Contents

What's new in Windows 10

5/21/2019 • 2 minutes to read • Edit Online

Windows 10 provides IT professionals with advanced protection against modern security threats and comprehensive management and control over devices and apps, as well as flexible deployment, update, and support options. Learn about new features in Windows 10 for IT professionals, such as Windows Information Protection, Windows Hello, Device Guard, and more.

In this section

Learn more

- Windows 10 release information
- Windows 10 update history
- Windows 10 content from Microsoft Ignite
- Compare Windows 10 Editions

See also

Windows 10 Enterprise LTSC
Edit an existing topic using the Edit link

What's new in Windows 10, version 1903 IT Pro content

6/18/2019 • 10 minutes to read • Edit Online

Applies to

- Windows 10, version 1903

This article lists new and updated features and content that are of interest to IT Pros for Windows 10 version 1903, also known as the Windows 10 May 2019 Update. This update also contains all features and fixes included in previous cumulative updates to Windows 10, version 1809.

> **NOTE**
> New disk space requirement for Windows 10, version 1903 applies only to OEMs for the manufacture of new PCs. This new requirement does not apply to existing devices. PCs that don't meet new device disk space requirements will continue to receive updates and the 1903 update will require about the same amount of free disk space as previous updates. For more information, see Reserved storage.

Deployment

Windows Autopilot

Windows Autopilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. The following Windows Autopilot features are available in Windows 10, version 1903 and later:

- Windows Autopilot for white glove deployment is new in this version of Windows. "White glove" deployment enables partners or IT staff to pre-provision devices so they are fully configured and business ready for your users.
- The Intune enrollment status page (ESP) now tracks Intune Management Extensions.
- Cortana voiceover and speech recognition during OOBE is disabled by default for all Windows 10 Pro Education, and Enterprise SKUs.
- Windows Autopilot is self-updating during OOBE. Starting with the Windows 10, version 1903 Autopilot functional and critical updates will begin downloading automatically during OOBE.
- Windows Autopilot will set the diagnostics data level to Full on Windows 10 version 1903 and later during OOBE.

Windows 10 Subscription Activation

Windows 10 Education support has been added to Windows 10 Subscription Activation.

With Windows 10, version 1903, you can step-up from Windows 10 Pro Education to the enterprise-grade edition for educational institutions – Windows 10 Education. For more information, see Windows 10 Subscription Activation.

SetupDiag

SetupDiag version 1.4.1 is available.

SetupDiag is a command-line tool that can help diagnose why a Windows 10 update failed. SetupDiag works by searching Windows Setup log files. When searching log files, SetupDiag uses a set of rules to match known issues.

In the current version of SetupDiag there are 53 rules contained in the rules.xml file, which is extracted when SetupDiag is run. The rules.xml file will be updated as new versions of SetupDiag are made available.

Reserved storage

Reserved storage: Reserved storage sets aside disk space to be used by updates, apps, temporary files, and system caches. It improves the day-to-day function of your PC by ensuring critical OS functions always have access to disk space. Reserved storage will be enabled automatically on new PCs with Windows 10, version 1903 pre-installed, and for clean installs. It will not be enabled when updating from a previous version of Windows 10.

Servicing

- **Delivery Optimization**: Improved Peer Efficiency for enterprises and educational institutions with complex networks is enabled with of new policies. This now supports Office 365 ProPlus updates, and Intune content, with System Center Configuration Manager content coming soon!
- **Automatic Restart Sign-on (ARSO)**: Windows will automatically logon as the user and lock their device in order to complete the update, ensuring that when the user returns and unlocks the device, the update will be completed.
- **Windows Update for Business**: There will now be a single, common start date for phased deployments (no more SAC-T designation). In addition, there will a new notification and reboot scheduling experience for end users, the ability to enforce update installation and reboot deadlines, and the ability to provide end user control over reboots for a specific time period.
- **Update rollback improvements**: You can now automatically recover from startup failures by removing updates if the startup failure was introduced after the installation of recent driver or quality updates. When a device is unable to start up properly after the recent installation of Quality of driver updates, Windows will now automatically uninstall the updates to get the device back up and running normally.
- **Pause updates**: We have extended the ability to pause updates for both feature and monthly updates. This extension ability is for all editions of Windows 10, including Home. You can pause both feature and monthly updates for up to 35 days (seven days at a time, up to five times). Once the 35-day pause period is reached, you will need to update your device before pausing again.
- **Improved update notifications**: When there's an update requiring you to restart your device, you'll see a colored dot on the Power button in the Start menu and on the Windows icon in your taskbar.
- **Intelligent active hours**: To further enhance active hours, users will now have the option to let Windows Update intelligently adjust active hours based on their device-specific usage patterns. You must enable the intelligent active hours feature for the system to predict device-specific usage patterns.
- **Improved update orchestration to improve system responsiveness**: This feature will improve system performance by intelligently coordinating Windows updates and Microsoft Store updates, so they occur when users are away from their devices to minimize disruptions.

Security

Windows Information Protection

With this release, Windows Defender ATP extends discovery and protection of sensitive information with Auto Labeling.

Security configuration framework

With this release of Windows 10, Microsoft is introducing a new taxonomy for security configurations, called the **SECCON framework**, comprised of 5 device security configurations.

Security baseline for Windows 10 and Windows Server

The draft release of the security configuration baseline settings for Windows 10, version 1903 and for Windows Server version 1903 is available.

Intune security baselines

Intune Security Baselines (Preview): Now includes many settings supported by Intune that you can use to help secure and protect your users and devices. You can automatically set these settings to values recommended by security teams.

Microsoft Defender Advanced Threat Protection (ATP):

- Attack surface area reduction – IT admins can configure devices with advanced web protection that enables them to define allow and deny lists for specific URL's and IP addresses.
- Next generation protection – Controls have been extended to protection from ransomware, credential misuse, and attacks that are transmitted through removable storage.
  - Integrity enforcement capabilities – Enable remote runtime attestation of Windows 10 platform.
  - Tamper-proofing capabilities – Uses virtualization-based security to isolate critical ATP security capabilities away from the OS and attackers.
- Platform support – In addition to Windows 10, Windows Defender ATP's functionality has been extended to support Windows 7 and Windows 8.1 clients, as well as macOS, Linux, and Windows Server with both its Endpoint Detection (EDR) and Endpoint Protection Platform (EPP) capabilities.

Microsoft Defender ATP next-gen protection technologies:

- **Advanced machine learning**: Improved with advanced machine learning and AI models that enable it to protect against apex attackers using innovative vulnerability exploit techniques, tools and malware.
- **Emergency outbreak protection**: Provides emergency outbreak protection which will automatically update devices with new intelligence when a new outbreak has been detected.
- **Certified ISO 27001 compliance**: Ensures that the cloud service has analyzed for threats, vulnerabilities and impacts, and that risk management and security controls are in place.
- **Geolocation support**: Support geolocation and sovereignty of sample data as well as configurable retention policies.

Threat Protection

- Windows Sandbox: Isolated desktop environment where you can run untrusted software without the fear of lasting impact to your device.
- Microphone privacy settings: A microphone icon appears in the notification area letting you see which apps are using your microphone.
- Windows Defender Application Guard enhancements:
  - Standalone users can install and configure their Windows Defender Application Guard settings without needing to change Registry key settings. Enterprise users can check their settings to see what their administrators have configured for their machines to better understand the behavior.
  - WDAG is now an extension in Google Chrome and Mozilla Firefox. Many users are in a hybrid browser environment, and would like to extend WDAG's browser isolation technology beyond Microsoft Edge. In the latest release, users can install the WDAG extension in their Chrome or Firefox browsers. This extension will redirect untrusted navigations to the WDAG Edge browser. There is also a companion app to enable this feature in the Microsoft Store. Users can quickly launch WDAG from their desktop using this app. This feature is also available in Windows 10, version 1803 or later with the latest updates.

    To try this extension:

    1. Configure WDAG policies on your device.
    2. Go to the Chrome Web Store or Firefox Add-ons and search for Application Guard. Install the extension.
    3. Follow any additional configuration steps on the extension setup page.

4. Reboot the device.
5. Navigate to an untrusted site in Chrome and Firefox.

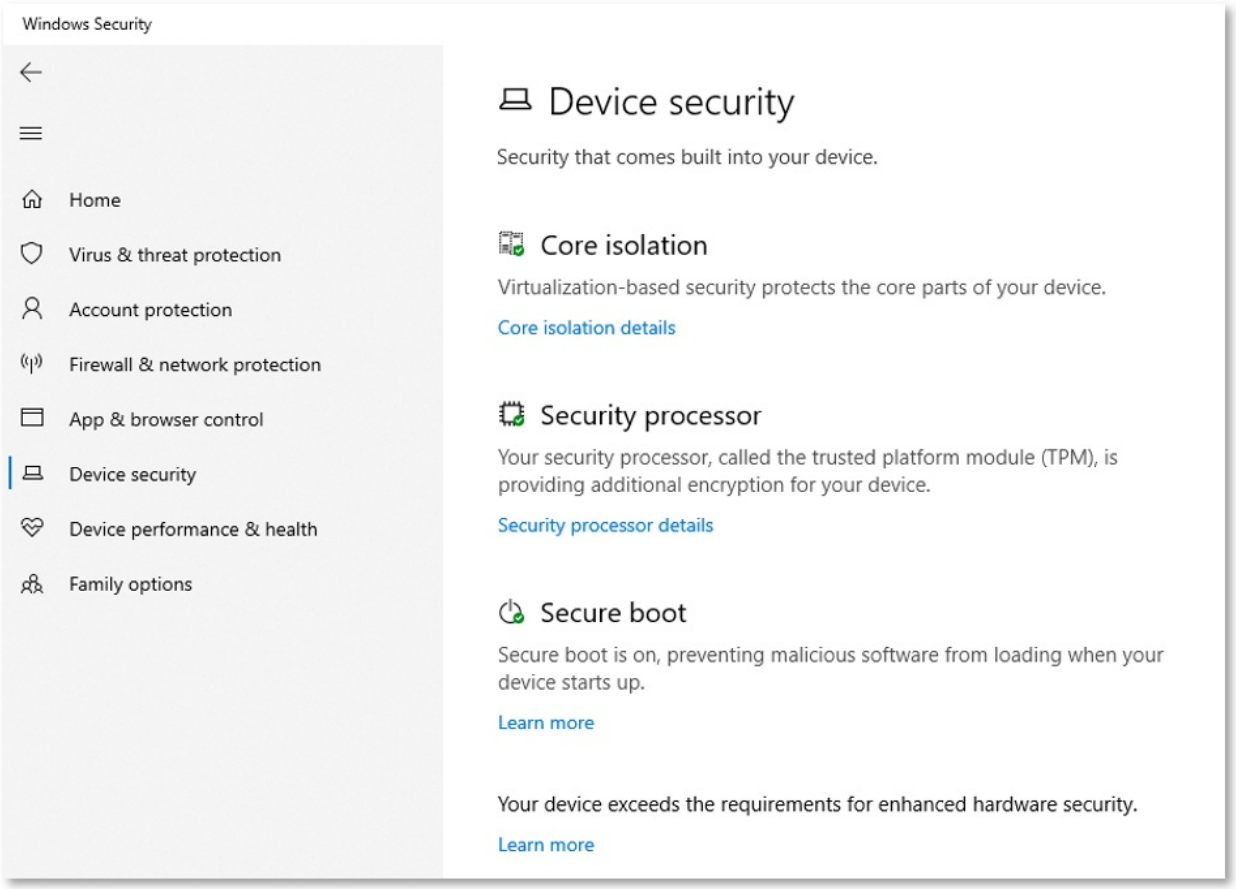
- WDAG allows dynamic navigation: Application Guard now allows users to navigate back to their default host browser from the WDAG Microsoft Edge. Previously, users browsing in WDAG Edge would see an error page when they try to go to a trusted site within the container browser. With this new feature, users will automatically be redirected to their host default browser when they enter or click on a trusted site in WDAG Edge. This feature is also available in Windows 10, version 1803 or later with the latest updates.

- Windows Defender Application Control (WDAC): In Windows 10, version 1903 WDAC has a number of new features that light up key scenarios and provide feature parity with AppLocker.
  - Multiple Policies: WDAC now supports multiple simultaneous code integrity policies for one device in order to enable the following scenarios: 1) enforce and audit side-by-side, 2) simpler targeting for policies with different scope/intent, 3) expanding a policy using a new 'supplemental' policy.
  - Path-Based Rules: The path condition identifies an app by its location in the file system of the computer or on the network instead of a signer or hash identifier. Additionally, WDAC has an option that allows admins to enforce at runtime that only code from paths that are not user-writeable is executed. When code tries to execute at runtime, the directory is scanned and files will be checked for write permissions for non-known admins. If a file is found to be user writeable, the executable is blocked from running unless it is authorized by something other than a path rule like a signer or hash rule.
    This brings WDAC to functionality parity with AppLocker in terms of support for file path rules. WDAC improves upon the security of policies based on file path rules with the availability of the user-writability permission checks at runtime time, which is a capability that is not available with AppLocker.
  - Allow COM Object Registration: Previously, WDAC enforced a built-in allow list for COM object registration. While this mechanism works for most common application usage scenarios, customers have provided feedback that there are cases where additional COM objects need to be allowed. The 1903 update to Windows 10 introduces the ability to specify allowed COM objects via their GUID in the WDAC policy.

System Guard

System Guard has added a new feature in this version of Windows called **SMM Firmware Measurement**. This feature is built on top of System Guard Secure Launch to check that the System Management Mode (SMM) firmware on the device is operating in a healthy manner - specifically, OS memory and secrets are protected from SMM. There are currently no devices out there with compatible hardware, but they will be coming out in the next few months.

This new feature is displayed under the Device Security page with the string "Your device exceeds the requirements for enhanced hardware security" if configured properly:



Identity Protection

- Windows Hello FIDO2 certification: Windows Hello is now a FIDO2 Certified authenticator and enables password-less login for websites supporting FIDO2 authentication, such as Microsoft account and Azure AD.
- Streamlined Windows Hello PIN reset experience: Microsoft account users have a revamped Windows Hello PIN reset experience with the same look and feel as signing in on the web.
- Sign-in with Password-less Microsoft accounts: Sign in to Windows 10 with a phone number account. Then use Windows Hello for an even easier sign-in experience!
- Remote Desktop with Biometrics: Azure Active Directory and Active Directory users using Windows Hello for Business can use biometrics to authenticate to a remote desktop session.

Security management

- Windows Defender Firewall now supports Windows Subsystem for Linux (WSL): Lets you add rules for WSL process, just like for Windows processes.
- Windows Security app improvements now include Protection history, including detailed and easier to understand information about threats and available actions, Controlled Folder Access blocks are now in the Protection history, Windows Defender Offline Scanning tool actions, and any pending recommendations.
- Tamper Protection lets you prevent others from tampering with important security features.

Microsoft Edge

Several new features are coming in the next version of Edge. See the news from Build 2019 for more information.

See Also

What's New in Windows Server, version 1903: New and updated features in Windows Server.
Windows 10 Features: Review general information about Windows 10 features.
What's New in Windows 10: See what's new in other versions of Windows 10.
What's new in Windows 10: See what's new in Windows 10 hardware.

What's new in Windows 10 for developers: New and updated features in Windows 10 that are of interest to developers.

What's new in Windows 10, version 1809 for IT Pros

5/31/2019 • 14 minutes to read • Edit Online

Applies To: Windows 10, version 1809

In this article we describe new and updated features of interest to IT Pros for Windows 10, version 1809. This update also contains all features and fixes included in previous cumulative updates to Windows 10, version 1803.

The following 3-minute video summarizes some of the new features that are available for IT Pros in this release.

Deployment

Windows Autopilot self-deploying mode

Windows Autopilot self-deploying mode enables a zero touch device provisioning experience. Simply power on the device, plug it into the Ethernet, and the device is fully configured automatically by Windows Autopilot.

This self-deploying capability removes the current need to have an end user interact by pressing the "Next" button during the deployment process.

You can utilize Windows Autopilot self-deploying mode to register the device to an AAD tenant, enroll in your organization's MDM provider, and provision policies and applications, all with no user authentication or user interaction required.

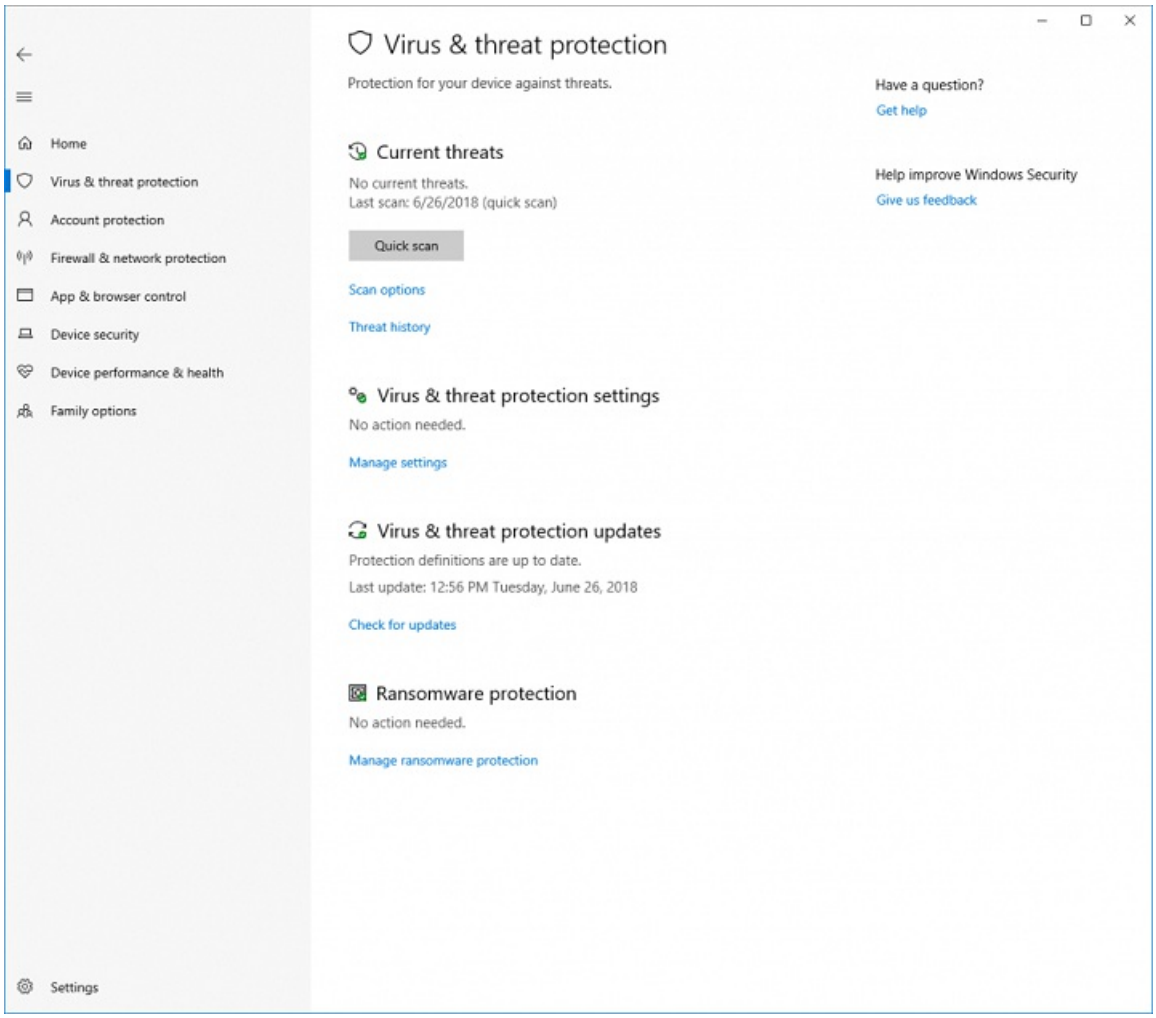
To learn more about Autopilot self-deploying mode and to see step-by-step instructions to perform such a deployment, Windows Autopilot self-deploying mode.

SetupDiag

SetupDiag version 1.4 is released. SetupDiag is a standalone diagnostic tool that can be used to troubleshoot issues when a Windows 10 upgrade is unsuccessful.

Security

We've continued to work on the **Current threats** area in Virus & threat protection, which now displays all threats that need action. You can quickly take action on threats from this screen:



With controlled folder access you can help prevent ransomware and other destructive malware from changing your personal files. In some cases, apps that you normally use might be blocked from making changes to common folders like **Documents** and **Pictures**. We've made it easier for you to add apps that were recently blocked so you can keep using your device without turning off the feature altogether.

When an app is blocked, it will appear in a recently blocked apps list, which you can get to by clicking **Manage settings** under the **Ransomware protection** heading. Click **Allow an app through Controlled folder access**. After the prompt, click the **+** button and choose **Recently blocked apps**. Select any of the apps to add them to the allowed list. You can also browse for an app from this page.

We added a new assessment for the Windows time service to the **Device performance & health** section. If we detect that your device's time is not properly synced with our time servers and the time-syncing service is disabled, we'll provide the option for you to turn it back on.

We're continuing to work on how other security apps you've installed show up in the **Windows Security** app. There's a new page called **Security providers** that you can find in the **Settings** section of the app. Click **Manage providers** to see a list of all the other security providers (including antivirus, firewall, and web protection) that are running on your device. Here you can easily open the providers' apps or get more information on how to resolve issues reported to you through **Windows Security**.

This also means you'll see more links to other security apps within **Windows Security**. For example, if you open the **Firewall & network protection** section, you'll see the firewall apps that are running on your device under each firewall type, which includes domain, private, and public networks).

BitLocker

Silent enforcement on fixed drives

Through a Modern Device Management (MDM) policy, BitLocker can be enabled silently for standard Azure Active Directory (AAD) joined users. In Windows 10, version 1803 automatic BitLocker encryption was enabled for

standard AAD users, but this still required modern hardware that passed the Hardware Security Test Interface (HSTI). This new functionality enables BitLocker via policy even on devices that don't pass the HSTI.

This is an update to the BitLocker CSP, which was introduced in Windows 10, version 1703, and leveraged by Intune and others.

This feature will soon be enabled on Olympia Corp as an optional feature.

Delivering BitLocker policy to AutoPilot devices during OOBE

You can choose which encryption algorithm to apply to BitLocker encryption capable devices, rather than automatically having those devices encrypt themselves with the default algorithm. This allows the encryption algorithm (and other BitLocker policies that must be applied prior to encryption), to be delivered before BitLocker encryption begins.

For example, you can choose the XTS-AES 256 encryption algorithm, and have it applied to devices that would normally encrypt themselves automatically with the default XTS-AES 128 algorithm during OOBE.

To achieve this:

1. Configure the encryption method settings in the Windows 10 Endpoint Protection profile to the desired encryption algorithm.
2. Assign the policy to your Autopilot device group.
   - **IMPORTANT**: The encryption policy must be assigned to **devices** in the group, not users.
3. Enable the Autopilot Enrollment Status Page (ESP) for these devices.
   - **IMPORTANT**: If the ESP is not enabled, the policy will not apply before encryption starts.

For more information, see Setting the BitLocker encryption algorithm for Autopilot devices.

Windows Defender Application Guard Improvements

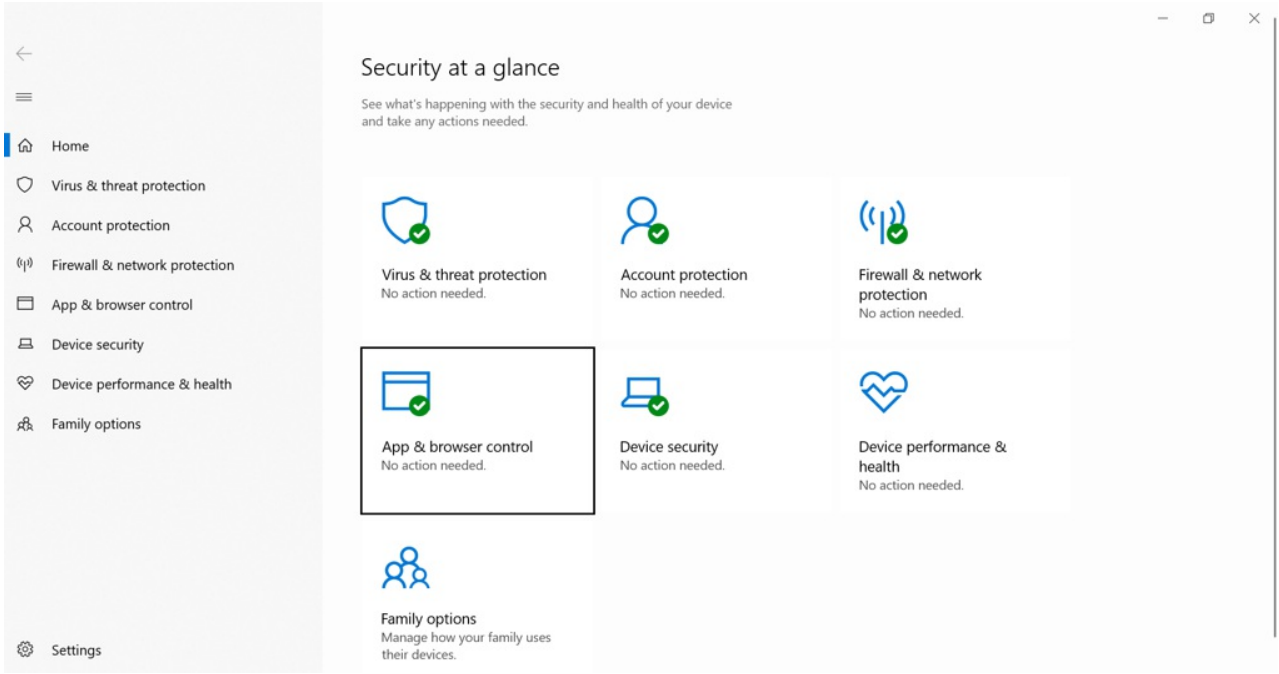
Windows Defender Application Guard (WDAG) introduced a new user interface inside **Windows Security** in this release. Standalone users can now install and configure their Windows Defender Application Guard settings in Windows Security without needing to change registry key settings.

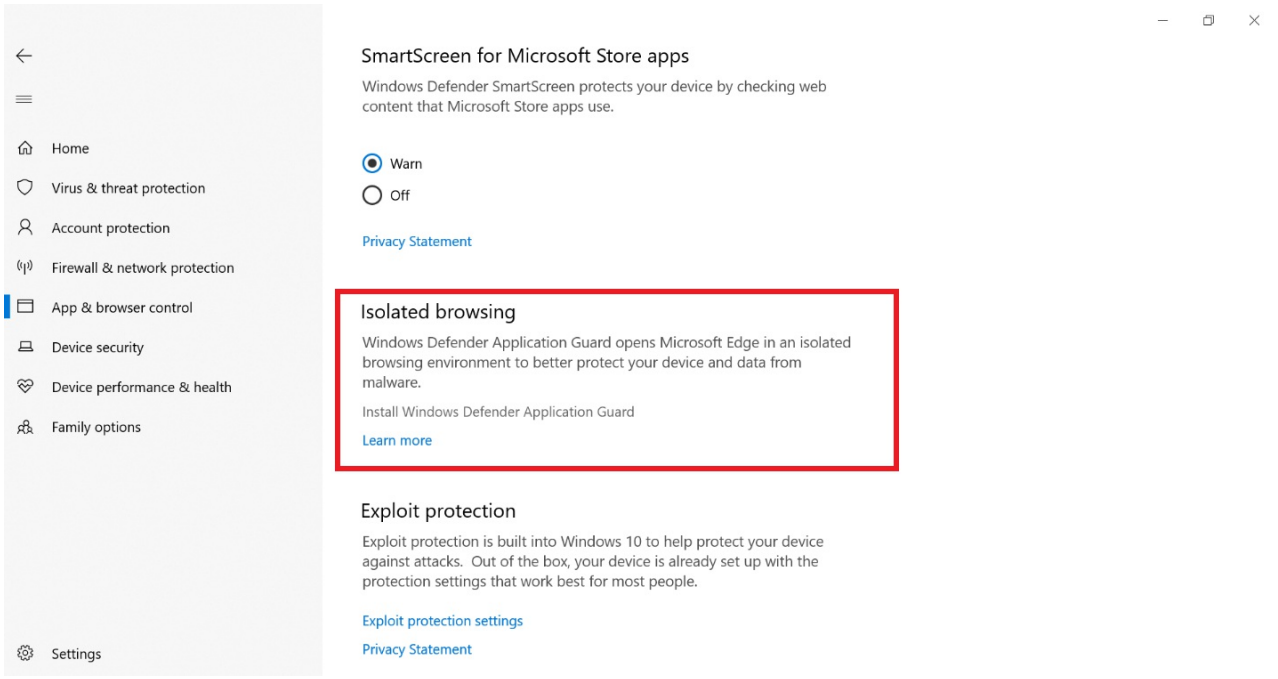
Additionally, users who are managed by enterprise policies will be able to check their settings to see what their administrators have configured for their machines to better understand the behavior of Windows Defender Application Guard. This new UI improves the overall experience for users while managing and checking their Windows Defender Application Guard settings. As long as devices meet the minimum requirements, these settings will appear in Windows Security. For more information, see Windows Defender Application Guard inside Windows Security App.

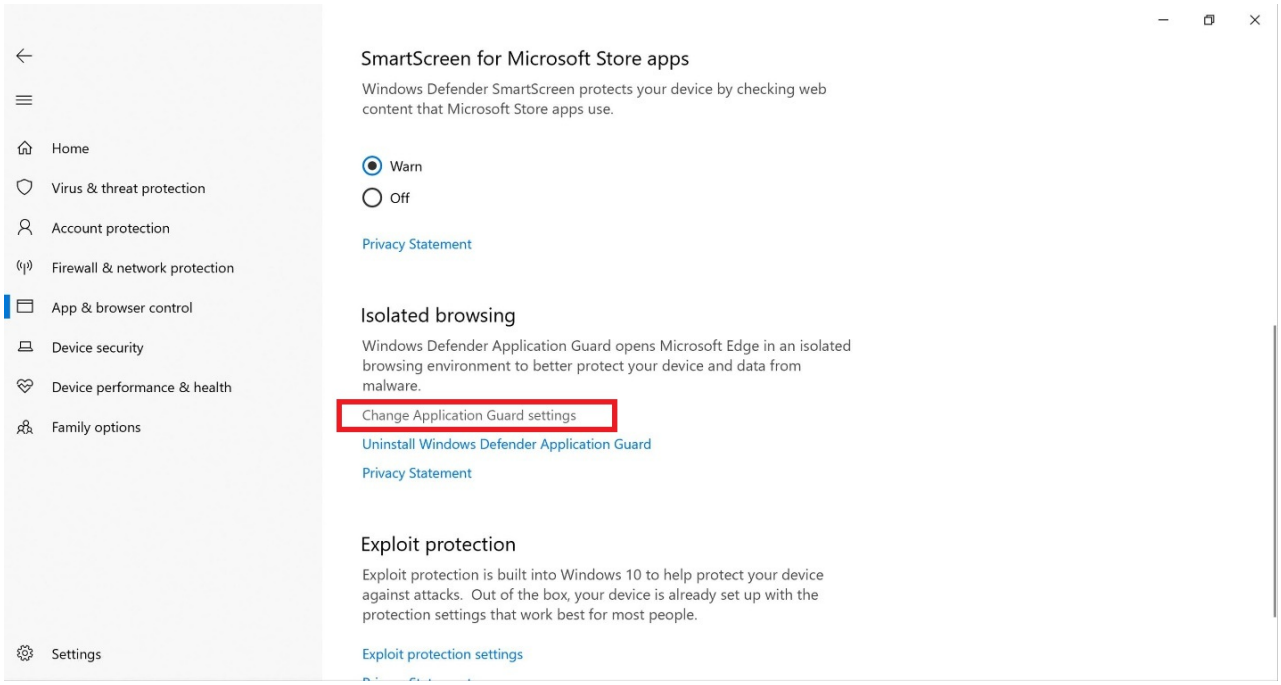
To try this:

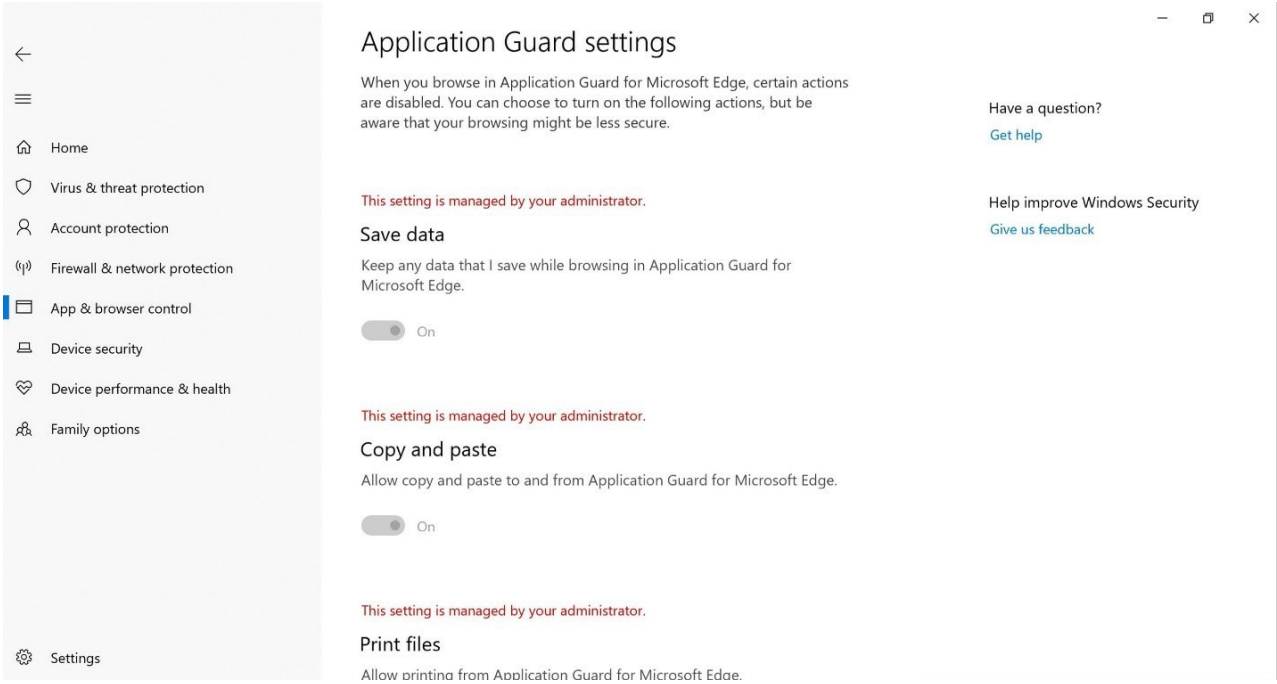
1. Go to**Windows Security** and select **App & browser control**.
2. Under **Isolated browsing**, select **Install Windows Defender Application Guard**, then install and restart the device.
3. Select **Change Application Guard** settings.
4. Configure or check Application Guard settings.

See the following example:


Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Virus & threat protection
No action needed.
Account protection
No action needed.
Firewall & network protection
No action needed.
App & browser control
No action needed.
Device security
No action needed.
Device performance & health
No action needed.
Family options
Manage how your family uses their devices.


SmartScreen for Microsoft Store apps
Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.
Warn
Off
Privacy Statement
Isolated browsing
Windows Defender Application Guard opens Microsoft Edge in an isolated browsing environment to better protect your device and data from malware.
Install Windows Defender Application Guard
Learn more
Exploit protection
Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.
Exploit protection settings
Privacy Statement
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings


SmartScreen for Microsoft Store apps
Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.
Warn
Off
Privacy Statement
Isolated browsing
Windows Defender Application Guard opens Microsoft Edge in an isolated browsing environment to better protect your device and data from malware.
Change Application Guard settings
Uninstall Windows Defender Application Guard
Privacy Statement
Exploit protection
Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.
Exploit protection settings
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings



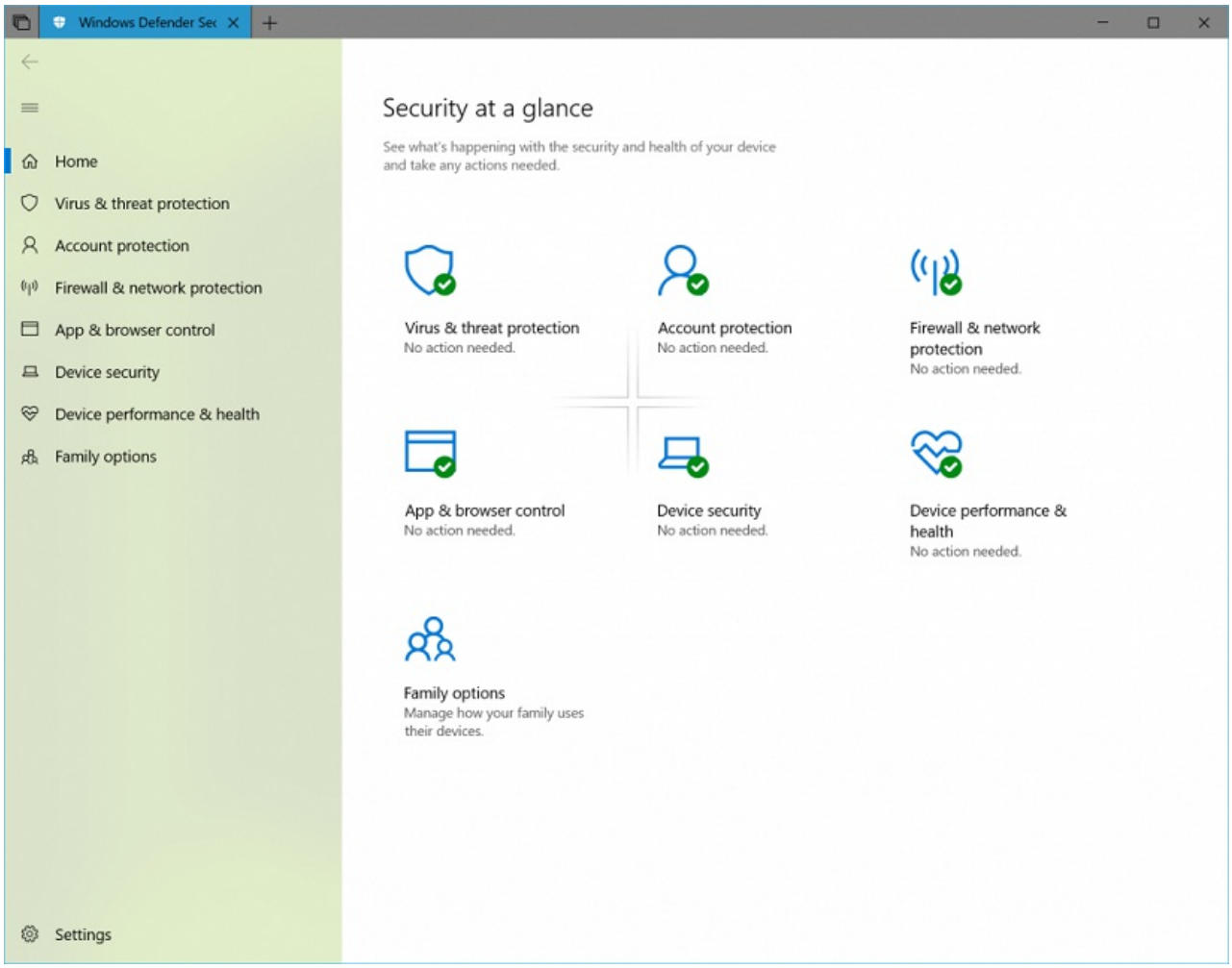
Windows Security Center

Windows Defender Security Center is now called **Windows Security Center**.

You can still get to the app in all the usual ways – simply ask Cortana to open Windows Security Center(WSC) or interact with the taskbar icon. WSC lets you manage all your security needs, including **Windows Defender Antivirus** and **Windows Defender Firewall**.

The WSC service now requires antivirus products to run as a protected process to register.Products that have not yet implemented this will not appear in the Windows Security Center user interface, and Windows Defender Antivirus will remain enabled side-by-side with these products.

WSC now includes the Fluent Design System elements you know and love. You'll also notice we've adjusted the spacing and padding around the app. It will now dynamically size the categories on the main page if more room is needed for extra info. We also updated the title bar so that it will use your accent color if you have enabled that option in **Color Settings**.



Windows Defender Firewall now supports Windows Subsystem for Linux (WSL) processes

You can add specific rules for a WSL process in Windows Defender Firewall, just as you would for any Windows process. Also, Windows Defender Firewall now supports notifications for WSL processes. For example, when a Linux tool wants to allow access to a port from the outside (like SSH or a web server like nginx), Windows Defender Firewall will prompt to allow access just like it would for a Windows process when the port starts accepting connections. This was first introduced in Build 17627.

Microsoft Edge Group Policies

We introduced new group policies and Modern Device Management settings to manage Microsoft Edge. The new policies include enabling and disabling full-screen mode, printing, favorites bar, and saving history; preventing certificate error overrides; configuring the Home button and startup options; setting the New Tab page and Home button URL, and managing extensions. Learn more about the new Microsoft Edge policies.

Windows Defender Credential Guard is supported by default on 10S devices that are AAD Joined

Windows Defender Credential Guard is a security service in Windows 10 built to protect Active Directory (AD) domain credentials so that they can't be stolen or misused by malware on a user's machine. It is designed to protect against well-known threats such as Pass-the-Hash and credential harvesting.

Windows Defender Credential Guard has always been an optional feature, but Windows 10-S turns this functionality on by default when the machine has been Azure Active Directory joined. This provides an added level of security when connecting to domain resources not normally present on 10-S devices. Please note that Windows Defender Credential Guard is available only to S-Mode devices or Enterprise and Education Editions.

Windows 10 Pro S Mode requires a network connection

A network connection is now required to set up a new device. As a result, we removed the “skip for now” option in the network setup page in Out Of Box Experience (OOBE).

Windows Defender ATP

Windows Defender ATP has been enhanced with many new capabilities. For more information, see the following topics:

- Threat analytics
  Threat Analytics is a set of interactive reports published by the Windows Defender ATP research team as soon as emerging threats and outbreaks are identified. The reports help security operations teams assess impact on their environment and provides recommended actions to contain, increase organizational resilience, and prevent specific threats.

- Custom detection
  With custom detections, you can create custom queries to monitor events for any kind of behavior such as suspicious or emerging threats. This can be done by leveraging the power of Advanced hunting through the creation of custom detection rules.

- Managed security service provider (MSSP) support
  Windows Defender ATP adds support for this scenario by providing MSSP integration. The integration will allow MSSPs to take the following actions: Get access to MSSP customer's Windows Defender Security Center portal, fetch email notifications, and fetch alerts through security information and event management (SIEM) tools.

- Integration with Azure Security Center
  Windows Defender ATP integrates with Azure Security Center to provide a comprehensive server protection solution. With this integration Azure Security Center can leverage the power of Windows Defender ATP to provide improved threat detection for Windows Servers.

- Integration with Microsoft Cloud App Security
  Microsoft Cloud App Security leverages Windows Defender ATP endpoint signals to allow direct visibility into cloud application usage including the use of unsupported cloud services (shadow IT) from all Windows Defender ATP monitored machines.

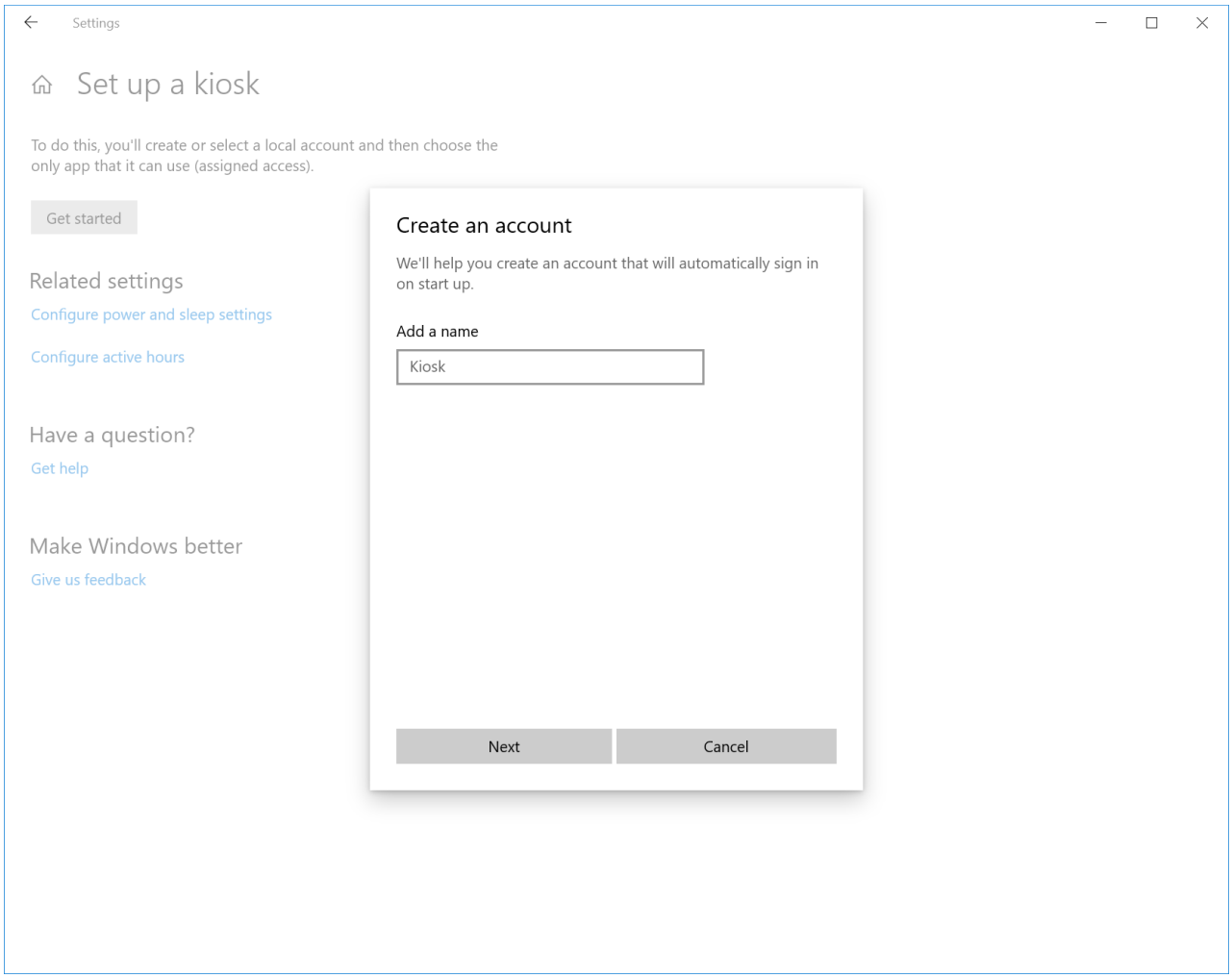
- Onboard Windows Server 2019
  Windows Defender ATP now adds support for Windows Server 2019. You'll be able to onboard Windows Server 2019 in the same method available for Windows 10 client machines.

- Onboard previous versions of Windows
  Onboard supported versions of Windows machines so that they can send sensor data to the Windows Defender ATP sensor

Kiosk setup experience

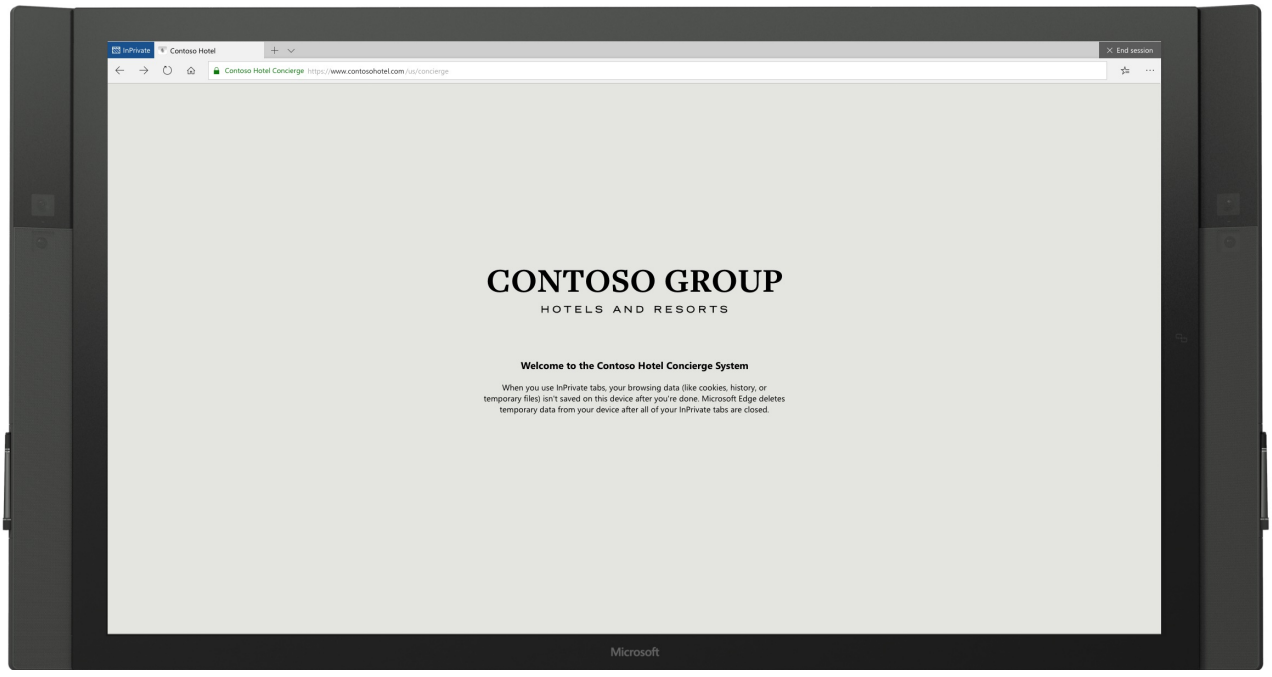
We introduced a simplified assigned access configuration experience in **Settings** that allows device administrators to easily set up a PC as a kiosk or digital sign. A wizard experience walks you through kiosk setup including creating a kiosk account that will automatically sign in when a device starts.

To use this feature, go to **Settings**, search for **assigned access**, and open the **Set up a kiosk** page.



Microsoft Edge kiosk mode running in single-app assigned access has two kiosk types.

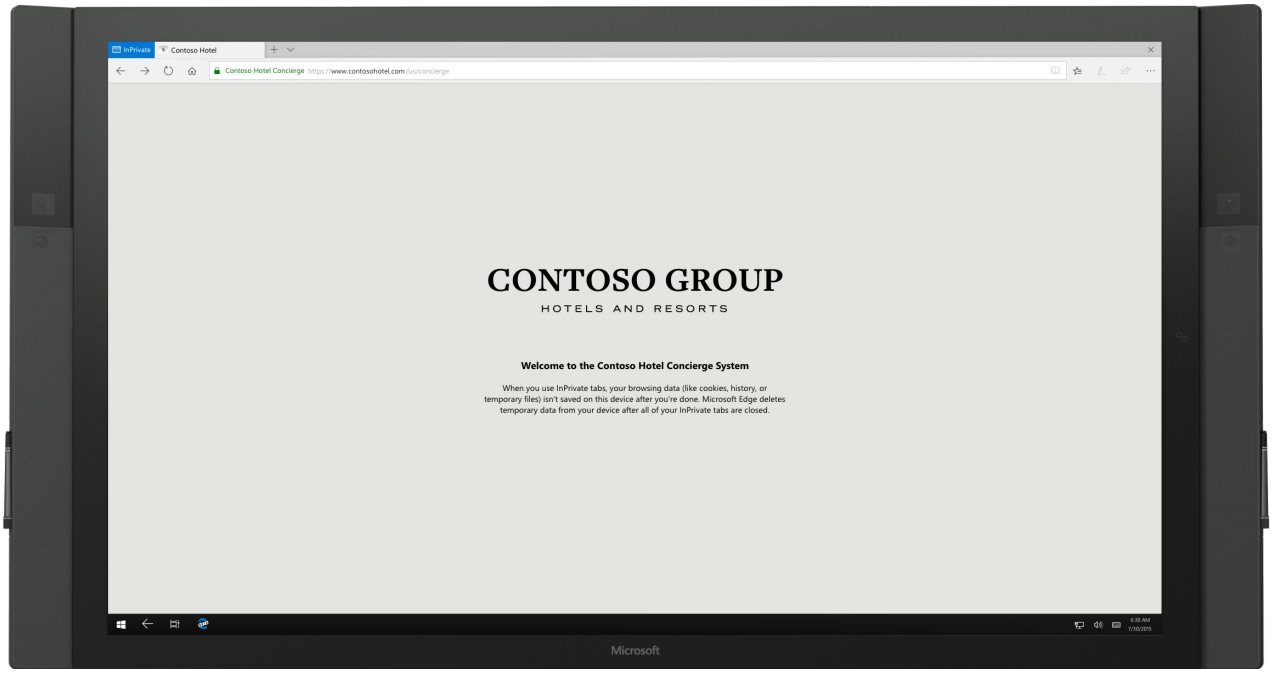
1. **Digital / Interactive signage** that displays a specific website full-screen and runs InPrivate mode.
2. **Public browsing** supports multi-tab browsing and runs InPrivate mode with minimal features available. Users cannot minimize, close, or open new Microsoft Edge windows or customize them using Microsoft Edge Settings. Users can clear browsing data and downloads, and restart Microsoft Edge by clicking **End session**. Administrators can configure Microsoft Edge to restart after a period of inactivity.



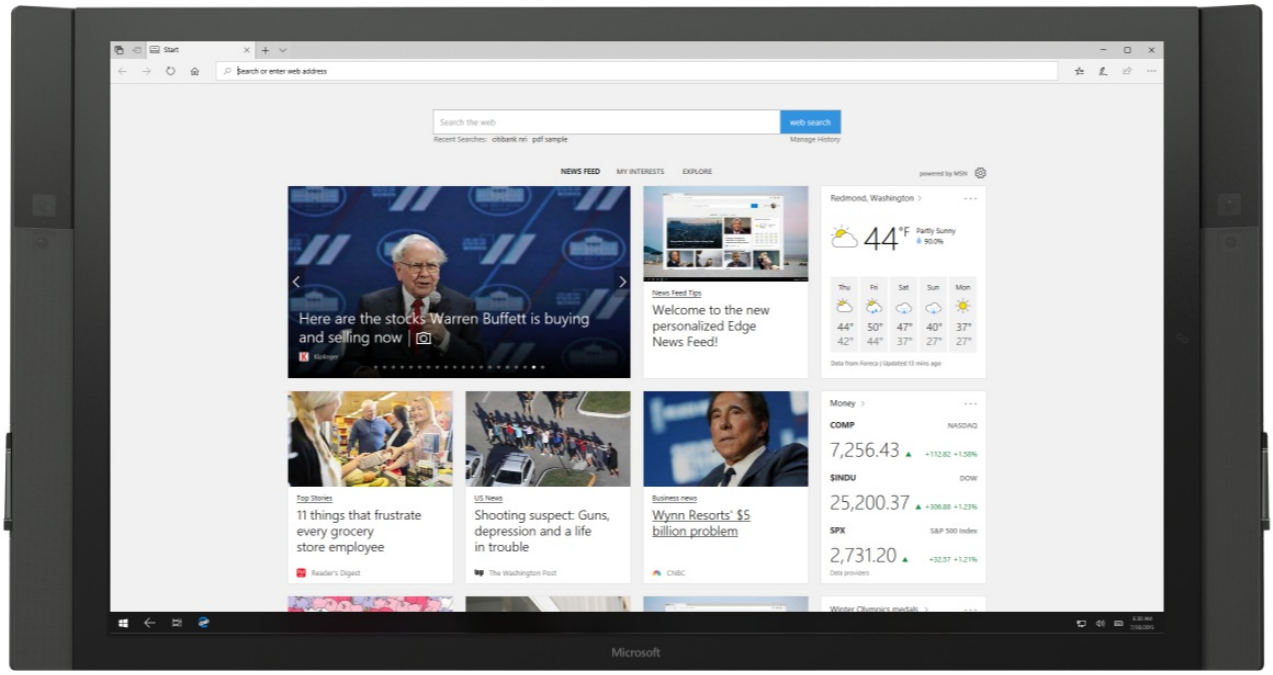
Microsoft Edge kiosk mode running in multi-app assigned access has two kiosk types.

> **NOTE**
>
> The following Microsoft Edge kiosk mode types cannot be set up using the new simplified assigned access configuration wizard in Windows 10 Settings.

Public browsing supports multi-tab browsing and runs InPrivate mode with minimal features available. In this configuration, Microsoft Edge can be one of many apps available. Users can close and open multiple InPrivate mode windows.



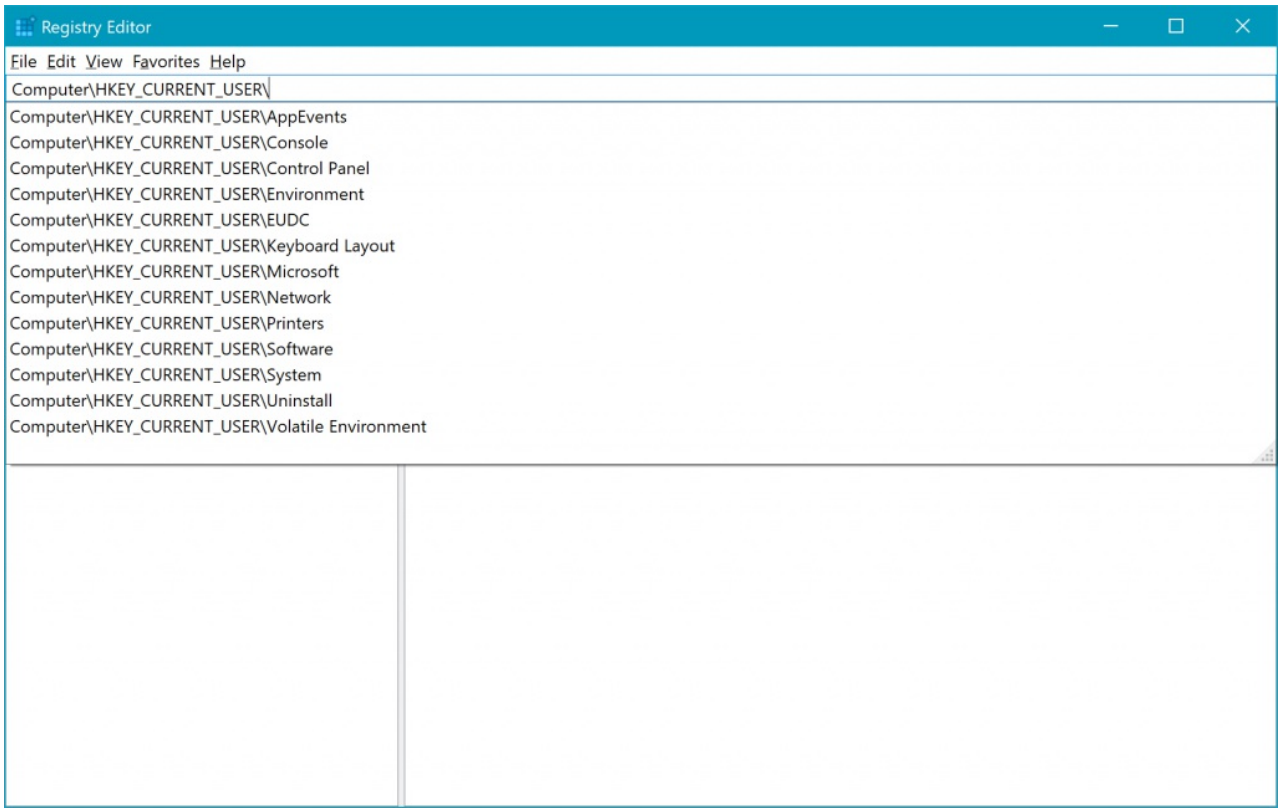
Normal mode runs a full version of Microsoft Edge, although some features may not work depending on what apps are configured in assigned access. For example, if the Microsoft Store is not set up, users cannot get books.



Learn more about Microsoft Edge kiosk mode.

Registry editor improvements

We added a dropdown that displays as you type to help complete the next part of the path. You can also press **Ctrl + Backspace** to delete the last word, and **Ctrl + Delete** to delete the next word.

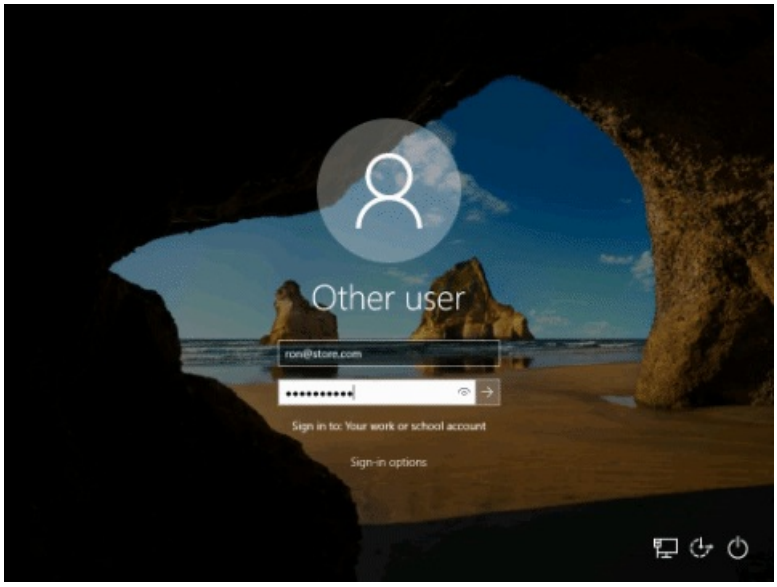


Faster sign-in to a Windows 10 shared pc

Do you have shared devices deployed in your work place? **Fast sign-in** enables users to sign in to a shared Windows 10 PC in a flash!

To enable fast sign-in:

1. Set up a shared or guest device with Windows 10, version 1809.
2. Set the Policy CSP, and the Authentication and EnableFastFirstSignIn policies to enable fast sign-in.
3. Sign-in to a shared PC with your account. You'll notice the difference!



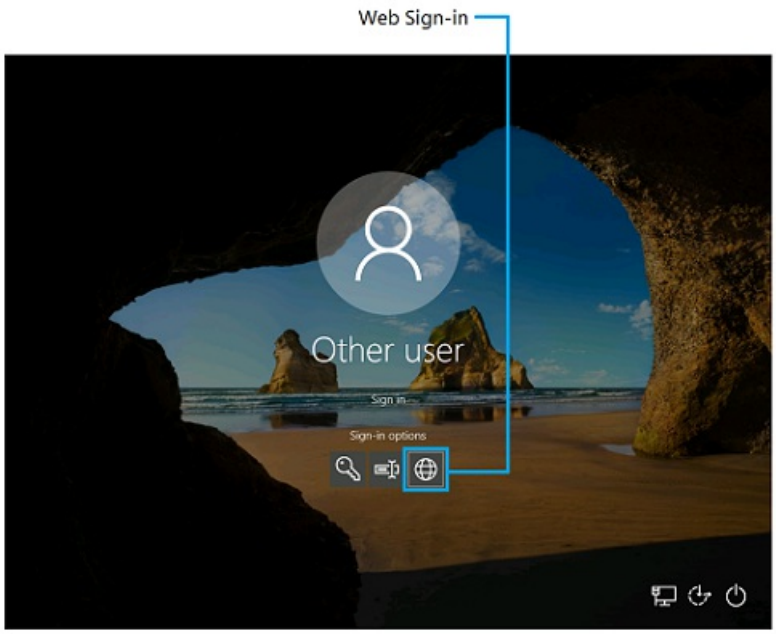
> **NOTE**
>
> This is a preview feature and therefore not meant or recommended for production purposes.

Web sign-in to Windows 10

Until now, Windows logon only supported the use of identities federated to ADFS or other providers that support the WS-Fed protocol. We are introducing "web sign-in," a new way of signing into your Windows PC. Web Sign-in enables Windows logon support for non-ADFS federated providers (e.g.SAML).

To try out web sign-in:

1. Azure AD Join your Windows 10 PC. (Web sign-in is only supported on Azure AD Joined PCs).
2. Set the Policy CSP, and the Authentication and EnableWebSignIn polices to enable web sign-in.
3. On the lock screen, select web sign-in under sign-in options.
4. Click the "Sign in" button to continue.

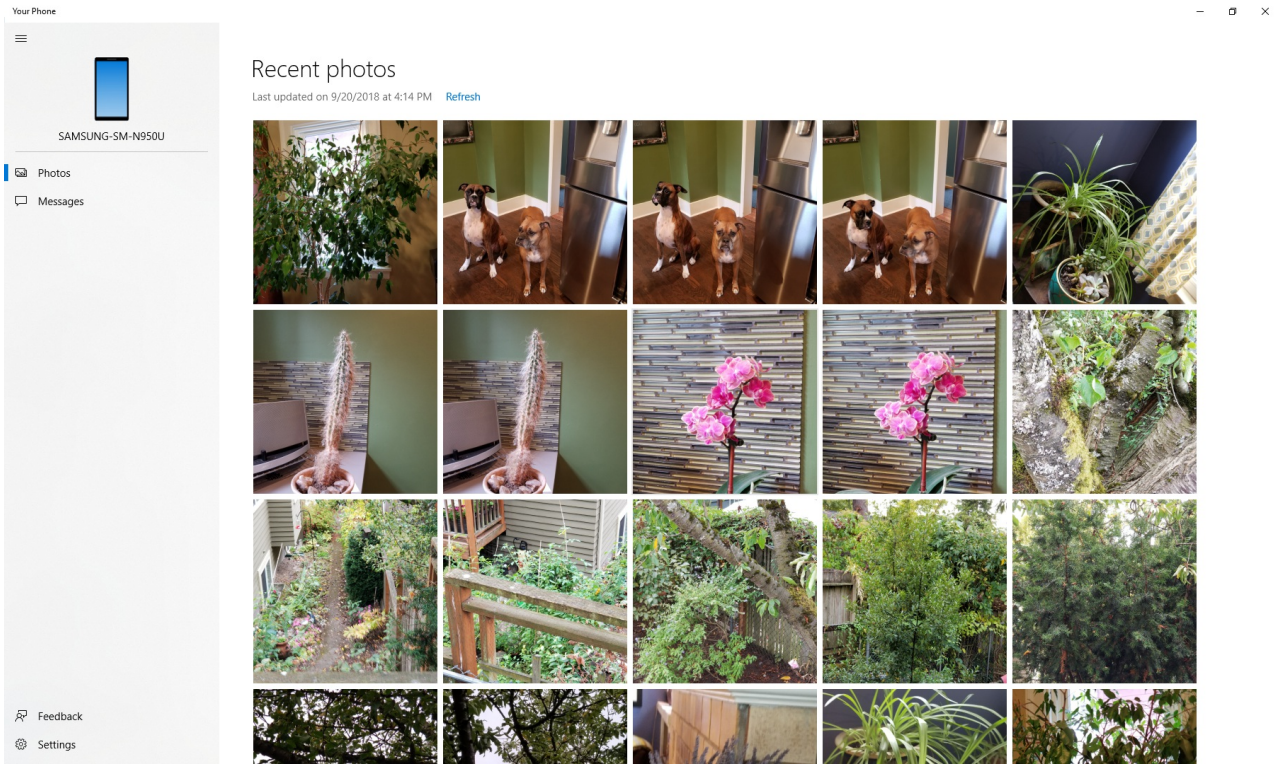


> **NOTE**
> This is a preview feature and therefore not meant or recommended for production purposes.

Your Phone app

Android phone users, you can finally stop emailing yourself photos. With Your Phone you get instant access to your Android's most recent photos on your PC. Drag and drop a photo from your phone onto your PC, then you can copy, edit, or ink on the photo. Try it out by opening the **Your Phone** app. You'll receive a text with a link to download an app from Microsoft to your phone. Android 7.0+ devices with ethernet or Wi-Fi on unmetered networks are compatible with the **Your Phone** app. For PCs tied to the China region, **Your Phone** app services will be enabled in the future.

For iPhone users, **Your Phone** app also helps you to link your phone to your PC. Surf the web on your phone, then send the webpage instantly to your computer to continue what you're doing—read, watch, or browse-- with all the benefits of a bigger screen.

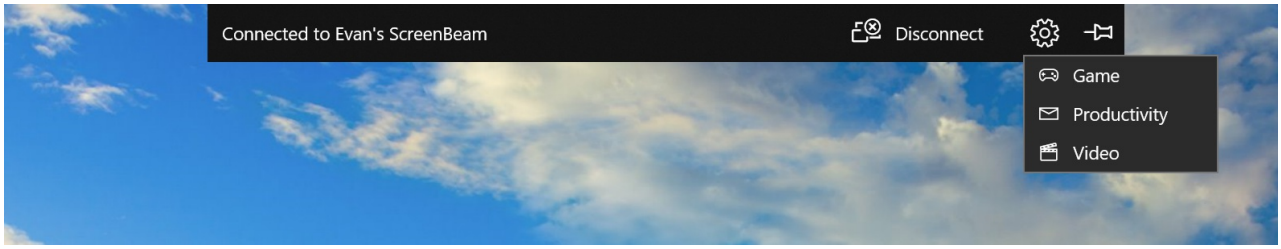


The desktop pin takes you directly to the **Your Phone** app for quicker access to your phone's content. You can also go through the all apps list in Start, or use the Windows key and search for **Your Phone**.

Wireless projection experience

One of the things we've heard from you is that it's hard to know when you're wirelessly projecting and how to disconnect your session when started from file explorer or from an app. In Windows 10, version 1809, you'll see a control banner at the top of your screen when you're in a session (just like you see when using remote desktop). The banner keeps you informed of the state of your connection, allows you to quickly disconnect or reconnect to the same sink, and allows you to tune the connection based on what you are doing. This tuning is done via **Settings**, which optimizes the screen-to-screen latency based on one of the three modes:

- Game mode minimizes the screen-to-screen latency to make gaming over a wireless connection possible
- Video mode increases the screen-to-screen latency to ensure the video on the big screen plays back smoothly
- Productivity modes strikes a balance between game mode and video mode; the screen-to screen-latency is responsive enough that typing feels natural, while ensuring videos don't glitch as often.



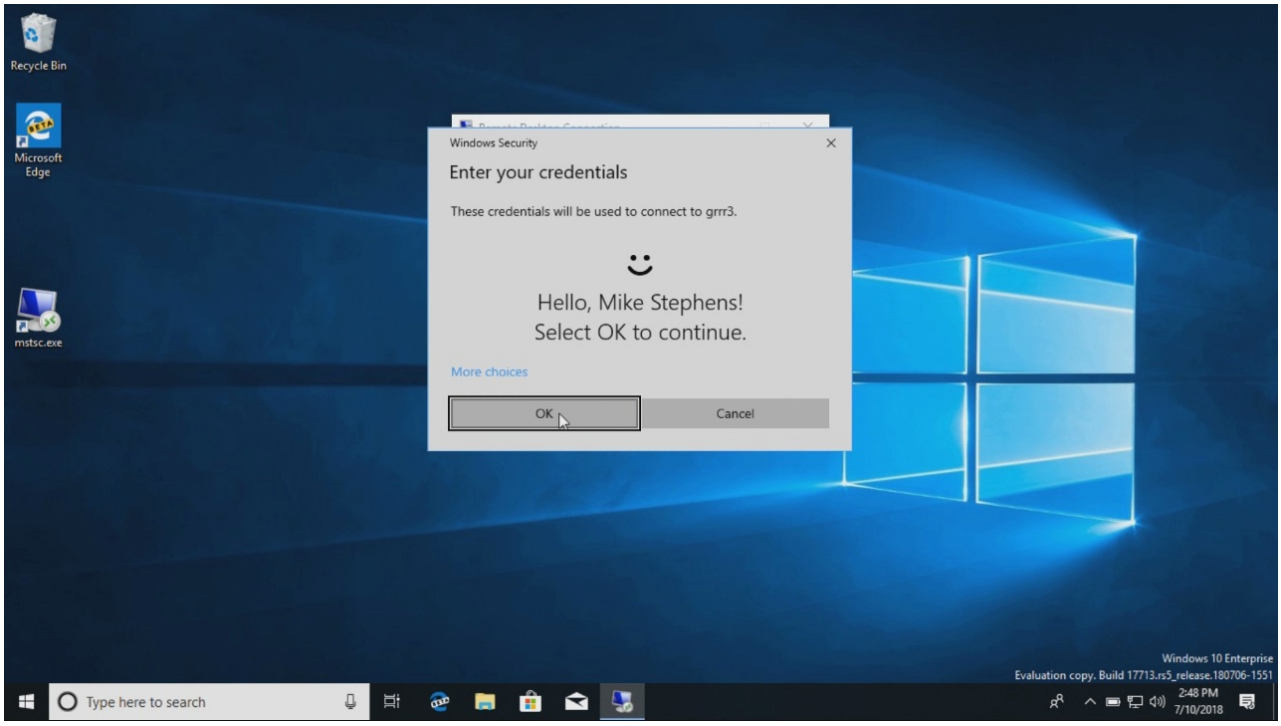
Remote Desktop with Biometrics

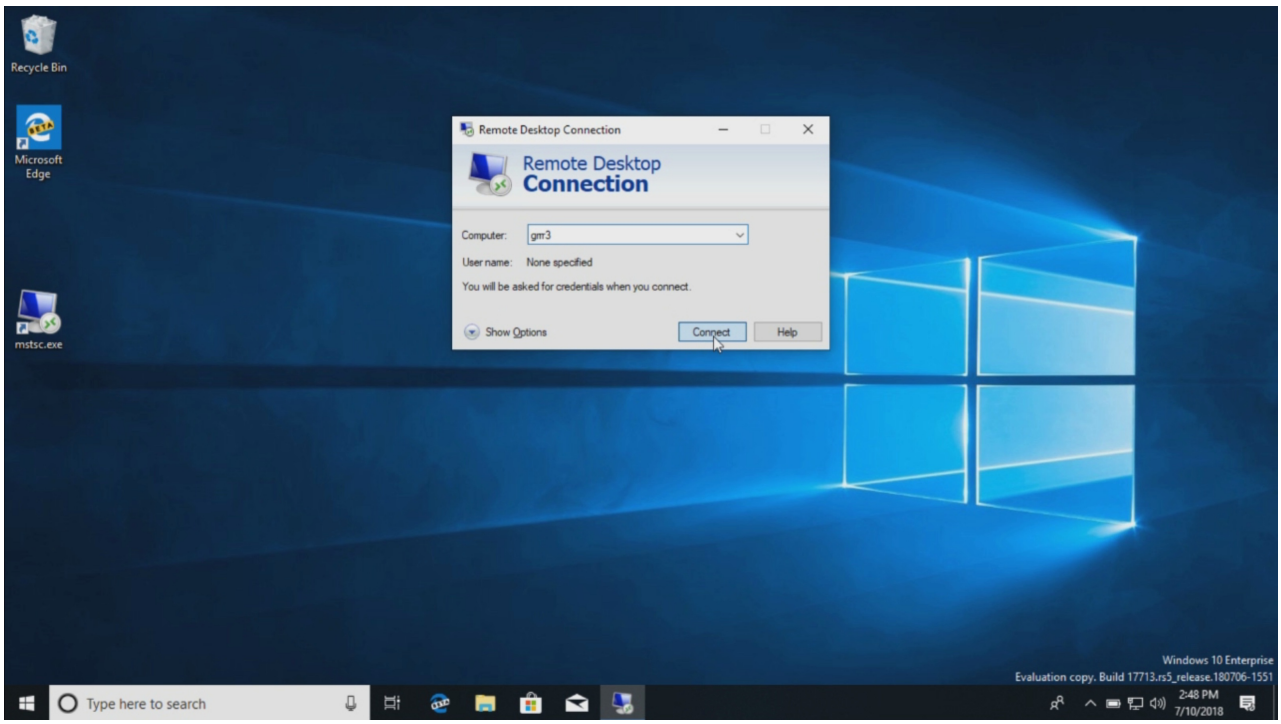
Azure Active Directory and Active Directory users using Windows Hello for Business can use biometrics to authenticate to a remote desktop session.

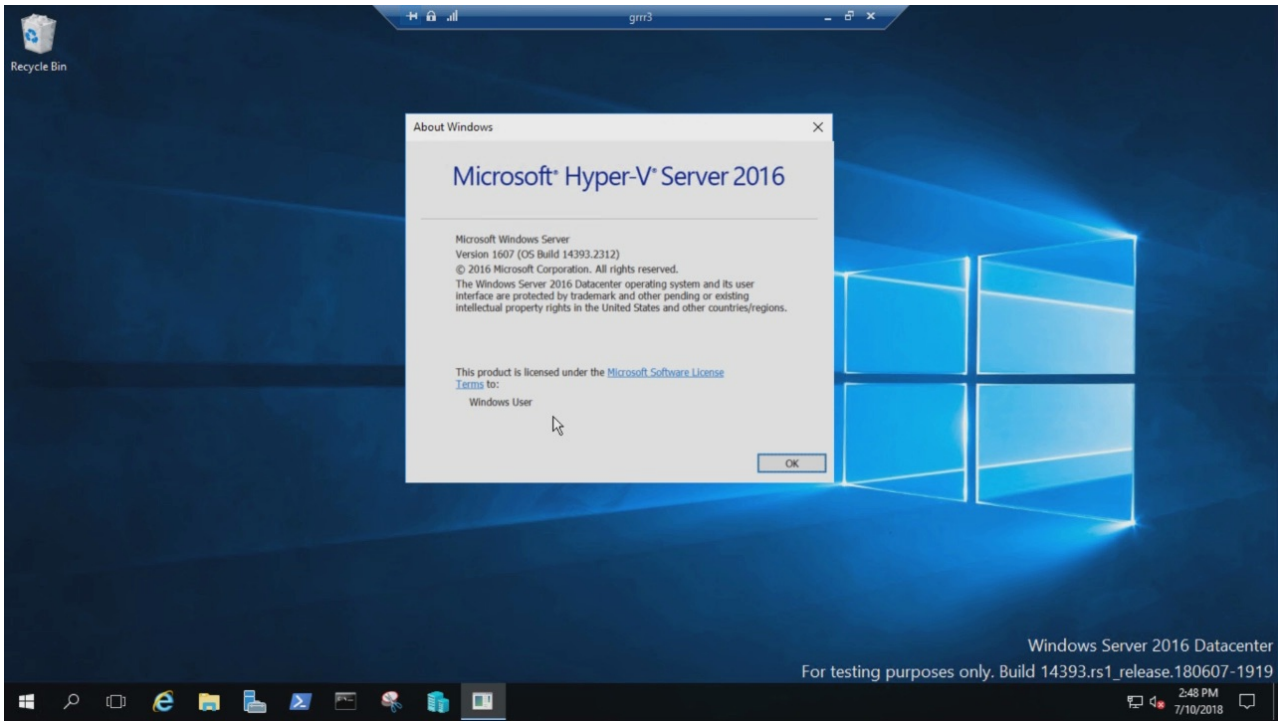
To get started, sign into your device using Windows Hello for Business. Bring up **Remote Desktop Connection** (mstsc.exe), type the name of the computer you want to connect to, and click **Connect**. Windows remembers that you signed using Windows Hello for Business, and automatically selects Windows Hello for Business to authenticate you to your RDP session. You can also click **More choices** to choose alternate credentials. Windows

uses facial recognition to authenticate the RDP session to the Windows Server 2016 Hyper-V server. You can continue to use Windows Hello for Business in the remote session, but you must use your PIN.

See the following example:






grrr3
Recycle Bin
About Windows
Microsoft® Hyper-V® Server 2016
Microsoft Windows Server
Version 1607 (OS Build 14393.2312)
© 2016 Microsoft Corporation. All rights reserved.
The Windows Server 2016 Datacenter operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.
This product is licensed under the Microsoft Software License Terms to:
Windows User
OK
Windows Server 2016 Datacenter
For testing purposes only. Build 14393.rs1_release.180607-1919
2:48 PM
7/10/2018

What's new in Windows 10, version 1803 IT Pro content

5/31/2019 • 10 minutes to read • Edit Online

Applies to

- Windows 10, version 1803

This article lists new and updated features and content that are of interest to IT Pros for Windows 10 version 1803, also known as the Windows 10 April 2018 Update. This update also contains all features and fixes included in previous cumulative updates to Windows 10, version 1709.

> If you are not an IT Pro, see the following topics for information about what's new in Windows 10, version 1803 in hardware, for developers, and for consumers.

The following 3-minute video summarizes some of the new features that are available for IT Pros in this release.

Deployment

Windows Autopilot

Windows Autopilot provides a modern device lifecycle management service powered by the cloud that delivers a zero touch experience for deploying Windows 10.

Using Intune, Autopilot now enables locking the device during provisioning during the Windows Out Of Box Experience (OOBE) until policies and settings for the device get provisioned, thereby ensuring that by the time the user gets to the desktop, the device is secured and configured correctly.

Windows Autopilot is now available with Surface, Lenovo, and Dell. Other OEM partners such as HP, Toshiba, Panasonic, and Fujitsu will support Autopilot in coming months. Check back here later for more information.

Windows 10 in S mode

Windows 10 in S mode is now available on both Windows 10 Home and Pro PCs, and commercial customers will be able to deploy Windows 10 Enterprise in S mode - by starting with Windows 10 Pro in S mode and then activating Windows 10 Enterprise on the computer.

Some additional information about Windows 10 in S mode:

- Microsoft-verified. All of your applications are verified by Microsoft for security and performance.
- Performance that lasts. Start-ups are quick, and S mode is built to keep them that way.
- Choice and flexibility. Save your files to your favorite cloud, like OneDrive or DropBox, and access them from any device you choose. Browse the Microsoft Store for thousands of apps.
- S mode, on a range of modern devices. Enjoy all the great Windows multi-tasking features, like snapping Windows, task view and virtual desktops on a range of S mode enabled devices.

If you want to switch out of S mode, you will be able to do so at no charge, regardless of edition. Once you switch out of S mode, you cannot switch back.

For more information, see Windows 10 Pro/Enterprise in S mode.

Windows 10 kiosk and Kiosk Browser

With this release you can easily deploy and manage kiosk devices with Microsoft Intune in single and multiple app scenarios. This includes the new Kiosk Browser available from the Microsoft Store. Kiosk Browser is great for delivering a reliable and custom-tailored browsing experience for scenarios such as retail and signage. A summary of new features is below.

- Using Intune, you can deploy the Kiosk Browser from the Microsoft Store, configure start URL, allowed URLs, and enable/disable navigation buttons.
- Using Intune, you can deploy and configure shared devices and kiosks using assigned access to create a curated experience with the correct apps and configuration policies
- Support for multiple screens for digital signage use cases.
- The ability to ensure all MDM configurations are enforced on the device prior to entering assigned access using the Enrollment Status page.
- The ability to configure and run Shell Launcher in addition to existing UWP Store apps.
- A simplified process for creating and configuring an auto-logon kiosk account so that a public kiosk automatically enters a desired state after a reboot, a critical security requirement for public-facing use cases.
- For multi-user Firstline Worker kiosk devices, instead of specifying every user, it's now possible to assign different assigned access configurations to Azure AD groups or Active Directory groups.
- To help with troubleshooting, you can now view error reports generated if an assigned access-configured app has issues.

For more information, see:

- Making IT simpler with a modern workplace
- Simplifying kiosk management for IT with Windows 10

Windows 10 Subscription Activation

With this release, Subscription Activation supports Inherited Activation. Inherited Activation allows Windows 10 virtual machines to inherit activation state from their Windows 10 host.

For more information, see Windows 10 Subscription Activation.

DISM

The following new DISM commands have been added to manage feature updates:

```
DISM /Online /Initiate-OSUninstall
    - Initiates a OS uninstall to take the computer back to the previous installation of windows.
DISM /Online /Remove-OSUninstall
    - Removes the OS uninstall capability from the computer.
DISM /Online /Get-OSUninstallWindow
    - Displays the number of days after upgrade during which uninstall can be performed.
DISM /Online /Set-OSUninstallWindow
    - Sets the number of days after upgrade during which uninstall can be performed.
```

For more information, see DISM operating system uninstall command-line options.

Windows Setup

You can now run your own custom actions or scripts in parallel with Windows Setup. Setup will also migrate your scripts to next feature release, so you only need to add them once.

Prerequisites:

- Windows 10, version 1803 or later.
- Windows 10 Enterprise or Pro

For more information, see Run custom actions during feature update.

It is also now possible to run a script if the user rolls back their version of Windows using the PostRollback option.

```
/PostRollback<location> [\setuprollback.cmd] [/postrollback {system / admin}]
```

For more information, see Windows Setup Command-Line Options

New command-line switches are also available to control BitLocker:

```
Setup.exe /BitLocker AlwaysSuspend
    - Always suspend bitlocker during upgrade.
Setup.exe /BitLocker TryKeepActive
    - Enable upgrade without suspending bitlocker but if upgrade, does not work then suspend bitlocker and
complete the upgrade.
Setup.exe /BitLocker ForceKeepActive
    - Enable upgrade without suspending bitlocker, but if upgrade does not work, fail the upgrade.
```

For more information, see Windows Setup Command-Line Options

SetupDiag

SetupDiag is a new command-line tool that can help diagnose why a Windows 10 update failed.

SetupDiag works by searching Windows Setup log files. When searching log files, SetupDiag uses a set of rules to match known issues. In the current version of SetupDiag there are 26 rules contained in the rules.xml file, which is extracted when SetupDiag is run. The rules.xml file will be updated as new versions of SetupDiag are made available.

Windows Update for Business (WUfB)

Windows Update for Business now provides greater control over updates, with the ability to pause and uninstall problematic updates using Intune. For more information, see Manage software updates in Intune.

Feature update improvements

Portions of the work done during the offline phases of a Windows update have been moved to the online phase. This has resulted in a significant reduction of offline time when installing updates. For more information, see We're listening to you.

Configuration

Co-management

Intune and **System Center Configuration Manager** policies have been added to enable hybrid Azure AD-joined authentication. Mobile Device Management (MDM) has added over 150 new policies and settings in this release, including the MDMWinsOverGP policy, to enable easier transition to cloud-based management.

For more information, see What's New in MDM enrollment and management

OS uninstall period

The OS uninstall period is a length of time that users are given when they can optionally roll back a Windows 10 update. With this release, administrators can use Intune or DISM to customize the length of the OS uninstall period.

Windows Hello for Business

Windows Hello now supports FIDO 2.0 authentication for Azure AD Joined Windows 10 devices and has enhanced support for shared devices, as described in the Kiosk configuration section.

- Windows Hello is now password-less on S-mode.
- Support for S/MIME with Windows Hello for Business and APIs for non-Microsoft identity lifecycle

management solutions.

- Windows Hello is part of the account protection pillar in Windows Defender Security Center. Account Protection will encourage password users to set up Windows Hello Face, Fingerprint or PIN for faster sign in, and will notify Dynamic lock users if Dynamic lock has stopped working because their phone or device Bluetooth is off.
- You can set up Windows Hello from lock screen for MSA accounts. We've made it easier for Microsoft account users to set up Windows Hello on their devices for faster and more secure sign-in. Previously, you had to navigate deep into Settings to find Windows Hello. Now, you can set up Windows Hello Face, Fingerprint or PIN straight from your lock screen by clicking the Windows Hello tile under Sign-in options.
- New public API for secondary account SSO for a particular identity provider.
- It is easier to set up Dynamic lock, and WD SC actionable alerts have been added when Dynamic lock stops working (ex: phone Bluetooth is off).

For more information, see: Windows Hello and FIDO2 Security Keys enable secure and easy authentication for shared devices

Accessibility and Privacy

Accessibility

"Out of box" accessibility is enhanced with auto-generated picture descriptions. For more information about accessibility, see Accessibility information for IT Professionals. Also see the accessibility section in the What's new in the Windows 10 April 2018 Update blog post.

Privacy

In the Feedback and Settings page under Privacy Settings you can now delete the diagnostic data your device has sent to Microsoft. You can also view this diagnostic data using the Diagnostic Data Viewer app.

Security

Security Baselines

The new security baseline for Windows 10 version 1803 has been published.

Windows Defender Antivirus

Windows Defender Antivirus now shares detection status between M365 services and interoperates with Windows Defender ATP. Additional policies have also been implemented to enhance cloud based protection, and new channels are available for emergency protection. For more information, see Virus and threat protection and Use next-gen technologies in Windows Defender Antivirus through cloud-delivered protection.

Windows Defender Exploit Guard

Windows Defender Exploit Guard enhanced attack surface area reduction, extended support to Microsoft Office applications, and now supports Windows Server. Virtualization-based Security (VBS) and Hypervisor-protected code integrity (HVCI) can now be enabled across the Windows 10 ecosystem. These Exploit Guard features can now be enabled through the Windows Defender Security Center.

For more information, see Reduce attack surfaces with Windows Defender Exploit Guard

Windows Defender ATP

Windows Defender ATP has been enhanced with many new capabilities. For more information, see the following topics:

- Query data using Advanced hunting in Windows Defender ATP
- Use Automated investigations to investigate and remediate threats
- Enable conditional access to better protect users, devices, and data

Also see New capabilities of Windows Defender ATP further maximizing the effectiveness and robustness of endpoint security

Windows Defender Application Guard

Windows Defender Application Guard has added support for Edge. For more information, see System requirements for Windows Defender Application Guard

Windows Defender Device Guard

Configurable code integrity is being rebranded as Windows Defender Application Control. This is to help distinguish it as a standalone feature to control execution of applications. For more information about Device Guard, see Windows Defender Device Guard deployment guide.

Windows Information Protection

This release enables support for WIP with Files on Demand, allows file encryption while the file is open in another app, and improves performance. For more information, see OneDrive Files On-Demand For The Enterprise.

Office 365 Ransomware Detection

For Office 365 Home and Office 365 Personal subscribers, Ransomware Detection notifies you when your OneDrive files have been attacked and guides you through the process of restoring your files. For more information, see Ransomware detection and recovering your files

Windows Analytics

Upgrade Readiness

Upgrade Readiness has added the ability to assess Spectre and Meltdown protections on your devices. This addition allows you to see if your devices have Windows OS and firmware updates with Spectre and Meltdown mitigations installed, as well as whether your antivirus client is compatible with these updates. For more information, see Upgrade Readiness now helps assess Spectre and Meltdown protections

Update Compliance

Update Compliance has added Delivery Optimization to assess the bandwidth consumption of Windows Updates. For more information, see Delivery Optimization in Update Compliance

Device Health

Device Health's new App Reliability reports enable you to see where app updates or configuration changes may be needed to reduce crashes. The Login Health reports reveal adoption, success rates, and errors for Windows Hello and for passwords— for a smooth migration to the password-less future. For more information, see Using Device Health

Microsoft Edge

iOS and Android versions of Edge are now available. For more information, see Microsoft Edge Tips.

Support in Windows Defender Application Guard is also improved.

See Also

- Windows 10 Features: Review general information about Windows 10 features.
- What's New in Windows 10: See what's new in other versions of Windows 10.
- What's new in Windows 10, version 1709: See what's new in Windows 10 hardware.
- Windows 10 Fall Creators Update Next Generation Security: YouTube video about Windows Defender ATP in Windows 10, version 1709.

What's new in Windows 10, version 1709 IT Pro content

5/31/2019 • 5 minutes to read • Edit Online

Applies to

- Windows 10, version 1709

Below is a list of some of the new and updated content that discusses IT Pro features in Windows 10, version 1709, also known as the Fall Creators Update. Windows 10, version 1709 also contains all features and fixes included in previous cumulative updates to Windows 10, version 1703.

A brief description of new or updated features in this version of Windows 10 is provided, with links to content with more detailed information. The following 3-minute video summarizes these features.

Deployment

Windows Autopilot

Windows Autopilot is a zero touch experience for deploying Windows 10 devices. Configuration profiles can now be applied at the hardware vendor with devices being shipped directly to employees. For more information, see Overview of Windows Autopilot.

You can also apply an Autopilot deployment profile to your devices using Microsoft Store for Business. When people in your organization run the out-of-box experience on the device, the profile configures Windows based on the Autopilot deployment profile you applied to the device. For more information, see Manage Windows device deployment with Windows Autopilot Deployment.

Windows 10 Subscription Activation

Windows 10 Subscription Activation lets you deploy Windows 10 Enterprise in your organization with no keys and no reboots using a list of subscribed users. When a subscribed user signs in on their Windows 10 Pro device, features that are Enterprise-only are automatically enabled. For more information, see Windows 10 Subscription Activation.

Autopilot Reset

IT Pros can use Autopilot Reset to quickly remove personal files, apps, and settings. A custom login screen is available from the lock screen that enables you to apply original settings and management enrollment (Azure Active Directory and device management) so that devices are returned to a fully configured, known, IT-approved state and ready to use. For more information, see Reset devices with Autopilot Reset.

Update

Windows Update for Business (WUfB)

WUfB now has additional controls available to manage Windows Insider Program enrollment through policies. For more information, see Manage Windows Insider Program flights.

Windows Insider Program for Business

You can now register your Azure AD domains to the Windows Insider Program. For more information, see

Windows Insider Program for Business.

Administration

Mobile Device Management (MDM)

MDM has been expanded to include domain joined devices with Azure Active Directory registration. Group Policy can be used with Active Directory joined devices to trigger auto-enrollment to MDM. For more information, see Enroll a Windows 10 device automatically using Group Policy.

Multiple new configuration items are also added. For more information, see What's new in MDM enrollment and management.

Application Management

Mixed Reality Apps

This version of Windows 10 introduces Windows Mixed Reality. Organizations that use WSUS must take action to enable Windows Mixed Reality. You can also prohibit use of Windows Mixed Reality by blocking installation of the Mixed Reality Portal. For more information, see Enable or block Windows Mixed Reality apps in the enterprise.

Configuration

Kiosk Configuration

The AssignedAccess CSP has been expanded to make it easy for administrators to create kiosks that run more than one app. You can configure multi-app kiosks using a provisioning package. For more information, see Create a Windows 10 kiosk that runs multiple apps.

Security

> **NOTE**
> Windows security features have been rebranded as Windows Defender security features, including Windows Defender Device Guard, Windows Defender Credential Guard, and Windows Defender Firewall.

Windows security baselines have been updated for Windows 10. A security baseline is a group of Microsoft-recommended configuration settings and explains their security impact. For more information, and to download the Policy Analyzer tool, see Microsoft Security Compliance Toolkit 1.0.

Windows Defender ATP

Windows Defender ATP has been expanded with powerful analytics, security stack integration, and centralized management for better detection, prevention, investigation, response, and management. For more information, see View the Windows Defender Advanced Threat Protection Security analytics dashboard.

Windows Defender Application Guard

Windows Defender Application Guard hardens a favorite attacker entry-point by isolating malware and other threats away from your data, apps, and infrastructure. For more information, see Windows Defender Application Guard overview.

Window Defender Exploit Guard

Window Defender Exploit Guard provides intrusion prevention capabilities to reduce the attack and exploit surface of applications. Exploit Guard has many of the threat mitigations that were available in Enhanced Mitigation Experience Toolkit (EMET) toolkit, a deprecated security download. These mitigations are now built into Windows and configurable with Exploit Guard. For more information, see Windows Defender Exploit Guard.

Windows Defender Device Guard

Configurable code integrity is being rebranded as Windows Defender Application Control. This is to help distinguish it as a standalone feature to control execution of applications. For more information about Device Guard, see Windows Defender Device Guard deployment guide.

Windows Information Protection

Windows Information Protection is now designed to work with Microsoft Office and Azure Information Protection. For more information, see Deploying and managing Windows Information Protection (WIP) with Azure Information Protection.

Windows Hello

New features in Windows Hello enable a better device lock experience, using multifactor unlock with new location and user proximity signals. Using Bluetooth signals, you can configure your Windows 10 device to automatically lock when you walk away from it, or to prevent others from accessing the device when you are not present. More details about this feature will be available soon. For general information, see Windows Hello for Business.

BitLocker

The minimum PIN length is being changed from 6 to 4, with a default of 6. For more information, see BitLocker Group Policy settings.

Windows security baselines

Microsoft has released new Windows security baselines for Windows Server and Windows 10. A security baseline is a group of Microsoft-recommended configuration settings with an explanation of their security impact. For more information, and to download the Policy Analyzer tool, see Microsoft Security Compliance Toolkit 1.0.

SMBLoris vulnerability

An issue, known as "SMBLoris  ?, which could result in denial of service, has been addressed.

Windows Analytics

Upgrade Readiness

Upgrade Readiness provides insights into application and driver compatibility issues. New capabilities include better app coverage, post-upgrade health reports, and enhanced report filtering capabilities. For more information, see Manage Windows upgrades with Upgrade Readiness.

Update Compliance

New capabilities in Update Compliance let you monitor Windows Defender protection status, compare compliance with industry peers, and optimize bandwidth for deploying updates. For more information, see Monitor Windows Updates and Windows Defender Antivirus with Update Compliance.

Device Health

Maintaining devices is made easier with Device Health, a new, premium analytic tool that identifies devices and drivers that crash frequently and might need to be rebuilt or replaced. For more information, see Monitor the health of devices with Device Health.

Networking

Network stack

Several network stack enhancements are available in this release. Some of these features were also available in Windows 10, version 1703. For more information, see Core Network Stack Features in the Creators Update for Windows 10.

See Also

Windows 10 Features: Review general information about Windows 10 features.
What's New in Windows 10: See what's new in other versions of Windows 10.
What's new in Windows 10, version 1709: See what's new in Windows 10 hardware.
Windows 10 Fall Creators Update Next Generation Security: YouTube video about Windows Defender ATP in Windows 10, version 1709.

What's new in Windows 10, version 1703 IT pro content

6/18/2019 • 18 minutes to read • Edit Online

Below is a list of some of what's new in Information Technology (IT) pro features in Windows 10, version 1703 (also known as the Creators Update).

For more general info about Windows 10 features, see Features available only on Windows 10. For info about previous versions of Windows 10, see What's New in Windows 10. Also see this blog post: What's new for IT pros in the Windows 10 Creators Update.

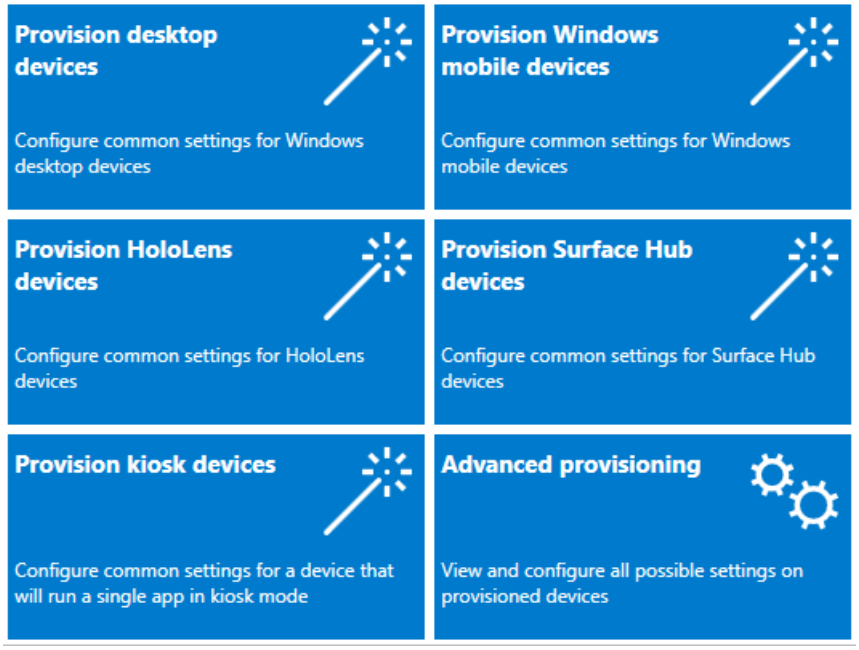
> **NOTE**
> Windows 10, version 1703 contains all fixes included in previous cumulative updates to Windows 10, version 1607. For info about each version, see Windows 10 release information. For a list of removed features, see Features that are removed or deprecated in Windows 10 Creators Update.

Configuration

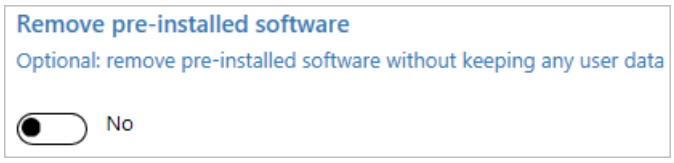
Windows Configuration Designer

Previously known as *Windows Imaging and Configuration Designer (ICD)*, the tool for creating provisioning packages is renamed **Windows Configuration Designer**. The new Windows Configuration Designer is available in Microsoft Store as an app. To run Windows Configuration Designer on earlier versions of Windows, you can still install Windows Configuration Designer from the Windows Assessment and Deployment Kit (ADK).

Windows Configuration Designer in Windows 10, version 1703, includes several new wizards to make it easier to create provisioning packages.



Both the desktop and kiosk wizards include an option to remove pre-installed software, based on the new CleanPC configuration service provider (CSP).



Learn more about Windows Configuration Designer.

Azure Active Directory join in bulk

Using the new wizards in Windows Configuration Designer, you can create provisioning packages to enroll devices in Azure Active Directory. Azure AD join in bulk is available in the desktop, mobile, kiosk, and Surface Hub wizards.

Windows Spotlight

The following new Group Policy and mobile device management (MDM) settings are added to help you configure Windows Spotlight user experiences:

- **Turn off the Windows Spotlight on Action Center**
- **Do not use diagnostic data for tailored experiences**
- **Turn off the Windows Welcome Experience**

Learn more about Windows Spotlight.

Start and taskbar layout

Enterprises have been able to apply customized Start and taskbar layouts to devices running Windows 10 Enterprise and Education. In Windows 10, version 1703, customized Start and taskbar layout can also be applied to Windows 10 Pro.

Previously, the customized taskbar could only be deployed using Group Policy or provisioning packages. Windows 10, version 1703, adds support for customized taskbars to MDM.

Additional MDM policy settings are available for Start and taskbar layout. New MDM policy settings include:

- Settings for the User tile: **Start/HideUserTile**, **Start/HideSwitchAccount**, **Start/HideSignOut**, **Start/HideLock**, and **Start/HideChangeAccountSettings**
- Settings for Power: **Start/HidePowerButton**, **Start/HideHibernate**, **Start/HideRestart**, **Start/HideShutDown**, and **Start/HideSleep**
- Additional new settings: **Start/HideFrequentlyUsedApps**, **Start/HideRecentlyAddedApps**, **AllowPinnedFolder**, **ImportEdgeAssets**, **Start/HideRecentJumplists**, **Start/NoPinningToTaskbar**, **Settings/PageVisibilityList**, and **Start/HideAppsList**.

Cortana at work

Cortana is Microsoft's personal digital assistant, who helps busy people get things done, even while at work. Cortana has powerful configuration options, specifically optimized for your business. By signing in with an Azure Active Directory (Azure AD) account, your employees can give Cortana access to their enterprise/work identity, while getting all the functionality Cortana provides to them outside of work.

Using Azure AD also means that you can remove an employee's profile (for example, when an employee leaves your organization) while respecting Windows Information Protection (WIP) policies and ignoring enterprise content, such as emails, calendar items, and people lists that are marked as enterprise data.

For more info about Cortana at work, see Cortana integration in your business or enterprise

Deployment

MBR2GPT.EXE

MBR2GPT.EXE is a new command-line tool available in Windows 10 version 1703 and later versions. MBR2GPT converts a disk from Master Boot Record (MBR) to GUID Partition Table (GPT) partition style without modifying or deleting data on the disk. The tool is designed to be run from a Windows Preinstallation Environment (Windows PE) command prompt, but can also be run from the full Windows 10 operating system (OS).

The GPT partition format is newer and enables the use of larger and more disk partitions. It also provides added data reliability, supports additional partition types, and enables faster boot and shutdown speeds. If you convert the system disk on a computer from MBR to GPT, you must also configure the computer to boot in UEFI mode, so make sure that your device supports UEFI before attempting to convert the system disk.

Additional security features of Windows 10 that are enabled when you boot in UEFI mode include: Secure Boot, Early Launch Anti-malware (ELAM) driver, Windows Trusted Boot, Measured Boot, Device Guard, Credential Guard, and BitLocker Network Unlock.

For details, see MBR2GPT.EXE.

Security

Windows Defender Advanced Threat Protection

New features in Windows Defender Advanced Threat Protection (ATP) for Windows 10, version 1703 include:

- **Detection**
  Enhancements to the detection capabilities include:
  - Use the threat intelligence API to create custom alerts - Understand threat intelligence concepts, enable the threat intel application, and create custom threat intelligence alerts for your organization.
  - Improvements on OS memory and kernel sensors to enable detection of attackers who are using in-memory and kernel-level attacks
  - Upgraded detections of ransomware and other advanced attacks
  - Historical detection capability ensures new detection rules apply to up to six months of stored data to detect previous attacks that might not have been noticed
- **Investigation**
  Enterprise customers can now take advantage of the entire Windows security stack with Windows Defender Antivirus detections and Device Guard blocks being surfaced in the Windows Defender ATP portal. Other capabilities have been added to help you gain a holistic view on investigations.

  Other investigation enhancements include:
  - Investigate a user account - Identify user accounts with the most active alerts and investigate cases of potential compromised credentials.
  - Alert process tree - Aggregates multiple detections and related events into a single view to reduce case resolution time.
  - Pull alerts using REST API - Use REST API to pull alerts from Windows Defender ATP.
- **Response**
  When detecting an attack, security response teams can now take immediate action to contain a breach:
  - Take response actions on a machine - Quickly respond to detected attacks by isolating machines or collecting an investigation package.
  - Take response actions on a file - Quickly respond to detected attacks by stopping and quarantining files or blocking a file.
- **Other features**
  - Check sensor health state - Check an endpoint's ability to provide sensor data and communicate with the Windows Defender ATP service and fix known issues.

You can read more about ransomware mitigations and detection capability in Windows Defender Advanced Threat Protection in the blog: Averting ransomware epidemics in corporate networks with Windows Defender ATP.

Get a quick, but in-depth overview of Windows Defender ATP for Windows 10 and the new capabilities in Windows 10, version 1703 see Windows Defender ATP for Windows 10 Creators Update.

Windows Defender Antivirus

Windows Defender is now called Windows Defender Antivirus, and we've increased the breadth of the documentation library for enterprise security admins.

The new library includes information on:

- Deploying and enabling AV protection
- Managing updates
- Reporting
- Configuring features
- Troubleshooting

Some of the highlights of the new library include:

- Evaluation guide for Windows Defender AV
- Deployment guide for Windows Defender AV in a virtual desktop infrastructure environment

New features for Windows Defender AV in Windows 10, version 1703 include:

- Updates to how the Block at First Sight feature can be configured
- The ability to specify the level of cloud-protection
- Windows Defender Antivirus protection in the Windows Defender Security Center app

In Windows 10, version 1607, we invested heavily in helping to protect against ransomware, and we continue that investment in version 1703 with updated behavior monitoring and always-on real-time protection.

You can read more about ransomware mitigations and detection capability in Windows Defender AV in the Ransomware Protection in Windows 10 Anniversary Update whitepaper (PDF) and at the Microsoft Malware Protection Center blog.

Device Guard and Credential Guard

Additional security qualifications for Device Guard and Credential Guard help protect vulnerabilities in UEFI runtime. For more information, see Device Guard Requirements and Credential Guard Security Considerations.

Group Policy Security Options

The security setting **Interactive logon: Display user information when the session is locked** has been updated to work in conjunction with the **Privacy** setting in **Settings** > **Accounts** > **Sign-in options**.

A new security policy setting **Interactive logon: Don't display username at sign-in** has been introduced in Windows 10 version 1703. This security policy setting determines whether the username is displayed during sign in. It works in conjunction with the **Privacy** setting in **Settings** > **Accounts** > **Sign-in options**. The setting only affects the **Other user** tile.

Windows Hello for Business

You can now reset a forgotten PIN without deleting company managed data or apps on devices managed by Microsoft Intune.

For Windows Phone devices, an administrator is able to initiate a remote PIN reset through the Intune portal.

For Windows desktops, users are able to reset a forgotten PIN through **Settings > Accounts > Sign-in options**.

For more details, check out What if I forget my PIN?.

Windows Information Protection (WIP) and Azure Active Directory (Azure AD)

Microsoft Intune helps you create and deploy your Windows Information Protection (WIP) policy, including letting you choose your allowed apps, your WIP-protection level, and how to find enterprise data on the network. For more info, see Create a Windows Information Protection (WIP) policy using Microsoft Intune and Associate and deploy your Windows Information Protection (WIP) and VPN policies by using Microsoft Intune.

You can also now collect your audit event logs by using the Reporting configuration service provider (CSP) or the Windows Event Forwarding (for Windows desktop domain-joined devices). For info, see the brand-new topic, How to collect Windows Information Protection (WIP) audit event logs.

Update

Windows Update for Business

The pause feature has been changed, and now requires a start date to set up. Users are now able to pause through **Settings > Update & security > Windows Update > Advanced options** in case a policy has not been configured. We have also increased the pause limit on quality updates to 35 days. You can find more information on pause in Pause Feature Updates and Pause Quality Updates.

Windows Update for Business managed devices are now able to defer feature update installation by up to 365 days (it used to be 180 days). In settings, users are able to select their branch readiness level and update deferal periods. See Configure devices for Current Branch (CB) or Current Branch for Business (CBB), Configure when devices receive Feature Updates and Configure when devices receive Quality Updates for details.

Windows Insider for Business

We recently added the option to download Windows 10 Insider Preview builds using your corporate credentials in Azure Active Directory (AAD). By enrolling devices in AAD, you increase the visibility of feedback submitted by users in your organization – especially on features that support your specific business needs. For details, see Windows Insider Program for Business.

Optimize update delivery

With changes delivered in Windows 10, version 1703, Express updates are now fully supported with System Center Configuration Manager, starting with version 1702 of Configuration Manager, as well as with other third-party updating and management products that implement this new functionality. This is in addition to current Express support on Windows Update, Windows Update for Business and WSUS.

> **NOTE**
> The above changes can be made available to Windows 10, version 1607, by installing the April 2017 cumulative update.

Delivery Optimization policies now enable you to configure additional restrictions to have more control in various scenarios.

Added policies include:

- Allow uploads while the device is on battery while under set Battery level
- Enable Peer Caching while the device connects via VPN
- Minimum RAM (inclusive) allowed to use Peer Caching
- Minimum disk size allowed to use Peer Caching
- Minimum Peer Caching Content File Size

To check out all the details, see Configure Delivery Optimization for Windows 10 updates

Uninstalled in-box apps no longer automatically reinstall

Starting with Windows 10, version 1703, in-box apps that were uninstalled by the user won't automatically reinstall as part of the feature update installation process.

Additionally, apps de-provisioned by admins on Windows 10, version 1703 machines will stay de-provisioned after future feature update installations. This will not apply to the update from Windows 10, version 1607 (or earlier) to version 1703.

Management

New MDM capabilities

Windows 10, version 1703 adds many new configuration service providers (CSPs) that provide new capabilities for managing Windows 10 devices using MDM or provisioning packages. Among other things, these CSPs enable you to configure a few hundred of the most useful Group Policy settings via MDM - see Policy CSP - ADMX-backed policies.

Some of the other new CSPs are:

- The DynamicManagement CSP allows you to manage devices differently depending on location, network, or time. For example, managed devices can have cameras disabled when at a work location, the cellular service can be disabled when outside the country to avoid roaming charges, or the wireless network can be disabled when the device is not within the corporate building or campus. Once configured, these settings will be enforced even if the device can't reach the management server when the location or network changes. The Dynamic Management CSP enables configuration of policies that change how the device is managed in addition to setting the conditions on which the change occurs.
- The CleanPC CSP allows removal of user-installed and pre-installed applications, with the option to persist user data.
- The BitLocker CSP is used to manage encryption of PCs and devices. For example, you can require storage card encryption on mobile devices, or require encryption for operating system drives.
- The NetworkProxy CSP is used to configure a proxy server for ethernet and Wi-Fi connections.
- The Office CSP enables a Microsoft Office client to be installed on a device via the Office Deployment Tool. For more information, see Configuration options for the Office Deployment Tool.
- The EnterpriseAppVManagement CSP is used to manage virtual applications in Windows 10 PCs (Enterprise and Education editions) and enables App-V sequenced apps to be streamed to PCs even when managed by MDM.

IT pros can use the new MDM Migration Analysis Tool (MMAT) to determine which Group Policy settings have been configured for a user or computer and cross-reference those settings against a built-in list of supported MDM policies. MMAT can generate both XML and HTML reports indicating the level of support for each Group Policy setting and MDM equivalents.

Learn more about new MDM capabilities.

Mobile application management support for Windows 10

The Windows version of mobile application management (MAM) is a lightweight solution for managing company data access and security on personal devices. MAM support is built into Windows on top of Windows Information Protection (WIP), starting in Windows 10, version 1703.

For more info, see Implement server-side support for mobile application management on Windows.

MDM diagnostics

In Windows 10, version 1703, we continue our work to improve the diagnostic experience for modern

management. By introducing auto-logging for mobile devices, Windows will automatically collect logs when encountering an error in MDM, eliminating the need to have always-on logging for memory-constrained devices. Additionally, we are introducing Microsoft Message Analyzer as an additional tool to help Support personnel quickly reduce issues to their root cause, while saving time and cost.

Application Virtualization for Windows (App-V)

Previous versions of the Microsoft Application Virtualization Sequencer (App-V Sequencer) have required you to manually create your sequencing environment. Windows 10, version 1703 introduces two new PowerShell cmdlets, New-AppVSequencerVM and Connect-AppvSequencerVM, which automatically create your sequencing environment for you, including provisioning your virtual machine. Additionally, the App-V Sequencer has been updated to let you sequence or update multiple apps at the same time, while automatically capturing and storing your customizations as an App-V project template (.appvt) file, and letting you use PowerShell or Group Policy settings to automatically cleanup your unpublished packages after a device restart.

For more info, see the following topics:

- Automatically provision your sequencing environment using Microsoft Application Virtualization Sequencer (App-V Sequencer)
- Automatically sequence multiple apps at the same time using Microsoft Application Virtualization Sequencer (App-V Sequencer)
- Automatically update multiple apps at the same time using Microsoft Application Virtualization Sequencer (App-V Sequencer)
- Automatically cleanup unpublished packages on the App-V client

Windows diagnostic data

Learn more about the diagnostic data that's collected at the Basic level and some examples of the types of data that is collected at the Full level.

- Windows 10, version 1703 basic level Windows diagnostic events and fields
- Windows 10, version 1703 Diagnostic Data

Group Policy spreadsheet

Learn about the new Group Policies that were added in Windows 10, version 1703.

- Group Policy Settings Reference for Windows and Windows Server

Windows 10 Mobile enhancements

Lockdown Designer

The Lockdown Designer app helps you configure and create a lockdown XML file to apply to devices running Windows 10 Mobile, and includes a remote simulation to help you determine the layout for tiles on the Start screen. Using Lockdown Designer is easier than manually creating a lockdown XML file.

Learn more about the Lockdown Designer app.

Other enhancements

Windows 10 Mobile, version 1703 also includes the following enhancements:

- SD card encryption
- Remote PIN resets for Azure Active Directory accounts

- SMS text message archiving
- WiFi Direct management
- OTC update tool
- Continuum display management
  - Individually turn off the monitor or phone screen when not in use
  - Indiviudally adjust screen time-out settings
- Continuum docking solutions
  - Set Ethernet port properties
  - Set proxy properties for the Ethernet port

Miracast on existing wireless network or LAN

In the Windows 10, version 1703, Microsoft has extended the ability to send a Miracast stream over a local network rather than over a direct wireless link. This functionality is based on the Miracast over Infrastructure Connection Establishment Protocol (MS-MICE).

Miracast over Infrastructure offers a number of benefits:

- Windows automatically detects when sending the video stream over this path is applicable.
- Windows will only choose this route if the connection is over Ethernet or a secure Wi-Fi network.
- Users do not have to change how they connect to a Miracast receiver. They use the same UX as for standard Miracast connections.
- No changes to current wireless drivers or PC hardware are required.
- It works well with older wireless hardware that is not optimized for Miracast over Wi-Fi Direct.
- It leverages an existing connection which both reduces the time to connect and provides a very stable stream.

How it works

Users attempt to connect to a Miracast receiver as they did previously. When the list of Miracast receivers is populated, Windows 10 will identify that the receiver is capable of supporting a connection over the infrastructure. When the user selects a Miracast receiver, Windows 10 will attempt to resolve the device's hostname via standard DNS, as well as via multicast DNS (mDNS). If the name is not resolvable via either DNS method, Windows 10 will fall back to establishing the Miracast session using the standard Wi-Fi direct connection.

Enabling Miracast over Infrastructure

If you have a device that has been updated to Windows 10, version 1703, then you automatically have this new feature. To take advantage of it in your environment, you need to ensure the following is true within your deployment:

- The device (PC, phone, or Surface Hub) needs to be running Windows 10, version 1703.
- A Windows PC or Surface Hub can act as a Miracast over Infrastructure *receiver*. A Windows PC or phone can act as a Miracast over Infrastructure *source*.
  - As a Miracast receiver, the PC or Surface Hub must be connected to your enterprise network via either Ethernet or a secure Wi-Fi connection (e.g. using either WPA2-PSK or WPA2-Enterprise security). If the Hub is connected to an open Wi-Fi connection, Miracast over Infrastructure will disable itself.
  - As a Miracast source, the PC or phone must be connected to the same enterprise network via Ethernet or a secure Wi-Fi connection.
- The DNS Hostname (device name) of the device needs to be resolvable via your DNS servers. You can achieve this by either allowing your device to register automatically via Dynamic DNS, or by manually creating an A or AAAA record for the device's hostname.
- Windows 10 PCs must be connected to the same enterprise network via Ethernet or a secure Wi-Fi connection.

It is important to note that Miracast over Infrastructure is not a replacement for standard Miracast. Instead, the

functionality is complementary, and provides an advantage to users who are part of the enterprise network. Users who are guests to a particular location and don't have access to the enterprise network will continue to connect using the Wi-Fi Direct connection method.

New features in related products

The following new features aren't part of Windows 10, but help you make the most of it.

Upgrade Readiness

Upgrade Readiness helps you ensure that applications and drivers are ready for a Windows 10 upgrade. The solution provides up-to-date application and driver inventory, information about known issues, troubleshooting guidance, and per-device readiness and tracking details. The Upgrade Readiness tool moved from public preview to general availability on March 2, 2017.

The development of Upgrade Readiness has been heavily influenced by input from the community the development of new features is ongoing. To begin using Upgrade Readiness, add it to an existing Operation Management Suite (OMS) workspace or sign up for a new OMS workspace with the Upgrade Readiness solution enabled.

For more information about Upgrade Readiness, see the following topics:

- Windows Analytics blog
- Manage Windows upgrades with Upgrade Readiness

Update Compliance

Update Compliance helps you to keep Windows 10 devices in your organization secure and up-to-date.

Update Compliance is a solution built using OMS Log Analytics that provides information about installation status of monthly quality and feature updates. Details are provided about the deployment progress of existing updates and the status of future updates. Information is also provided about devices that might need attention to resolve issues.

For more information about Update Compliance, see Monitor Windows Updates with Update Compliance.

What's new in Windows 10, version 1607

5/31/2019 • 7 minutes to read • Edit Online

Below is a list of some of the new and updated features in Windows 10, version 1607 (also known as the Anniversary Update).

> **NOTE**
> For release dates and servicing options for each version, see Windows 10 release information.

Deployment

Windows Imaging and Configuration Designer (ICD)

In previous versions of the Windows 10 Assessment and Deployment Kit (ADK), you had to install additional features for Windows ICD to run. Starting in version 1607, you can install just the configuration designer component independent of the rest of the imaging components. Install the ADK.

Windows ICD now includes simplified workflows for creating provisioning packages:

- Simple provisioning to set up common settings for Active Directory-joined devices
- Advanced provisioning to deploy certificates and apps
- School provisioning to set up classroom devices for Active Directory

Learn more about using provisioning packages in Windows 10.

Windows Upgrade Readiness

Microsoft developed Upgrade Readiness in response to demand from enterprise customers looking for additional direction and details about upgrading to Windows 10. Upgrade Readiness was built taking into account multiple channels of customer feedback, testing, and Microsoft's experience upgrading millions of devices to Windows 10.

With Windows diagnostic data enabled, Upgrade Readiness collects system, application, and driver data for analysis. We then identify compatibility issues that can block an upgrade and suggest fixes when they are known to Microsoft.

Use Upgrade Readiness to get:

- A visual workflow that guides you from pilot to production
- Detailed computer and application inventory
- Powerful computer level search and drill-downs
- Guidance and insights into application and driver compatibility issues, with suggested fixes
- Data driven application rationalization tools
- Application usage information, allowing targeted validation; workflow to track validation progress and decisions
- Data export to commonly used software deployment tools

The Upgrade Readiness workflow steps you through the discovery and rationalization process until you have a list of computers that are upgrade-ready.

Learn more about planning and managing Windows upgrades with Windows Upgrade Readiness.

Windows updates

Windows 10, version 1607, provides administrators with increased control over updates by changing the update deferral increment from weeks to days. Other changes:

- Quality Updates can be deferred up to 30 days and paused for 35 days
- Feature Updates can be deferred up to 180 days and paused for 60 days
- Update deferrals can be applied to both Current Branch (CB) and Current Branch for Business (CBB)
- Drivers can be excluded from updates

Security

Credential Guard and Device Guard

Isolated User Mode is now included with Hyper-V so you don't have to install it separately.

Windows Hello for Business

When Windows 10 first shipped, it included Microsoft Passport and Windows Hello, which worked together to provide multi-factor authentication. To simplify deployment and improve supportability, Microsoft has combined these technologies into a single solution under the Windows Hello name in Windows 10, version 1607. Customers who have already deployed Microsoft Passport for Work will not experience any change in functionality. Customers who have yet to evaluate Windows Hello will find it easier to deploy due to simplified policies, documentation, and semantics.

Additional changes for Windows Hello in Windows 10, version 1607:

- Personal (Microsoft account) and corporate (Active Directory or Azure AD) accounts use a single container for keys.
- Group Policy settings for managing Windows Hello for Business are now available for both **User Configuration** and **Computer Configuration**.
- Beginning in version 1607, Windows Hello as a convenience PIN is disabled by default on all domain-joined computers. To enable a convenience PIN for Windows 10, version 1607, enable the Group Policy setting **Turn on convenience PIN sign-in**.

Learn more about Windows Hello for Business.

VPN

- The VPN client can integrate with the Conditional Access Framework, a cloud-based policy engine built into Azure Active Directory, to provide a device compliance option for remote clients.
- The VPN client can integrate with Windows Information Protection (WIP) policy to provide additional security. Learn more about Windows Information Protection, previously known as Enterprise Data Protection.
- New VPNv2 configuration service provider (CSP) adds configuration settings. For details, see What's new in MDM enrollment and management
- Microsoft Intune: *VPN Profile (Windows 10 Desktop and Mobile and later)* policy template includes support for native VPN plug-ins.

Windows Information Protection (WIP), formerly known as enterprise data protection (EDP)

With the increase of employee-owned devices in the enterprise, there's also an increasing risk of accidental data leak through apps and services, like email, social media, and the public cloud, which are outside of the enterprise's control. For example, when an employee sends the latest engineering pictures from their personal email account, copies and pastes product info into a tweet, or saves an in-progress sales report to their public cloud storage.

Windows Information Protection (WIP) helps to protect against this potential data leakage without otherwise interfering with the employee experience. WIP also helps to protect enterprise apps and data against accidental data leak on enterprise-owned devices and personal devices that employees bring to work without requiring changes to your environment or other apps.

- Create a Windows Information Protection (WIP) policy
- General guidance and best practices for Windows Information Protection (WIP)

Learn more about Windows Information Protection (WIP)

Windows Defender

Several new features and management options have been added to Windows Defender in Windows 10, version 1607.

- Windows Defender Offline in Windows 10 can be run directly from within Windows, without having to create bootable media.
- Use PowerShell cmdlets for Windows Defender to configure options and run scans.
- Enable the Block at First Sight feature in Windows 10 to leverage the Windows Defender cloud for near-instant protection against new malware.
- Configure enhanced notifications for Windows Defender in Windows 10 to see more information about threat detections and removal.
- Run a Windows Defender scan from the command line.
- Detect and block Potentially Unwanted Applications with Windows Defender during download and install times.

Windows Defender Advanced Threat Protection (ATP)

With the growing threat from more sophisticated targeted attacks, a new security solution is imperative in securing an increasingly complex network ecosystem. Windows Defender Advanced Threat Protection (Windows Defender ATP) is a security service, built into Windows 10 that enables enterprise customers detect, investigate, and respond to advanced threats on their networks.

Learn more about Windows Defender Advanced Threat Protection (ATP).

Management

Use Remote Desktop Connection for PCs joined to Azure Active Directory

From its release, Windows 10 has supported remote connections to PCs that are joined to Active Directory. Starting in Windows 10, version 1607, you can also connect to a remote PC that is joined to Azure Active Directory (Azure AD). Learn about the requirements and supported configurations.

Taskbar configuration

Enterprise administrators can add and remove pinned apps from the taskbar. Users can pin apps, unpin apps, and change the order of pinned apps on the taskbar after the enterprise configuration is applied. Learn how to configure the taskbar.

Mobile device management and configuration service providers (CSPs)

Numerous settings have been added to the Windows 10 CSPs to expand MDM capabilities for managing devices. To learn more about the specific changes in MDM policies for Windows 10, version 1607, see What's new in MDM enrollment and management.

Shared PC mode

Windows 10, Version 1607, introduces shared PC mode, which optimizes Windows 10 for shared use scenarios, such as touchdown spaces in an enterprise and temporary customer use in retail. You can apply shared PC mode to Windows 10 Pro, Education, and Enterprise. Learn how to set up a shared or guest PC.

Application Virtualization (App-V) for Windows 10

Application Virtualization (App-V) enables organizations to deliver Win32 applications to users as virtual applications. Virtual applications are installed on centrally managed servers and delivered to users as a service – in real time and on as as-needed basis. Users launch virtual applications from familiar access points, including the

Microsoft Store, and interact with them as if they were installed locally.

With the release of Windows 10, version 1607, App-V is included with the Windows 10 for Enterprise edition. If you are new to Windows 10 and App-V or if you're upgrading from a previous version of App-V, you'll need to download, activate, and install server- and client-side components to start delivering virtual applications to users.

Learn how to deliver virtual applications with App-V.

User Experience Virtualization (UE-V) for Windows 10

Many users customize their settings for Windows and for specific applications. Customizable Windows settings include Microsoft Store appearance, language, background picture, font size, and accent colors. Customizable application settings include language, appearance, behavior, and user interface options.

With User Experience Virtualization (UE-V), you can capture user-customized Windows and application settings and store them on a centrally managed network file share. When users log on, their personalized settings are applied to their work session, regardless of which device or virtual desktop infrastructure (VDI) sessions they log on to.

With the release of Windows 10, version 1607, UE-V is included with the Windows 10 for Enterprise edition. If you are new to Windows 10 and UE-V or upgrading from a previous version of UE-V, you'll need to download, activate, and install server- and client-side components to start synchronizing user-customized settings across devices.

Learn how to synchronize user-customized settings with UE-V.

Learn more

- Windows 10 release information

What's new in Windows 10, versions 1507 and 1511

6/6/2019 • 16 minutes to read • Edit Online

Below is a list of some of the new and updated features included in the initial release of Windows 10 (version 1507) and the Windows 10 update to version 1511.

> **NOTE**
> For release dates and servicing options for each version, see Windows 10 release information.

Deployment

Provisioning devices using Windows Imaging and Configuration Designer (ICD)

With Windows 10, you can create provisioning packages that let you quickly and efficiently configure a device without having to install a new image. Windows provisioning makes it easy for IT administrators to configure end-user devices without imaging. Using Windows Provisioning, an IT administrator can easily specify desired configuration and settings required to enroll the devices into management (through a wizard-driven user interface) and then apply that configuration to target devices in a matter of minutes. It is best suited for small- to medium-sized businesses with deployments that range from tens to a few hundred computers.

Learn more about provisioning in Windows 10.

Security

Applocker

New Applocker features in Windows 10, version 1507

- A new parameter was added to the New-AppLockerPolicy Windows PowerShell cmdlet that lets you choose whether executable and DLL rule collections apply to non-interactive processes. To enable this, set the **ServiceEnforcement** to **Enabled**.
- A new AppLocker configuration service provider was add to allow you to enable AppLocker rules by using an MDM server.
- You can manage Windows 10 Mobile devices by using the new AppLocker CSP.

Learn how to manage AppLocker within your organization.

Bitlocker

New Bitlocker features in Windows 10, version 1511

- **XTS-AES encryption algorithm**. BitLocker now supports the XTS-AES encryption algorithm. XTS-AES provides additional protection from a class of attacks on encryption that rely on manipulating cipher text to cause predictable changes in plain text. BitLocker supports both 128-bit and 256-bit XTS-AES keys. It provides the following benefits:
  - The algorithm is FIPS-compliant.
  - Easy to administer. You can use the BitLocker Wizard, manage-bde, Group Policy, MDM policy, Windows PowerShell, or WMI to manage it on devices in your organization.

> **Note:** Drives encrypted with XTS-AES will not be accessible on older version of Windows. This is only recommended for fixed and operating system drives. Removable drives should continue to use the AES-CBC 128-bit or AES-CBC 256-bit algorithms.

New Bitlocker features in Windows 10, version 1507

- **Encrypt and recover your device with Azure Active Directory**. In addition to using a Microsoft Account, automatic Device Encryption can now encrypt your devices that are joined to an Azure Active Directory domain. When the device is encrypted, the BitLocker recovery key is automatically escrowed to Azure Active Directory. This will make it easier to recover your BitLocker key online.
- **DMA port protection**. You can use the DataProtection/AllowDirectMemoryAccess MDM policy to block DMA ports when the device is starting up. Also, when a device is locked, all unused DMA ports are turned off, but any devices that are already plugged into a DMA port will continue to work. When the device is unlocked, all DMA ports are turned back on.
- **New Group Policy for configuring pre-boot recovery**. You can now configure the pre-boot recovery message and recover URL that is shown on the pre-boot recovery screen. For more info, see the Configure pre-boot recovery message and URL section in "BitLocker Group Policy settings."

Learn how to deploy and manage BitLocker within your organization.

Credential Guard

New Credential Guard features in Windows 10, version 1511

- **Credential Manager support**. Credentials that are stored with Credential Manager, including domain credentials, are protected with Credential Guard with the following considerations:
  - Credentials that are saved by the Remote Desktop Protocol cannot be used. Employees in your organization can manually store credentials in Credential Manager as generic credentials.
  - Applications that extract derived domain credentials using undocumented APIs from Credential Manager will no longer be able to use those saved derived credentials.
  - You cannot restore credentials using the Credential Manager control panel if the credentials were backed up from a PC that has Credential Guard turned on. If you need to back up your credentials, you must do this before you enable Credential Guard. Otherwise, you won't be able to restore those credentials.
- **Enable Credential Guard without UEFI lock**. You can enable Credential Guard by using the registry. This allows you to disable Credential Guard remotely. However, we recommend that Credential Guard is enabled with UEFI lock. You can configure this by using Group Policy.
- **CredSSP/TsPkg credential delegation**. CredSSP/TsPkg cannot delegate default credentials when Credential Guard is enabled.

Learn how to deploy and manage Credential Guard within your organization.

Easier certificate management

For Windows 10-based devices, you can use your MDM server to directly deploy client authentication certificates using Personal Information Exchange (PFX), in addition to enrolling using Simple Certificate Enrollment Protocol (SCEP), including certificates to enable Windows Hello for Business in your enterprise. You'll be able to use MDM to enroll, renew, and delete certificates. As in Windows Phone 8.1, you can use the Certificates app to review the details of certificates on your device. Learn how to install digital certificates on Windows 10 Mobile.

Microsoft Passport

In Windows 10, Microsoft Passport replaces passwords with strong two-factor authentication that consists of an enrolled device and a Windows Hello (biometric) or PIN.

Microsoft Passport lets users authenticate to a Microsoft account, an Active Directory account, a Microsoft Azure Active Directory (AD) account, or non-Microsoft service that supports Fast ID Online (FIDO) authentication. After an initial two-step verification during Microsoft Passport enrollment, a Microsoft Passport is set up on the user's device and the user sets a gesture, which can be Windows Hello or a PIN. The user provides the gesture to verify identity; Windows then uses Microsoft Passport to authenticate users and help them to access protected resources and services.

Security auditing

New Security auditing features in Windows 10, version 1511

- The WindowsSecurityAuditing and Reporting configuration service providers allow you to add security audit policies to mobile devices.

New features in Windows 10, version 1507

In Windows 10, security auditing has added some improvements:

- New audit subcategories
- More info added to existing audit events

New audit subcategories

In Windows 10, two new audit subcategories were added to the Advanced Audit Policy Configuration to provide greater granularity in audit events:

- Audit Group Membership Found in the Logon/Logoff audit category, the Audit Group Membership subcategory allows you to audit the group membership information in a user's logon token. Events in this subcategory are generated when group memberships are enumerated or queried on the PC where the logon session was created. For an interactive logon, the security audit event is generated on the PC that the user logged on to. For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the PC hosting the resource. When this setting is configured, one or more security audit events are generated for each successful logon. You must also enable the **Audit Logon** setting under **Advanced Audit Policy Configuration\System Audit Policies\Logon/Logoff**. Multiple events are generated if the group membership information cannot fit in a single security audit event.
- Audit PNP Activity Found in the Detailed Tracking category, the Audit PNP Activity subcategory allows you to audit when plug and play detects an external device. Only Success audits are recorded for this category. If you do not configure this policy setting, no audit event is generated when an external device is detected by plug and play. A PnP audit event can be used to track down changes in system hardware and will be logged on the PC where the change took place. A list of hardware vendor IDs are included in the event.

More info added to existing audit events

With Windows 10, version 1507, we've added more info to existing audit events to make it easier for you to put together a full audit trail and come away with the information you need to protect your enterprise. Improvements were made to the following audit events:

- Changed the kernel default audit policy
- Added a default process SACL to LSASS.exe
- Added new fields in the logon event
- Added new fields in the process creation event
- Added new Security Account Manager events
- Added new BCD events
- Added new PNP events

Changed the kernel default audit policy

In previous releases, the kernel depended on the Local Security Authority (LSA) to retrieve info in some of its events. In Windows 10, the process creation events audit policy is automatically enabled until an actual audit policy is received from LSA. This results in better auditing of services that may start before LSA starts.

Added a default process SACL to LSASS.exe

In Windows 10, a default process SACL was added to LSASS.exe to log processes attempting to access LSASS.exe. The SACL is L"S:(AU;SAFA;0x0010;;;WD)". You can enable this under **Advanced Audit Policy Configuration\Object Access\Audit Kernel Object**. This can help identify attacks that steal credentials from the memory of a process.

New fields in the logon event

The logon event ID 4624 has been updated to include more verbose information to make them easier to analyze. The following fields have been added to event 4624:

1. **MachineLogon** String: yes or no If the account that logged into the PC is a computer account, this field will be

yes. Otherwise, the field is no.

2. **ElevatedToken** String: yes or no If the account that logged into the PC is an administrative logon, this field will be yes. Otherwise, the field is no. Additionally, if this is part of a split token, the linked login ID (LSAP_LOGON_SESSION) will also be shown.
3. **TargetOutboundUserName** String **TargetOutboundUserDomain** String The username and domain of the identity that was created by the LogonUser method for outbound traffic.
4. **VirtualAccount** String: yes or no If the account that logged into the PC is a virtual account, this field will be yes. Otherwise, the field is no.
5. **GroupMembership** String A list of all of the groups in the user's token.
6. **RestrictedAdminMode** String: yes or no If the user logs into the PC in restricted admin mode with Remote Desktop, this field will be yes. For more info on restricted admin mode, see Restricted Admin mode for RDP.

New fields in the process creation event

The logon event ID 4688 has been updated to include more verbose information to make them easier to analyze. The following fields have been added to event 4688:

1. **TargetUserSid** String The SID of the target principal.
2. **TargetUserName** String The account name of the target user.
3. **TargetDomainName** String The domain of the target user..
4. **TargetLogonId** String The logon ID of the target user.
5. **ParentProcessName** String The name of the creator process.
6. **ParentProcessId** String A pointer to the actual parent process if it's different from the creator process.

New Security Account Manager events

In Windows 10, new SAM events were added to cover SAM APIs that perform read/query operations. In previous versions of Windows, only write operations were audited. The new events are event ID 4798 and event ID 4799. The following APIs are now audited:

- SamrEnumerateGroupsInDomain
- SamrEnumerateUsersInDomain
- SamrEnumerateAliasesInDomain
- SamrGetAliasMembership
- SamrLookupNamesInDomain
- SamrLookupIdsInDomain
- SamrQueryInformationUser
- SamrQueryInformationGroup
- SamrQueryInformationUserAlias
- SamrGetMembersInGroup
- SamrGetMembersInAlias
- SamrGetUserDomainPasswordInformation

New BCD events

Event ID 4826 has been added to track the following changes to the Boot Configuration Database (BCD):

- DEP/NEX settings
- Test signing
- PCAT SB simulation
- Debug
- Boot debug
- Integrity Services
- Disable Winload debugging menu

New PNP events

Event ID 6416 has been added to track when an external device is detected through Plug and Play. One important scenario is if an external device that contains malware is inserted into a high-value machine that doesn't expect this type of action, such as a domain controller.

Learn how to manage your security audit policies within your organization.

Trusted Platform Module

New TPM features in Windows 10, version 1511

- Key Storage Providers (KSPs) and srvcrypt support elliptical curve cryptography (ECC).

New TPM features in Windows 10, version 1507

The following sections describe the new and changed functionality in the TPM for Windows 10:

- Device health attestation
- Microsoft Passport support
- Device Guard support
- Credential Guard support

Device health attestation

Device health attestation enables enterprises to establish trust based on hardware and software components of a managed device. With device health attestation, you can configure an MDM server to query a health attestation service that will allow or deny a managed device access to a secure resource. Some things that you can check on the device are:

- Is Data Execution Prevention supported and enabled?
- Is BitLocker Drive Encryption supported and enabled?
- Is SecureBoot supported and enabled?

> **Note** The device must be running Windows 10 and it must support at least TPM 2.0.

Learn how to deploy and manage TPM within your organization.

User Account Control

User Account Control (UAC) helps prevent malware from damaging a computer and helps organizations deploy a better-managed desktop environment.

You should not turn off UAC because this is not a supported scenario for devices running Windows 10. If you do turn off UAC, all Univeral Windows Platform apps stop working. You must always set the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA** registry value to 1. If you need to provide auto elevation for programmatic access or installation, you could set the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin** registry value to 0, which is the same as setting the UAC slider Never Notify. This is not recommended for devices running Windows 10.

For more info about how manage UAC, see UAC Group Policy Settings and Registry Key Settings.

In Windows 10, User Account Control has added some improvements.

New User Account Control features in Windows 10, version 1507

- **Integration with the Antimalware Scan Interface (AMSI)**. The AMSI scans all UAC elevation requests for malware. If malware is detected, the admin privilege is blocked.

Learn how to manage User Account Control within your organization.

VPN profile options

Windows 10 provides a set of VPN features that both increase enterprise security and provide an improved user

experience, including:

- Always-on auto connection behavior
- App=triggered VPN
- VPN traffic filters
- Lock down VPN
- Integration with Microsoft Passport for Work

Learn more about the VPN options in Windows 10.

Management

Windows 10 provides mobile device management (MDM) capabilities for PCs, laptops, tablets, and phones that enable enterprise-level management of corporate-owned and personal devices.

MDM support

MDM policies for Windows 10 align with the policies supported in Windows 8.1 and are expanded to address even more enterprise scenarios, such as managing multiple users who have Microsoft Azure Active Directory (Azure AD) accounts, full control over the Microsoft Store, VPN configuration, and more.

MDM support in Windows 10 is based on Open Mobile Alliance (OMA) Device Management (DM) protocol 1.2.1 specification.

Corporate-owned devices can be enrolled automatically for enterprises using Azure AD. Reference for Mobile device management for Windows 10

Unenrollment

When a person leaves your organization and you unenroll the user account or device from management, the enterprise-controlled configurations and apps are removed from the device. You can unenroll the device remotely or the person can unenroll by manually removing the account from the device.

When a personal device is unenrolled, the user's data and apps are untouched, while enterprise information such as certificates, VPN profiles, and enterprise apps are removed.

Infrastructure

Enterprises have the following identity and management choices.

AREA	CHOICES
Identity	Active Directory; Azure AD
Grouping	Domain join; Workgroup; Azure AD join
Device management	Group Policy; System Center Configuration Manager; Microsoft Intune; other MDM solutions; Exchange ActiveSync; Windows PowerShell; Windows Management Instrumentation (WMI)

> **Note** With the release of Windows Server 2012 R2, Network Access Protection (NAP) was deprecated and the NAP client has now been removed in Windows 10. For more information about support lifecycles, see Microsoft Support Lifecycle.

Device lockdown

Do you need a computer that can only do one thing? For example:

- A device in the lobby that customers can use to view your product catalog.
- A portable device that drivers can use to check a route on a map.
- A device that a temporary worker uses to enter data.

You can configure a persistent locked down state to create a kiosk-type device. When the locked-down account is logged on, the device displays only the app that you select.

You can also configure a lockdown state that takes effect when a given user account logs on. The lockdown restricts the user to only the apps that you specify.

Lockdown settings can also be configured for device look and feel, such as a theme or a custom layout on the Start screen.

Customized Start layout

A standard, customized Start layout can be useful on devices that are common to multiple users and devices that are locked down for specialized purposes. Starting in Windows 10, version 1511, administrators can configure a *partial* Start layout, which applies specified tile groups while allowing users to create and customize their own tile groups. Learn how to customize and export Start layout.

Administrators can also use mobile device management (MDM) or Group Policy to disable the use of Windows Spotlight on the lock screen.

Microsoft Store for Business

New in Windows 10, version 1511

With the Microsoft Store for Business, organizations can make volume purchases of Windows apps. The Store for Business provides app purchases based on organizational identity, flexible distribution options, and the ability to reclaim or re-use licenses. Organizations can also use the Store for Business to create a private store for their employees that includes apps from the Store, as well private Line-of-Business (LOB) apps.

For more information, see Microsoft Store for Business overview.

Updates

Windows Update for Business enables information technology administrators to keep the Windows 10-based devices in their organization always up to date with the latest security defenses and Windows features by directly connecting these systems to Microsoft's Windows Update service.

By using Group Policy Objects, Windows Update for Business is an easily established and implemented system which enables organizations and administrators to exercise control on how their Windows 10-based devices are updated, by allowing:

- **Deployment and validation groups**; where administrators can specify which devices go first in an update wave, and which devices will come later (to ensure any quality bars are met).
- **Peer-to-peer delivery**, which administrators can enable to make delivery of updates to branch offices and remote sites with limited bandwidth very efficient.
- **Use with existing tools** such as System Center Configuration Manager and the Enterprise Mobility Suite.

Together, these Windows Update for Business features help reduce device management costs, provide controls over update deployment, offer quicker access to security updates, as well as provide access to the latest innovations from Microsoft on an ongoing basis. Windows Update for Business is a free service for all Windows 10 Pro, Enterprise, and Education editions, and can be used independent of, or in conjunction with, existing device management solutions such as Windows Server Update Services (WSUS) and System Center Configuration Manager.

Learn more about Windows Update for Business.

For more information about updating Windows 10, see Windows 10 servicing options for updates and upgrades.

Microsoft Edge

Microsoft Edge takes you beyond just browsing to actively engaging with the web through features like Web Note, Reading View, and Cortana.

- **Web Note.** Microsoft Edge lets you annotate, highlight, and call things out directly on webpages.
- **Reading view.** Microsoft Edge lets you enjoy and print online articles in a distraction-free layout that's optimized for your screen size. While in reading view, you can also save webpages or PDF files to your reading list, for later viewing.
- **Cortana.** Cortana is automatically enabled on Microsoft Edge. Microsoft Edge lets you highlight words for more info and gives you one-click access to things like restaurant reservations and reviews, without leaving the webpage.
- **Compatibility and security.** Microsoft Edge lets you continue to use IE11 for sites that are on your corporate intranet or that are included on your Enterprise Mode Site List. You must use IE11 to run older, less secure technology, such as ActiveX controls.

Enterprise guidance

Microsoft Edge is the default browser experience for Windows 10 and Windows 10 Mobile. However, if you're running web apps that need ActiveX controls, we recommend that you continue to use Internet Explorer 11 for them. If you don't have IE11 installed anymore, you can download it from the Microsoft Store or from the Internet Explorer 11 download page.

We also recommend that you upgrade to IE11 if you're running any earlier versions of Internet Explorer. IE11 is supported on Windows 7, Windows 8.1, and Windows 10. So any legacy apps that work with IE11 will continue to work even as you migrate to Windows 10.

Learn more about using Microsoft Edge in the enterprise

Learn more

- Windows 10 release information