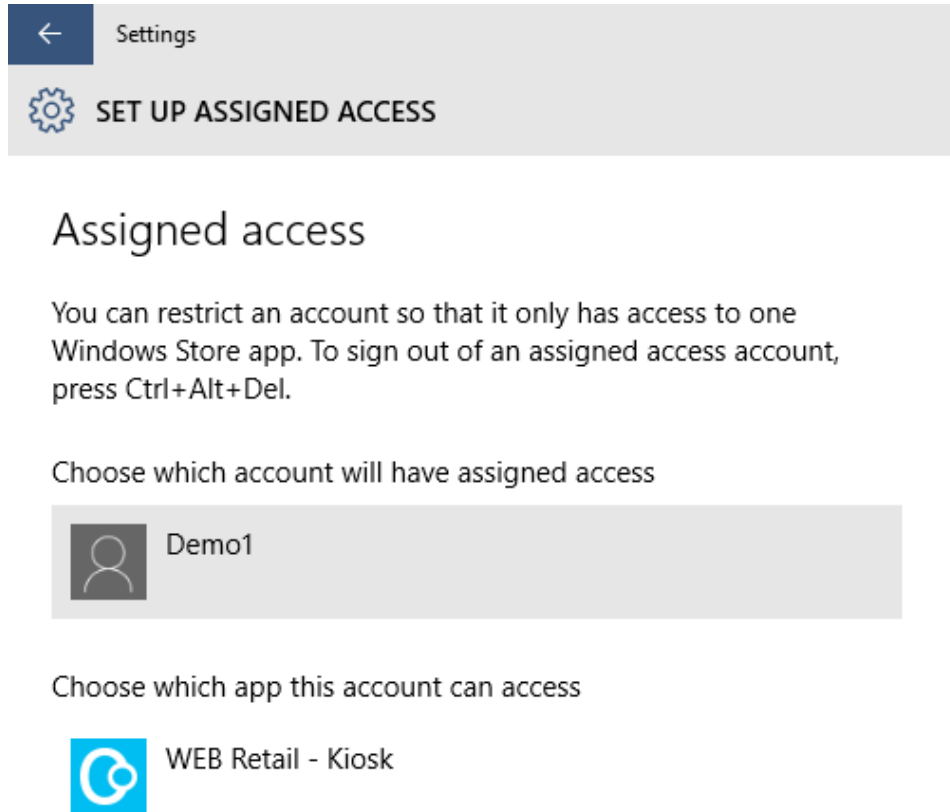
AppLocker



- Eliminate unwanted/unknown applications in your network
- Enforce application standardization within your organization
- Easily create and manage flexible rules using Group Policy

Available for Windows 10 IoT Enterprise and Windows 10 IoT Mobile Enterprise

Assigned access



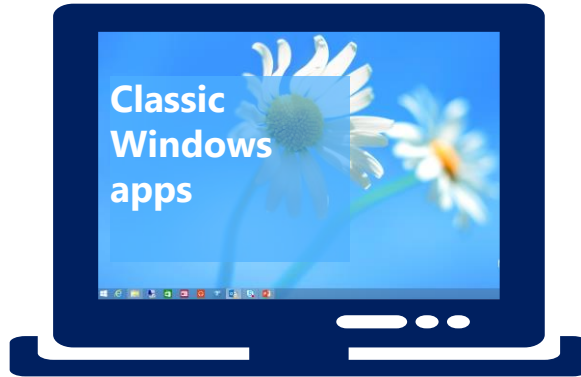
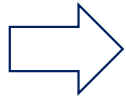
Easily create a single Universal Windows application experience

Available for Windows 10 IoT Enterprise
and Windows 10 IoT Mobile Enterprise

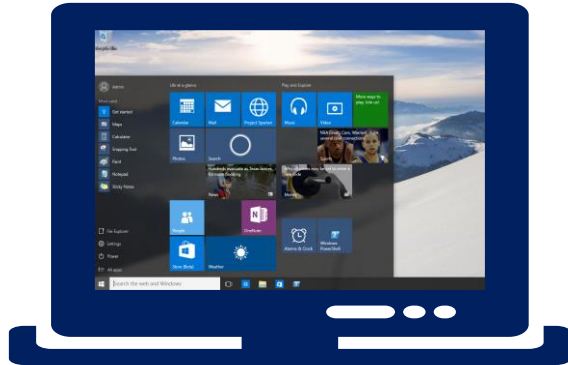
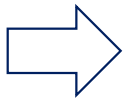
Shell Launcher



Users



Admins



- Launch Classic Windows apps as a custom shell
 - Dedicated device and app experience
- Different shells for different user groups
 - Admins can still have access to the Universal Windows Platform

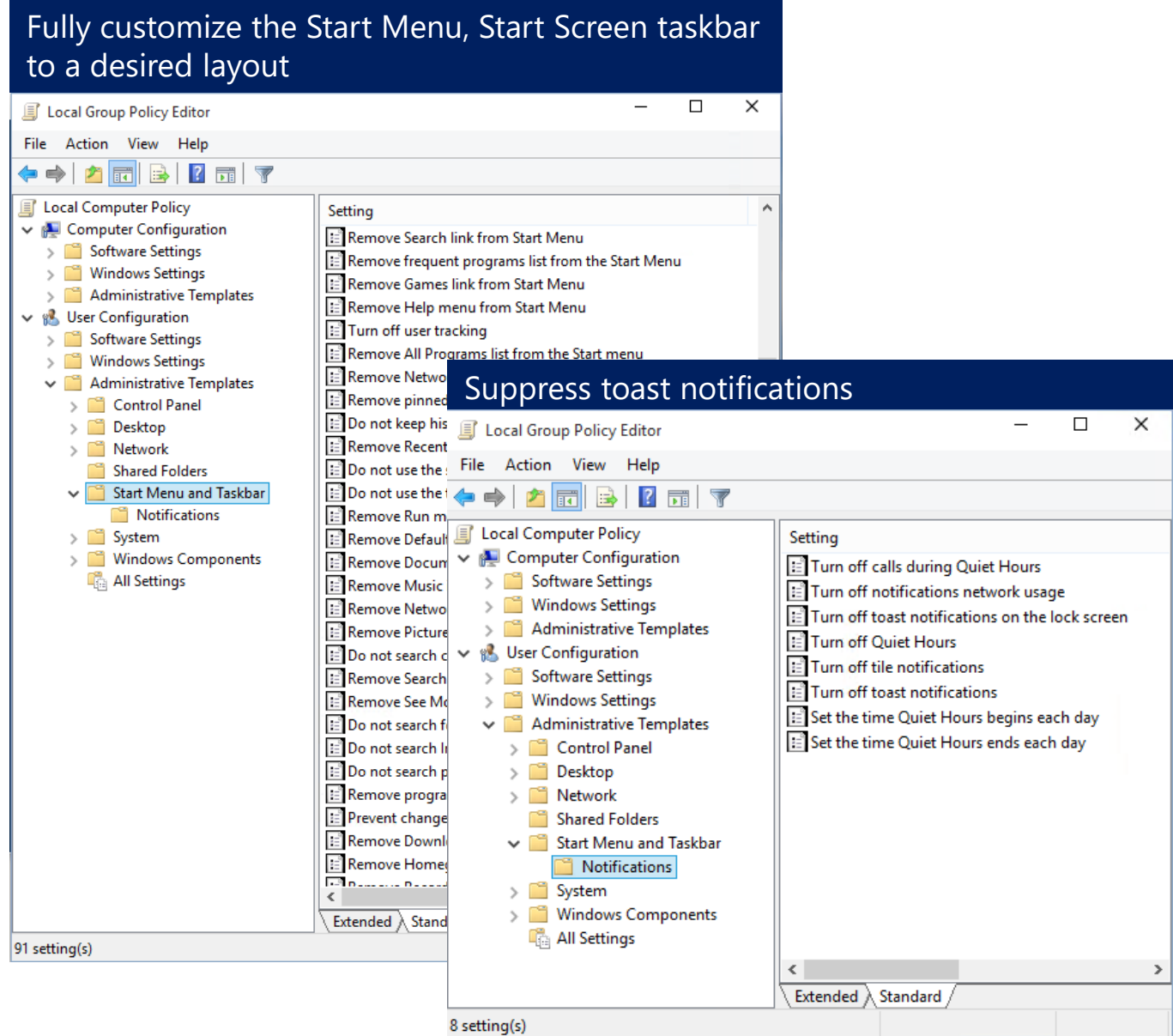
Available for Windows 10 IoT Enterprise only

Granular UX Control



- Customize the layout to meet the needs of the device and user experience
 - Keep users focused on line-of-business app(s) that matter
- Group Policy or ICD

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



The image displays two screenshots of the Windows Local Group Policy Editor. The top screenshot shows the 'Start Menu and Taskbar' category selected in the left-hand tree, with a list of 91 settings on the right. The bottom screenshot shows the 'Notifications' category selected, displaying 8 settings. A dark blue banner with white text 'Suppress toast notifications' is overlaid on the bottom screenshot.

Local Group Policy Editor

File Action View Help

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
- Remove pinned
- Do not keep his
- Remove Recent
- Do not use the
- Do not use the
- Remove Run m
- Remove Default
- Remove Docum
- Remove Music
- Remove Netwo
- Remove Picture
- Do not search c
- Remove Search
- Remove See Me
- Do not search f
- Do not search l
- Do not search p
- Remove progra
- Prevent change
- Remove Downl
- Remove Home

91 setting(s)

Suppress toast notifications

Local Group Policy Editor

File Action View Help

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

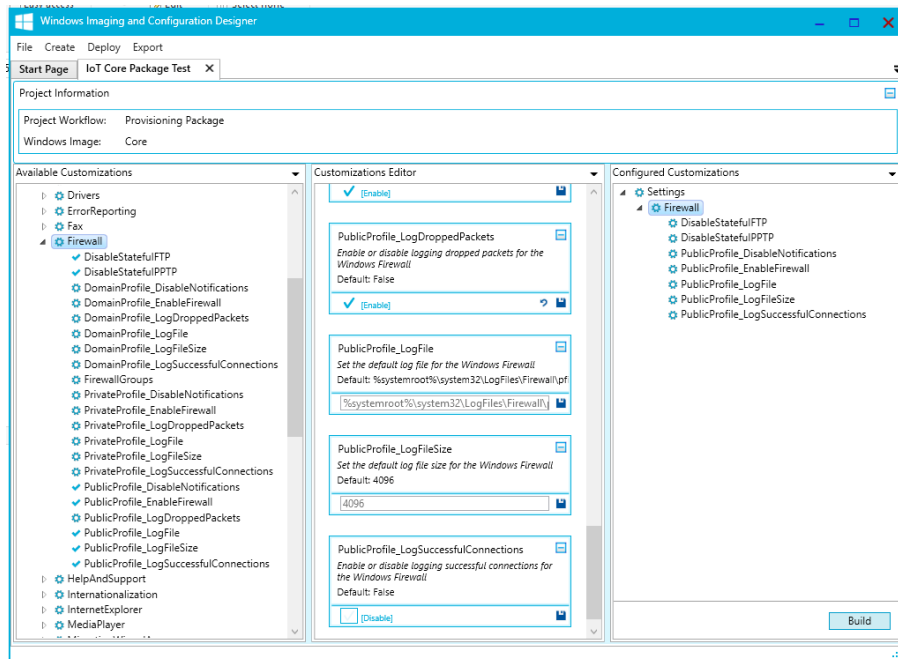
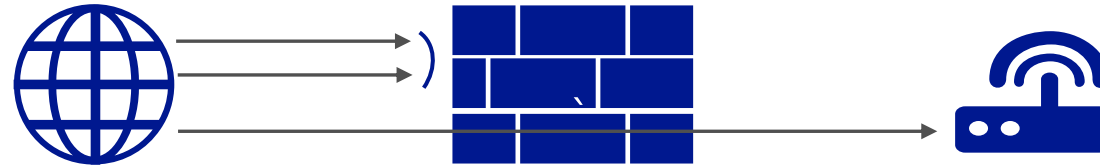
Setting

- 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

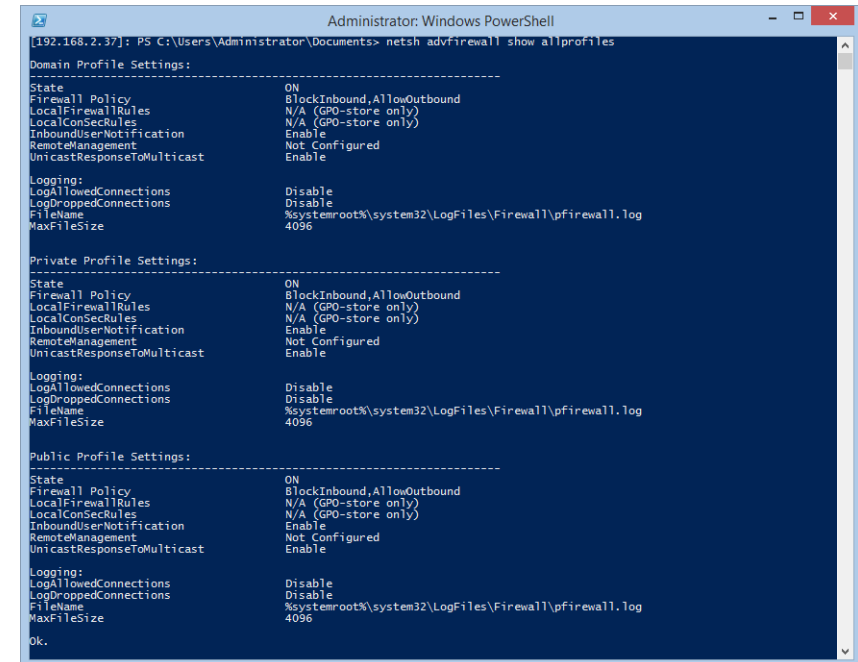
8 setting(s)

Windows Firewall

Block inbound connections, except those that you specifically allow



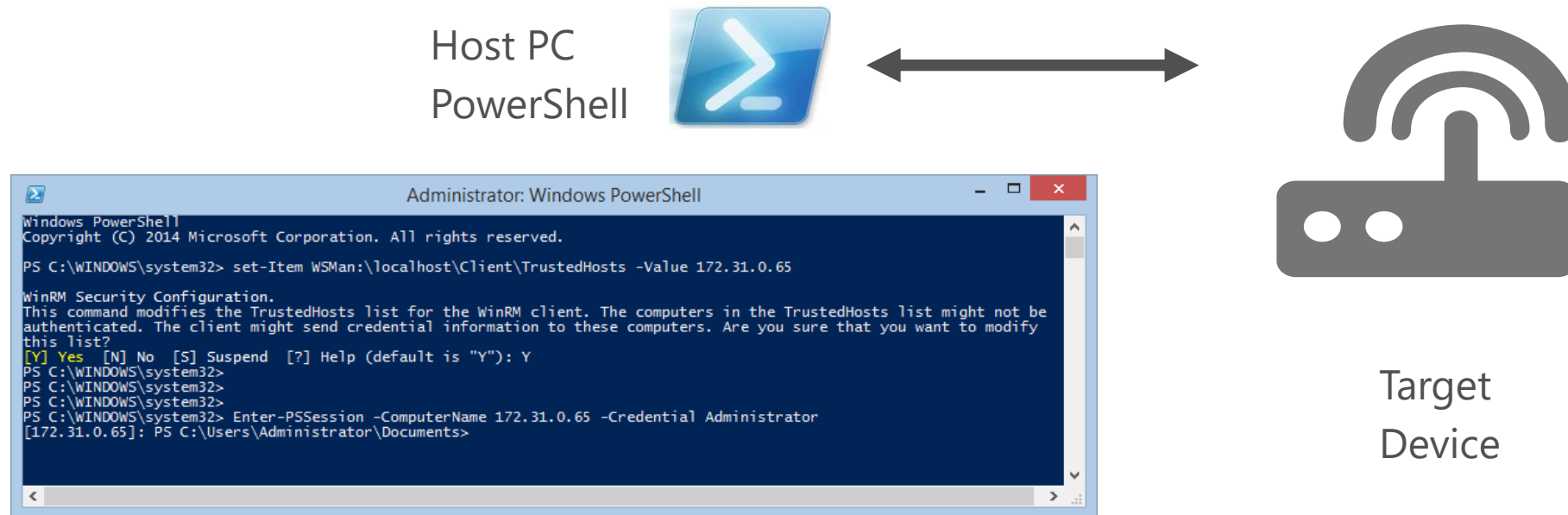
Configure firewall settings with
Image Configuration Designer



Configure firewall settings with
netsh advfirewall

Secure remote device connection

Trusted relationship between your host PC and your device



Windows 10 IoT Device Guard

Device Guard

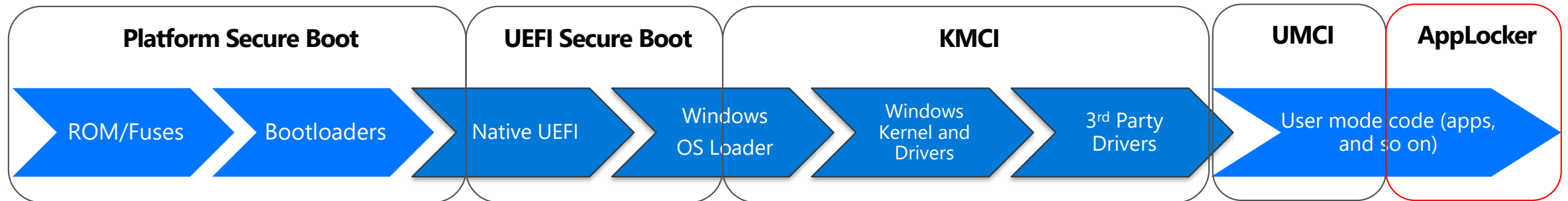
Enables a Windows desktop to be locked down to only run trusted apps:

- Similar to many mobile OSs (such as Windows Phone)
- Prevents untrusted apps and executables, such as malware, from running
- Provides resistance to tampering by an administrator, or by malware
- Requires devices specially configured by either the OEM or IT

Device Guard – components

Combination of hardware and software security features:

- Virtualization-based Security (VBS)
- Credential Guard
- Hypervisor-enforced Code Integrity
- Configurable Code Integrity (CI)



Device Guard – hardware requirements

- To enable Device Guard, the following hardware requirements must be met:
 - UEFI 2.3 or higher firmware, along with Secure Boot
 - Virtualization Extensions, such as Intel VT-X, AMD-V, and SLAT, must be enabled
 - BIOS lockdown
 - X64
 - IOMMU, such as Intel VT-D and AMD-Vi
 - Trusted Platform Module (TPM)

Device Guard – software requirements

- Supports UWP and Win32 apps – must be signed
- MSIs must be signed
- Windows Script Host requires signed scripts
 - WSH is the scripting host for VBScript (.vbs), JScript (.js), Windows Script File (.wsf) and Windows Script Component (.wsc) scripts
- .bat and .cmd scripts are not restricted
- PowerShell will be in “ConstrainedLanguage” mode
 - Signed PowerShell scripts can be in full language mode

Module review

In this module, you learned about:

- Windows 10 IoT security features
- Windows 10 IoT lockdown technologies
- Windows 10 IoT Device Guard





MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS ASSESSMENT AND ASSOCIATED TRAINING. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS ASSESSMENT AND ASSOCIATED TRAINING. Microsoft provides this document for information purposes only. It is provided "as is" and subject to change without notice.

This information is not warranted to be error-free. The information is not intended to constitute tax, accounting, legal or other professional advice. You should not act (or refrain from acting) based on information in this document without obtaining professional advice about your particular facts and circumstances. Some examples depicted herein are provided for illustration purposes only and are fictitious. No real association or connection is intended or should be inferred.

2016 Microsoft Corporation.

All rights reserved.