What's new in Windows

Find out about new features and capabilities in the latest release of Windows client for IT professionals.

Windows 11 planning

OVERVIEW

Windows 11 overview

Windows 11 requirements

Plan for Windows 11

Prepare for Windows 11

Windows commercial licensing overview

Windows 11

WHAT'S NEW

What's new in Windows 11, version 24H2

What's new in Windows 11, version 23H2

What's new in Windows 11, version 22H2

Windows 10

WHAT'S NEW

Extended Security Updates (ESU) program for Windows 10

What's new in Windows 10, version 22H2

Windows Enterprise LTSC

WHAT'S NEW

Windows Enterprise LTSC overview

What's new in Windows 11 Enterprise LTSC 2024

What's new in Windows 10 Enterprise LTSC 2021

What's new in Windows 10 Enterprise LTSC 2019

What's new in Windows 10 Enterprise LTSC 2016

What's new in Windows 10 Enterprise LTSC 2015

Deprecated features

REFERENCE

Windows features we're no longer developing

Features and functionality removed in Windows

Lifecycle terminology

Learn more

OVERVIEW

Windows 11 release information

Windows release health dashboard

Compare Windows 11 Editions

Windows 11 overview

Article • 03/27/2025 • Applies to: ✅ Windows 11

Windows 11 is a client operating system and includes features that organizations should know about. Windows 11 is built on the same foundation as Windows 10. If you use Windows 10, then Windows 11 is a natural transition. It's an update to what you know, and what you're familiar with.

Windows 11 offers innovations focused on enhancing end-user productivity, and is designed to support today's hybrid work environment.

Your investments in updates and device management are carried forward. For example, many of the same apps and tools can be used in Windows 11. Many of the same security settings and policies can be applied to Windows 11 devices, including PCs. You can use Windows Autopilot with a zero touch deployment to enroll your Windows devices in Microsoft Intune. You can also use newer features, such as Azure Virtual Desktop and Windows 365 on your Windows 11 devices.

This article lists what's new, and some of the features & improvements. For more information on what's new for OEMs, see What's new in manufacturing, customization, and design.

> **Tip**
>
> If you'd like to know what's coming to Windows, check out the **Windows Roadmap**. The roadmap is a high-level overview of the features and functionality that are planned for future releases of Windows.

Security and scanning

The security and privacy features in Windows 11 are similar to Windows 10. Security for your devices starts with the hardware, and includes OS security, application security, and user & identity security. There are features available in the Windows OS to help in these areas. This section describes some of these features. For a more comprehensive view, including zero trust, see Windows security.

- The **Windows Security** app is built into the OS. This app is an easy-to-use interface, and combines commonly used security features. For example, your get access to virus & threat protection, firewall & network protection, account protection, and more.

For more information, see the Windows Security app.

- **Security baselines** includes security settings that already configured, and ready to be deployed to your devices. If you don't know where to start, or it's too time consuming to go through all the settings, then you should look at Security Baselines.

  For more information, see Windows security baselines.

- **Microsoft Defender Antivirus** is built into Windows, and helps protect devices using next-generation security. When used with Microsoft Defender for Endpoint, your organization gets strong endpoint protection, and advanced endpoint protection & response. If you use Intune to manage devices, then you can create policies based on threat levels in Microsoft Defender for Endpoint.

  For more information, see:
  - Microsoft Defender Antivirus
  - Microsoft Defender for Endpoint
  - Enforce compliance for Microsoft Defender for Endpoint

- The application security features help prevent unwanted or malicious code from running, isolate untrusted websites & untrusted Office files, protect against phishing or malware websites, and more.

  For more information, see Windows application security.

- **Windows Hello for Business** helps protect users and identities. It replaces passwords, and uses a PIN or biometric that stays locally on the device. Device manufacturers are including more secure hardware features, such as IR cameras and TPM chips. These features are used with Windows Hello for Business to help protect user identities on your organization devices.

  As an admin, going passwordless help secures user identities. The Windows OS, Microsoft Entra ID, and Intune work together to remove passwords, create more secure policies, and help enforce compliance.

  For more information, see:
  - Windows Hello for Business Overview
  - Trusted Platform Module Technology Overview
  - Integrate Windows Hello for Business with Intune

For more information on the security features you can configure, manage, and enforce using Intune, see Protect data and devices with Microsoft Intune.

Easier access to new services, and services you already use

- **Windows 365** is a desktop operating system that's also a cloud service. From another internet-connected device, including Android and macOS devices, you can run Windows 365, just like a virtual machine.

  For more information, see What is Windows 365 Enterprise?.

- **Microsoft 365 Apps** can be installed on Windows 11 clients using the device management tools you're already familiar with:
  - What is Intune?
  - Add Microsoft 365 apps to Windows 10 devices with Microsoft Intune
  - What is Microsoft Configuration Manager?
  - Deploy Microsoft 365 Apps with Microsoft Configuration Manager

- **Power Automate for desktop** allows your users to create flows in a low-code app to help them with everyday tasks. For example, users can create flows that save a message to OneNote, notify a team when there's a new Forms response, get notified when a file is added to SharePoint, and more.

  For more information, see Getting started with Power Automate in Windows 11.

Customize the desktop experience

- **Snap Layouts, Snap Groups**: When you open an app, hover your mouse over the minimize or maximize option. When you do, you can select a different layout for the app:

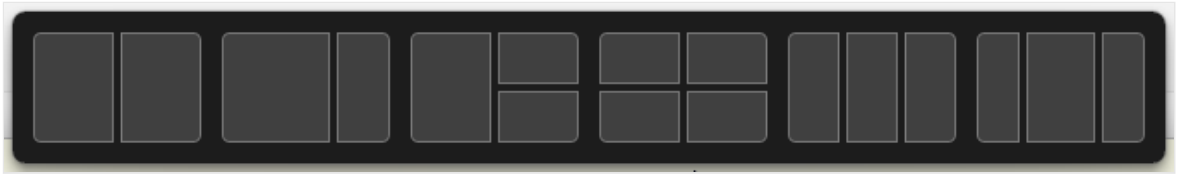
  This feature allows users to customize the sizes of apps on their desktop. And, when you add other apps to the layout, the snapped layout stays in place.

When you add your apps in a Snap Layout, that layout is saved in a Snap Group. In the taskbar, when you hover over an app in an existing snap layout, it shows all the apps in that layout. This feature is the Snap Group. You can select the group, and the apps are opened in the same layout. As you add more Snap Groups, you can switch between them just by selecting the Snap Group.

Users can manage some snap features using the **Settings** app > **System** > **Multitasking**. For more information on the end-user experience, see Snap your windows.

You can also add Snap Layouts to apps your organization creates. For more information, see Support snap layouts for desktop apps on Windows 11.

Starting in Windows 11, version 22H2, you can also activate snap layouts by dragging a window to the top of the screen. The feature is available for both mouse and touch.



For more information on the end-user experience, see Snap your windows.

- **Start menu**: The Start menu includes some apps that are pinned by default. You can customize the Start menu layout by pinning (and unpinning) the apps you want. For example, you can pin commonly used apps in your organization, such as Outlook, Microsoft Teams, apps your organization creates, and more.

  Using policy, you can deploy your customized Start menu layout to devices in your organization. For more information, see Customize the Start menu layout on Windows 11.

  Users can manage some Start menu features using the **Settings** app > **Personalization**. For more information on the end-user experience, see See what's on the Start menu.

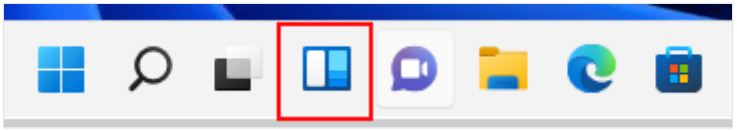
- **Taskbar**: You can also pin (and unpin) apps on the Taskbar. For example, you can pin commonly used apps in your organization, such as Outlook, Microsoft Teams, apps your organization creates, and more.

  Using policy, you can deploy your customized Taskbar to devices in your organization. For more information, see Customize the Taskbar on Windows 11.

Users can manage some Taskbar features using the **Settings** app > **Personalization**. For more information on the end-user experience, see:

- Customize the taskbar notification area
- Pin apps and folders to the desktop or taskbar

- **Widgets**: Widgets are available on the Taskbar. It includes a personalized feed that could be weather, calendar, stock prices, news, and more:

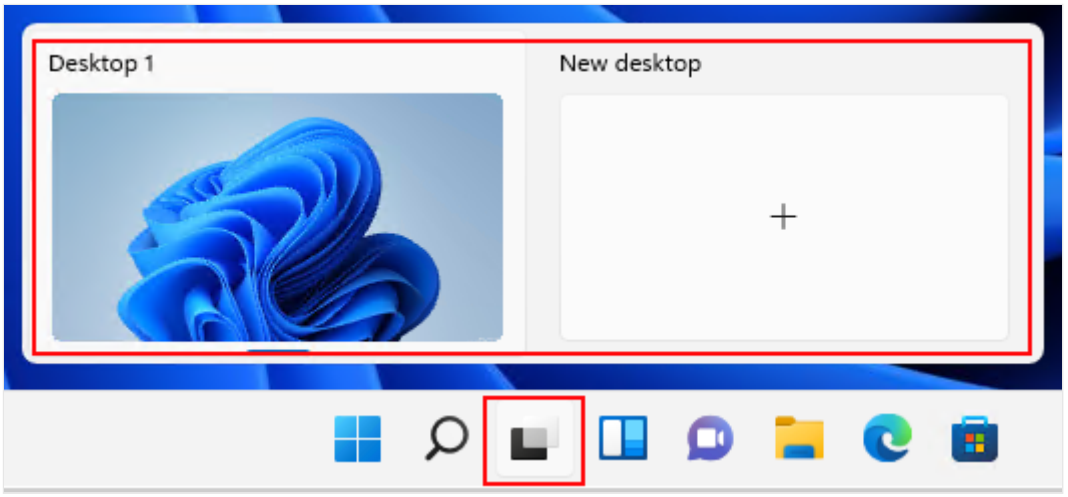


You can enable or disable this feature using the following policy:

- **Group Policy**: Computer Configuration\Administrative Templates\Windows Components\widgets
- **MDM**: ./Device/Vendor/MSFT/Policy/Config/NewsAndInterests/AllowNewsAndInterests

For information on the end-user experience, see Stay up to date with widgets.

- **Virtual desktops**: On the Taskbar, you can select the Desktops icon to create a new desktop:



Use the desktop to open different apps depending on what you're doing. For example, you can create a Travel desktop that includes web sites and apps that are focused on travel.

Using policy, you can deploy a customized Taskbar to devices in your organization. For more information, see Customize the Taskbar on Windows 11.

Users can manage some desktop features using **Settings** app > **System** > **Multitasking**. For more information on the end-user experience, see Multiple desktops in Windows.

Use your same apps, and new apps, improved

- Starting with Windows 11, users in the Windows Insider program can download and install **Android™ apps** from the Microsoft Store. This feature is called the **Windows Subsystem for Android**, and allows users to use Android apps on their Windows devices, similar to other apps installed from the Microsoft Store.

  Users open the Microsoft Store, install the **Amazon Appstore** app, and sign in with their Amazon account. When they sign in, they can search, download, and install Android apps.

  For more information, see:
  - Windows Subsystem for Android
  - Windows Subsystem for Android developer information

- Your Windows 10 apps also work on Windows 11. **App Assure** is also available if there are some issues.

  You can continue to use **MSIX packages** for your UWP, Win32, WPF, and WinForm desktop application files. Continue to use **Windows Package Manager** to install Windows apps. You can create **Azure virtual desktops** that run Windows 11. Use **Azure Virtual desktop with MSIX app attach** to virtualize desktops and apps. For more information on these features, see Overview of apps on Windows client devices.

  In the **Settings** app > **Apps**, users can manage some of the app settings. For example, they can get apps anywhere, but let the user know if there's a comparable app in the Microsoft Store. They can also choose which apps start when they sign in.

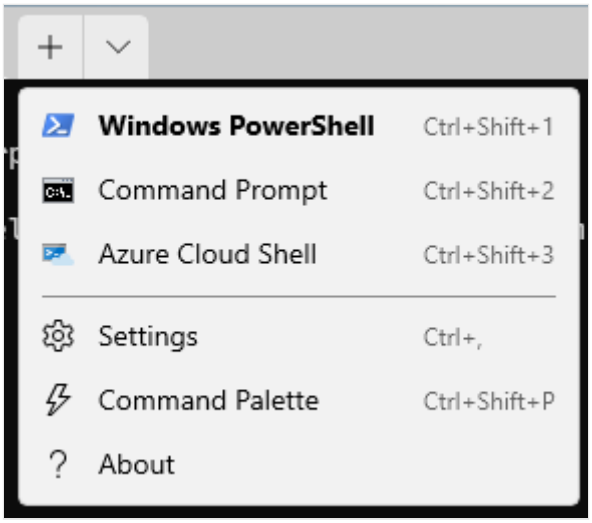
  Using an MDM provider, like Intune, you can create policies that also manage some app settings. For a list of settings, see App Store in Intune.

- If you manage devices using Intune, then you might be familiar with the **Company Portal app**. Starting with Windows 11, the Company Portal is your private app repository for your organization apps. For more information, see Private app repository in Windows 11.

  For public and retail apps, continue using the Microsoft Store.

- **Windows Terminal app**: This app is included with the OS. On previous Windows versions, it's a separate download in the Microsoft Store. For more information, see What is Windows Terminal?.

This app combines Windows PowerShell, a command prompt, and Azure Cloud Shell all within the same terminal window. You don't need to open separate apps to use these command-line applications. It has tabs. When you open a new tab, you can choose your command-line application:



If users or groups in your organization do a lot with Windows PowerShell or the command prompt, then use policy to add the Windows Terminal app to the Start menu layout or the Taskbar.

Users can also search for the Terminal app, right-select the app, and pin the app to the Start menu and taskbar.

- The **Microsoft Store** has a new look, and includes more public and retail apps. For more information on the end-user experience, see:
  - Get updates for apps and games in Microsoft Store
  - How to open Microsoft Store on Windows

- The **Microsoft Edge** browser is included with the OS. Internet Explorer (IE) isn't available in Windows 11. In Microsoft Edge, you can use IE Mode if a website needs Internet Explorer. Open Microsoft Edge, and enter `edge://settings/defaultBrowser` in the URL.

  To save system resources, Microsoft Edge uses sleeping tabs. Users can configure these settings, and more, in `edge://settings/system`.

  Using Group Policy or an MDM provider, such as Intune, you can configure some Microsoft Edge settings. For more information, see Microsoft Edge - Policies and Configure Microsoft Edge policy settings.

Deployment and servicing

- **Install Windows 11**: The same methods you use to install Windows 10 can also be used to install Windows 11. For example, you can deploy Windows to your devices using Windows Autopilot, Configuration Manager, and other methods. Windows 11 is delivered as an upgrade to eligible devices running Windows 10.

  For more information on getting started, see Windows client deployment resources and documentation and Plan for Windows 11.

  For more information on the end-user experience, see Ways to install Windows 11.

- **Windows Autopilot**: If you're purchasing new devices, you can use Windows Autopilot to set up and preconfigure the devices. When users get the device, they sign in with their organization account (`user@contoso.com`). In the background, Autopilot gets them ready for use, and deploys any apps or policies you set. You can also use Windows Autopilot to reset, repurpose, and recover devices. Autopilot offers zero touch deployment for admins.

  If you have a global or remote workforce, then Autopilot might be the right option to install the OS, and get it ready for use. For more information, see Overview of Windows Autopilot.

- **Microsoft Intune** is a mobile application management (MAM) and mobile device management (MDM) provider. It helps manage devices, and manage apps on devices in your organization. You configure policies, and then deploy these policies to users and groups. You can create and deploy policies that install apps, configure device features, enforce PIN requirements, block compromised devices, and more.

  If you use Group Policy to manage your Windows 10 devices, then you can also use Group Policy to manage Windows 11 devices. In Intune, there are administrative templates and the settings catalog that include many of the same policies. Group Policy analytics analyze your on-premises group policy objects.

- **Windows Updates and Delivery optimization** helps manage updates, and manage features on your devices. Starting with Windows 11, the OS feature updates are installed annually. For more information on servicing channels, and what they are, see Servicing channels.

  Like Windows 10, Windows 11 receives monthly quality updates.

  You have options to install updates on your Windows devices, including Intune, Group Policy, Windows Server Update Services (WSUS), and more. For more information, see Assign devices to servicing channels.

Some updates are large, and use bandwidth. Delivery optimization helps reduce bandwidth consumption. It shares the work of downloading the update packages with multiple devices in your deployment. Windows 11 updates are smaller, as they only pull down source files that are different. You can create policies that configure delivery optimization settings. For example, set the maximum upload and download bandwidth, set caching sizes, and more.

For more information, see Delivery Optimization for Windows updates.

For more information on the end-user experience, see:

- Installation & updates
- Manage updates in Windows

Education and apps

Windows 11 SE is a new edition of Windows designed for education. It runs on low-cost devices, and runs essential apps, including Microsoft 365. For more information, see Windows 11 SE for Education.

Next steps

- Windows 11 requirements
- Plan for Windows 11
- Prepare for Windows 11
- Windows release health

Feedback

Windows 11 requirements

Article • 03/13/2024 • Applies to: ✅ Windows 11

This article lists the system requirements for Windows 11. Windows 11 is also supported on a virtual machine (VM).

Hardware requirements

To install or upgrade to Windows 11, devices must meet the following minimum hardware requirements:

- **Processor**: 1 gigahertz (GHz) or faster with two or more cores on a compatible 64-bit processor or system on a chip (SoC).
- **Memory**: 4 gigabytes (GB) or greater.
- **Storage**: 64 GB or greater available disk space.

  > ⓘ **Note**
  >
  > There might be more storage requirements over time for updates, and to enable specific features within the OS. For more information, see Windows 11 specifications.

- **Graphics card**: Compatible with DirectX 12 or later, with a WDDM 2.0 driver.
- **System firmware**: UEFI, Secure Boot capable.
- **TPM**: Trusted Platform Module (TPM) version 2.0.
- **Display**: High definition (720p) display, 9" or greater monitor, 8 bits per color channel.
- **Internet connection**: Internet connectivity is necessary to perform updates, and to download and use some features.
  - Windows 11 Home edition requires an internet connection and a Microsoft Account to complete device setup on first use.

For more information, see the following Windows Insider blog post: Update on Windows 11 minimum system requirements.

For more information about tools to evaluate readiness, see Determine eligibility.

OS requirements

To upgrade directly to Windows 11, eligible Windows 10 devices must meet both of the following criteria:

- Running Windows 10, version 2004 or later.
- Installed the September 14, 2021 security update or later.

> **Note**
>
> - S mode is only supported on the Home edition of Windows 11.
> - If you're running a different edition of Windows in S mode, before upgrading to Windows 11, first switch out of S mode.
> - To switch a device out of Windows 10 in S mode also requires internet connectivity. If you switch out of S mode, you can't switch back to S mode later.

Feature-specific requirements

Some features in Windows 11 have requirements beyond the minimum hardware requirements.

- **5G support**: requires 5G capable modem.
- **Auto HDR**: requires an HDR monitor.
- **BitLocker to Go**: requires a USB flash drive. This feature is available in Windows Pro and above editions.
- **Client Hyper-V**: requires a processor with second-level address translation (SLAT) capabilities. This feature is available in Windows Pro editions and greater.
- **DirectStorage**: requires an NVMe SSD to store and run games that use the Standard NVM Express Controller driver and a DirectX12 GPU with Shader Model 6.0 support.
- **DirectX 12 Ultimate**: available with supported games and graphics chips.
- **Presence**: requires sensor that can detect human distance from device or intent to interact with device.
- **Intelligent Video Conferencing**: requires video camera, microphone, and speaker (audio output).
- **Multiple Voice Assistant**: requires a microphone and speaker.
- **Snap**: three-column layouts require a screen that is 1920 effective pixels or greater in width.

- **Mute** and **unmute**: from Taskbar requires video camera, microphone, and speaker (audio output). App must be compatible with feature to enable global mute/unmute.
- **Spatial Sound**: requires supporting hardware and software.
- **Microsoft Teams**: requires video camera, microphone, and speaker (audio output).
- **Touch**: requires a screen or monitor that supports multi-touch.
- **Two-factor authentication**: requires use of PIN, biometric (fingerprint reader or illuminated infrared camera), or a phone with Wi-Fi or Bluetooth capabilities.
- **Voice Typing**: requires a PC with a microphone.
- **Wake on Voice**: requires Modern Standby power model and microphone.
- **Wi-Fi 6E**: requires new WLAN IHV hardware and driver and a Wi-Fi 6E capable AP/router.
- **Windows Hello**: requires a camera configured for near infrared (IR) imaging or fingerprint reader for biometric authentication. Devices without biometric sensors can use Windows Hello with a PIN or portable Microsoft compatible security key. For more information, see IT tools to support Windows 10, version 21H1.
- **Windows Projection**: requires a display adapter that supports Windows Display Driver Model (WDDM) 2.0 and a Wi-Fi adapter that supports Wi-Fi Direct.
- **Xbox app**: requires an Xbox Live account, which isn't available in all regions. Go to the Xbox Live *Countries and Regions* page for the most up-to-date information on availability. Some features in the Xbox app require an active Xbox Game Pass subscription.

Virtual machine support

The following configuration requirements apply to VMs running Windows 11.

- **Generation**: 2

  > **Note**
  >
  > In-place upgrade of existing generation 1 VMs to Windows 11 isn't possible.

- **Storage**: 64 GB or greater disk space.

- **Security**:

  - **Azure**: Trusted launch with vTPM enabled.

  - **Hyper-V**: Secure boot and TPM enabled.
    - General settings: Secure boot capable, virtual TPM enabled.

- **Memory**: 4 GB or greater.
- **Processor**: Two or more virtual processors.
  - The VM host processor must also meet Windows 11 processor requirements.

    > **Note**
    >
    > There may be some instances where this requirement for the VM host doesn't apply. For more information, see Options for using Windows 11 with Mac computers.

  - Procedures to configure required VM settings depend on the VM host type. For example, VM hosts running Hyper-V, virtualization (VT-x, VT-d) must be enabled in the BIOS. Virtual TPM 2.0 is emulated in the guest VM independent of the Hyper-V host TPM presence or version.

Next steps

- What's new in Windows 11
- Plan for Windows 11
- Prepare for Windows 11
- Windows minimum hardware requirements

Feedback

Plan for Windows 11

Article • 03/27/2025 • Applies to: ✅ Windows 11

This article provides guidance to help you plan for Windows 11 in your organization.

Deployment planning

Since Windows 11 is built on the same foundation as Windows 10, you can use the same deployment capabilities, scenarios, and tools. You can also use the same basic deployment strategy that you use today for Windows 10. Make sure that you review and update your servicing strategy to adjust for changes in servicing and support for Windows 11.

At a high level, this strategy should include the following steps:

- Create a deployment plan
- Define readiness criteria
- Evaluate infrastructure and tools
- Test applications
- Define your servicing strategy

If you're looking for ways to optimize your approach to deploying Windows 11, or if deploying a new version of Windows isn't a familiar process for you, consider the factors in the following sections.

Determine eligibility

As a first step, determine which of your current devices meet the Windows 11 hardware requirements. To ensure compatibility, verify that your device meets or exceeds Windows 11 requirements.

Microsoft has analysis tools to help you evaluate your devices against the Windows 11 hardware requirements. If you're running Windows 10 Home, Pro, or Pro for Workstations editions, you can use the PC Health Check app to determine Windows 11 eligibility. Users running Windows 10 Enterprise and Education editions should rely on their IT administrators to let them know when they're eligible for the upgrade.

Enterprise organizations looking to evaluate device readiness in their environments can expect this capability to be integrated into existing Microsoft tools, such as Endpoint analytics.

Windows 11 availability

The availability of Windows 11 varies according to a device's hardware and whether the device receives updates directly from Microsoft, or from a management solution that's maintained by an IT administrator.

For more information, see Defining Windows update-managed devices.

Managed devices

Managed devices are devices that are under organizational control. Managed devices include those devices managed by Microsoft Intune, Microsoft Configuration Manager, or other endpoint management solutions.

If you manage devices on behalf of your organization, you can upgrade eligible devices to Windows 11 using your existing deployment and management tools.

Organizations that use Windows Update client policies also have the following benefits:

- Ensuring that devices that don't meet the minimum hardware requirements aren't automatically offered the Windows 11 upgrade.
- More insight into safeguard holds. While safeguard holds function for Windows 11 devices just as they do for Windows 10 today, administrators using Windows Update client policies have access to information on which safeguard holds are preventing individual devices from taking the upgrade to Windows 11.

> **Note**
>
> Also, Windows 11 has new Microsoft Software License Terms. If you deploy with Windows Update client policies or Windows Server Update Services, you accept these new license terms on behalf of the users in your organization.

Unmanaged devices

Unmanaged devices are devices that an IT administrator doesn't manage on behalf of an organization. For OS deployment, these devices aren't subject to organizational policies that manage upgrades or updates.

Windows 11 was offered to eligible Windows 10 devices in 2021. Messaging on new devices varies by PC manufacturer.

The Windows 11 upgrade is available on eligible, unmanaged devices to users who manually seek the upgrade through Windows Update. As with all Windows Update-managed devices, the **Windows Update** settings page confirms when a device is eligible.

Just like Windows 10, the machine learning-based intelligent rollout process is used when rolling out upgrades. Machine learning uses a combination of testing, close partner engagement, feedback, diagnostic data, and real-life insights to manage quality. This process improves the update experience and ensures that devices first nominated for updates are the devices likely to have a seamless experience. Devices that might have compatibility issues with the upgrade get the benefit of resolving these issues before the upgrade is offered.

Windows 11 readiness considerations

The recommended method to determine if your infrastructure, deployment processes, and management tools are ready for Windows 11 is to join the Windows Insider Program for Business. As a participant in the release preview channel, you can validate that your devices and applications work as expected, and explore new features.

As you plan your endpoint management strategy for Windows 11, consider moving to cloud-based mobile device management (MDM), such as Microsoft Intune. If a cloud-only approach isn't right for your organization yet, you can still modernize and streamline essential pieces of your endpoint management strategy as follows:

- To manage Configuration Manager clients over the internet, create a cloud management gateway (CMG).
- Attach your existing Configuration Management estate to the cloud with tenant attach so you can manage all devices from within the Microsoft Intune admin center.
- Use co-management to concurrently manage devices using both Configuration Manager and Microsoft Intune. This concurrent management allows you to take advantage of cloud-powered capabilities like conditional access.

For more information on the benefits of these approaches, see Cloud Attach Your Future: The Big 3.

The introduction of Windows 11 is also a good time to review your hardware refresh plans and prioritize eligible devices to ensure an optimal experience for your users.

Servicing and support

Along with user experience and security improvements, Windows 11 introduces enhancements to Microsoft's servicing approach based on your suggestions and feedback.

- **Quality updates**: Windows 11 and Windows 10 devices receive regular monthly quality updates to provide security updates and bug fixes.
- **Feature updates**: Microsoft provides a single Windows 11 feature update annually, targeted for release in the second half of each calendar year.
- **Lifecycle**:
  - Home, Pro, Pro for Workstations, and Pro for Education editions of Windows 11 receive 24 months of support from the general availability date.
  - Enterprise and Education editions of Windows 11 are supported for 36 months from the general availability date.

A consolidated Windows 11 update history is available. Similarly, the Windows release health hub offers quick access to Windows 11 servicing announcements, known issues, and safeguard holds.

It's important that organizations have adequate time to plan for Windows 11. Microsoft also recognizes that many organizations have a mix of Windows 11 and Windows 10 devices across their ecosystem. Devices on in-service versions of Windows 10 continue to receive monthly Windows 10 security updates, and incremental improvements to Windows 10 to support ongoing Microsoft 365 deployments. For more information, see the Windows 10 release information page.

> **Tip**
>
> If you'd like to know what's coming to Windows, check out the **Windows Roadmap**. The roadmap is a high-level overview of the features and functionality that are planned for future releases of Windows.

Application compatibility

Microsoft's compatibility promise for Windows 10 is maintained for Windows 11. Data from the App Assure program shows that Windows 10 compatibility rates are over 99.7% for enterprise organizations, including line of business (LOB) apps. Microsoft remains committed to ensuring that the apps you rely upon continue to work as expected when you upgrade. Windows 11 is subject to the same app compatibility

validation requirements that are in place for Windows 10 today, for both feature and quality updates.

For more information, see Windows compatibility cookbook.

App Assure

If you run into compatibility issues or want to ensure that your organization's applications are compatible from day one, App Assure can help. With enrollment in the App Assure service, any app compatibility issues that you find with Windows 11 can be resolved. Microsoft helps you remedy application issues at no cost. Since 2018, App Assure has evaluated almost 800,000 apps, and subscriptions are free for eligible customers with more than 150 devices.

Next steps

Prepare for Windows 11

Plan to deploy updates for Windows 10 and Microsoft 365 Apps

Feedback

Was this page helpful? Yes No

Provide product feedback

Prepare for Windows 11

Article • 07/17/2024 • Applies to: ✅ Windows 11, ✅ Windows 10

Windows 10 and Windows 11 are designed to coexist so that you can use the same familiar tools and processes to manage both operating systems. Using a single management infrastructure that supports common applications across both Windows 10 and Windows 11 helps to simplify the migration process. You can analyze endpoints, determine application compatibility, and manage Windows 11 deployments in the same way that you do with Windows 10.

After you evaluate your hardware to see if it meets requirements for Windows 11, it's a good time to review your deployment infrastructure, tools, and overall endpoint and update management processes. Use this review time to look for opportunities to simplify and optimize. This article provides some helpful guidance to accomplish these tasks.

Infrastructure and tools

The tools that you use for core workloads during Windows 10 deployments can still be used for Windows 11.

> ⓘ **Important**
>
> Be sure to check with the providers of any non-Microsoft solutions that you use. Verify compatibility of these tools with Windows 11, particularly if they provide security or data loss prevention capabilities.

On-premises solutions

- If you use Windows Server Update Services (WSUS), you need to sync the Windows 11 product category. After you sync the product category, you'll see Windows 11 offered as an option. If you want to validate Windows 11 builds before their broad release, you can also sync the **Windows Insider Pre-release** category.

  > ⓘ **Note**

During deployment, you'll be prompted to agree to the Microsoft Software License Terms on behalf of your users. Additionally, you won't see an x86 option because Windows 11 isn't supported on 32-bit architecture.

- If you use Microsoft Configuration Manager, you can sync the **Windows 11** product category and begin upgrading eligible devices. If you want to validate Windows 11 builds before their broad release, you can also sync the **Windows Insider Pre-release** category.

  > ⓘ **Note**
  >
  > Configuration Manager will prompt you to accept the Microsoft Software License Terms on behalf of the users in your organization.

Cloud-based solutions

- If you use Windows Update client policies policies, you need to use the **Target Version** capability. This option is either through policy or Windows Autopatch. You need to use this option instead of only using feature update deferrals to upgrade from Windows 10 to Windows 11. Feature update deferrals are great for moving to newer versions of your current product. For example, Windows 10, version 21H2 to version 22H2. They don't automatically move devices between products, for example Windows 10 to Windows 11.

  - If you use Microsoft Intune and have a Microsoft 365 E3 license, use the feature update deployments page to select the latest version of Windows 11 and upgrade Windows 10 devices to Windows 11. You can also continue using the same update experience controls to manage Windows 10 and Windows 11 on the **Update Rings** page in Intune. If you aren't ready to move to Windows 11, keep the feature update version set at the version you're currently on. When you're ready to start upgrading devices, change the feature update deployment setting to specify Windows 11.

  - In group policy, **Select target Feature Update version** has two entry fields: **Product Version** and **Target Version**.

  - The product field must specify Windows 11 in order for devices to upgrade to Windows 11. If only the target version field is configured, the service offers the device matching versions of the same product.

- Quality update deferrals continue to work the same across both Windows 10 and Windows 11. This behavior is true regardless of which management tool you use to configure Windows Update client policies.

  > ⓘ **Note**
  >
  > Endpoints managed by Windows Update client policies don't automatically upgrade to Windows 11 unless an administrator explicitly configures a **Target Version** using the TargetReleaseVersion setting using a Windows CSP, a feature update profile in Intune, or the Select target Feature Update version setting group policy.

Cloud-based management

The cloud-based management capabilities of the Microsoft Intune family of products help consolidate device management and endpoint security into a single platform. Microsoft Intune also supports the diverse bring-your-own-device (BYOD) ecosystem that's common with hybrid work scenarios. It can also enable you to track your progress against compliance and business objectives while protecting user data.

The following are some common use cases and the corresponding Microsoft Intune capabilities that support them:

- **Provision and pre-configure new Windows 11 devices**: Windows Autopilot enables you to deploy new Windows 11 devices in a business-ready state that includes your desired applications, settings, and policies. It can also be used to change the edition of Windows. For example, you can upgrade from Professional to Enterprise edition and gain the use of advanced features.

- **Configure rules and control settings for users, apps, and devices**: When you enroll devices in Microsoft Intune, you have full control over apps, settings, features, and security for both Windows 11 and Windows 10. You can also use app protection policies to require multifactor authentication (MFA) for specific apps.

- **Streamline device management for frontline, remote, and onsite workers**: Cloud configuration is a standard, easy-to-manage, device configuration that is cloud-optimized for users with specific workflow needs. You can use Microsoft Intune to deploy it to devices running the Pro, Enterprise, and Education editions of Windows 11.

If you're exclusively using an on-premises device management solution like Configuration Manager, you can still use the cloud management gateway, enable tenant attach, or enable co-management with Microsoft Intune. These solutions can make it easier to keep devices secure and up-to-date.

Review servicing approach and policies

Every organization transitions to Windows 11 at its own pace. Microsoft is committed to supporting you through your migration to Windows 11, whether you're a fast adopter or will make the transition over the coming months or years.

When you think of OS updates as an ongoing process, you improve your ability to deploy updates. This approach enables you to stay current with less effort, and less effect on productivity. To begin, think about how you roll out Windows feature updates today: which devices, and at what pace.

Next, craft a deployment plan for Windows 11 that includes deployment groups, rings, users, or devices. There are no absolute rules for exactly how many rings to have for your deployments, but the following example is a common structure:

- Preview (first or canary): Planning and development
- Limited (fast or early adopters): Pilot and validation
- Broad (users or critical): Wide deployment

For more information, see Create a deployment plan.

Review policies

Review deployment-related policies, and take into consideration your organization's security objectives, update compliance deadlines, and device activity. Apply changes where you can gain a clear improvement, particularly regarding the speed of the update process or security.

Validate apps and infrastructure

To validate that your apps, infrastructure, and deployment processes are ready for Windows 11, join the Windows Insider Program for Business. Then opt into the Release Preview Channel.

If you use Windows Server Update Services (WSUS), you can deploy directly from the Windows Insider Prerelease category using one of the following processes:

- Set **Manage Preview Builds** to **Release Preview** in Windows Update client policies.
- Use Azure Virtual Desktop and Azure Marketplace images.
- Download and deploy ISOs from Microsoft's Windows Insider Program ISO download page.

Regardless of the method you choose, you have the benefit of free Microsoft support when validating prerelease builds. Free support is available to any commercial customer deploying Windows 10 or Windows 11 Preview Builds, once they become available through the Windows Insider Program.

Analytics and assessment tools

If you use Microsoft Intune and have onboarded devices to Endpoint analytics, you have access to a hardware readiness assessment. This tool enables you to quickly identify which of your managed devices are eligible for the Windows 11 upgrade.

Prepare a pilot deployment

A pilot deployment is a proof of concept that rolls out an upgrade to a select number of devices in production, before deploying it broadly across the organization.

At a high level, the tasks involved are:

1. Assign a group of users or devices to receive the upgrade.
2. Implement baseline updates.
3. Implement operational updates.
4. Validate the deployment process.
5. Deploy the upgrade to devices.
6. Test and support the pilot devices.
7. Determine broad deployment readiness based on the results of the pilot.

User readiness

Don't overlook the importance of user readiness to deliver an effective, enterprise-wide deployment of Windows 11. Windows 11 has a familiar design, but your users will see several enhancements to the overall user interface. They'll also need to adapt to changes in menus and settings pages. Therefore, consider the following tasks to prepare users and IT support staff for Windows 11:

- Create a communications schedule to ensure that you provide the right message at the right time to the right groups of users, based on when they'll see the

changes.

- Draft concise emails that inform users of what changes they can expect to see. Offer tips on how to use or customize their experience. Include information about support and help desk options.
- Update help desk manuals with screenshots of the new user interface, the out-of-box experience for new devices, and the upgrade experience for existing devices.

For more information and resources, see the Meet Windows 11 video series.

See also

Stay current with Windows devices and Microsoft 365 Apps

Plan for Windows 11

Windows help & learning for users

Feedback

Was this page helpful? Yes No

Provide product feedback

Enterprise feature control in Windows 11

Article • 03/27/2025 • Applies to: ✅ Windows 11, version 22H2 and later

New features and enhancements are introduced through the monthly cumulative update to provide continuous innovation for Windows 11. To give organizations time to plan and prepare, some of these new features might be:

- Temporarily turned off by default using temporary enterprise feature control
- Controlled by a policy that allows for permanent enterprise feature control

Features that are turned off by default are listed in the KB article for the monthly cumulative update. Typically, a feature is selected to be off by default because it either impacts the user experience or IT administrators significantly. For example, a feature might be turned off by default if it requires a change in user behavior or if it requires IT administrators to take action before the feature can be used.

> **Tip**
>
> If you'd like to know what's coming to Windows, check out the **Windows Roadmap**. The roadmap is a high-level overview of the features and functionality that are planned for future releases of Windows.

Temporary enterprise feature control

Features behind temporary enterprise control are automatically disabled for devices that have their Windows updates managed by policies.

Enable features behind temporary enterprise feature control

Features that are behind temporary enterprise control will be enabled when one of the following conditions is met:

- The device installs the annual feature update that enables the new features by default
- The device receives a policy that enables features behind temporary enterprise control
  - When the policy is enabled, all features on the device behind temporary control are turned on when the device restarts.

Policy settings for temporary enterprise feature control

You can use a policy to enable features that are behind temporary enterprise feature control. When this policy is enabled, all features that were disabled behind temporary enterprise feature control are turned on when the device reboots. The following policies apply to Windows 11, version 22H2 with KB5022845 and later:

- **Group Policy:** Computer Configuration\Administrative Templates\Windows Components\Windows Update\Manage end user experience**Enable features introduced via servicing that are off by default**
- **CSP**: ./Device/Vendor/MSFT/Policy/Config/Update/AllowTemporaryEnterpriseFeatureControl
  - In the Intune settings catalog, this setting is named **Allow Temporary Enterprise Feature Control** under the **Windows Update for Business** category.

Windows 11 features behind temporary enterprise feature control

The following features are behind temporary enterprise control in Windows 11:

Expand table

Feature	KB article where the feature was introduced	Feature update that ends temporary control	Notes
Touch-optimized taskbar for 2-in-1 devices	February 28, 2023 - KB5022913	Feature Update to Windows 11, version 23H2	
Selecting **Uninstall** for a Win32 app from the right-click menu uses the **Installed Apps** page in **Settings** rather than **Programs and Features** under the **Control Panel**	September 2023 - KB5030310	Feature Update to Windows 11, version 23H2	
Windows Spotlight provides a minimized experience, opportunities to learn more about each image, and allows users to preview images at full screen.	September 2023 - KB5030310	Feature Update to Windows 11, version 23H2	This feature also has a permanent control: **CSP**: ./User/Vendor/MSFT/Policy/Config/Experience/AllowWindowsSpotlight **Group Policy**: User Configuration\Administrative Templates\Windows Components\Cloud Content**Turn off all Windows spotlight features**
Copilot in Windows	September 2023 - KB5030310	Feature Update to Windows 11, version 23H2	This feature has a permanent control. For more information, see the Windows 11 features with permanent enterprise feature control section.
Dev Home	September 2023 - KB5030310	Feature Update to Windows 11, version 23H2	`Get-AppxPackage -Name Microsoft.Windows.DevHome`

Feature	KB article where the feature was introduced	Feature update that ends temporary control	Notes
Dev Drive	September 2023 - KB5030310	Feature Update to Windows 11, version 23H2	This feature has multiple permanent controls. For more information, see the Windows 11 features with permanent enterprise feature control section

Permanent enterprise feature control

New features and enhancements used to be introduced only in feature updates. However, with continuous innovation for Windows 11, new features are introduced more frequently through the monthly cumulative update. Some new features can be controlled through policies that enable you to configure them for your organization. When a feature can be controlled by a policy, it has permanent enterprise feature control.

Windows 11 features with permanent enterprise feature control

The following features introduced through the monthly cumulative updates allow permanent enterprise feature control:

Expand table

Feature	KB article where the feature was introduced	Feature enabled by default	CSP and Group Policy
Configure search on the taskbar	February 28, 2023 - KB5022913	Yes	**CSP**: ./Device/Vendor/MSFT/Policy/Config/Search/ConfigureSearchOnTaskbarMode **Group Policy**: Computer Configuration\Administrative Templates\Windows Components\Search**Configures search on the taskbar**
The **Recommended** section of the **Start Menu** displays personalized website recommendations	September 2023 - KB5030310	No	**CSP**: ./Device/Vendor/MSFT/Policy/Config/Start/HideRecoPersonalizedSites **Group Policy**: Computer Configuration\Administrative Templates\Start Menu and Taskbar**Remove Personalized Website Recommendations from the Recommended section in the Start Menu**
Recommended section added to File Explorer Home for users signed into Windows with an Azure AD account.	September 2023 - KB5030310	Yes	**CSP**:./Device/Vendor/MSFT/Policy/Config/FileExplorer/DisableGraphRecentItems **Group Policy**: Computer Configuration\Administrative Templates\Windows Components\File Explorer**Turn off files from Office.com in Quick Access View** **Note**: This control disables additional items beyond the **Recommended** items. Review the policy before implementing this control.

Feature	KB article where the feature was introduced	Feature enabled by default	CSP and Group Policy
Transfer files to another PC using WiFi direct	September 2023 - KB5030310	Yes	**CSP**: ./Device/Vendor/MSFT/Policy/Config/Wifi/AllowWiFiDirect
Copilot in Windows	September 2023 - KB5030310	Yes	**CSP**: ./User/Vendor/MSFT/Policy/Config/WindowsAI/TurnOffWindowsCopilot **Group Policy**: User Configuration\Administrative Templates\Windows Components\Windows Copilot**Turn off Windows Copilot**
Dev Drive	September 2023 - KB5030310	Yes	**CSPs**: - ./Device/Vendor/MSFT/Policy/Config/FileSystem/EnableDevDrive - ./Device/Vendor/MSFT/Policy/Config/FileSystem/DevDriveAttachPolicy **Group Policies**: - Computer Configuration\Administrative Templates\System\FileSystem**Enable dev drive** - Computer Configuration\Administrative Templates\System\FileSystem**Dev drive filter attach policy**

Feedback

What's new in Windows 11, version 24H2

Article • 10/01/2024 • Applies to: ✅ Windows 11, version 24H2

Windows 11, version 24H2 is a feature update for Windows 11. It includes all features and fixes in previous cumulative updates to Windows 11, version 23H2. This article lists the new and updated features IT Pros should know.

> **Looking for consumer information?** See Windows 11 2024 update.

Windows 11, version 24H2 follows the Windows 11 servicing timeline:

- **Windows 11 Pro**: Serviced for 24 months from the release date.
- **Windows 11 Enterprise**: Serviced for 36 months from the release date.

Devices must be running Windows 11, version 23H2 or 22H2 with the May 2024 nonsecurity preview update, or a later update, installed in order to update to version 24H2. Windows 11, version 24H2 is a full OS swap so it isn't available as an enablement package. Windows 10 devices can be upgraded to to Windows 11, version 24H2 using the same familiar processes, policies, and management solutions you used to originally deploy Windows 10.

Windows 11, version 24H2 is available through Windows Server Update Services (including Configuration Manager), Windows Update client policies, and the Volume Licensing Service Center (VLSC). For more information, see How to get the Windows 11, version 24H2 update. Review the Windows 11, version 24H2 Windows IT Pro blog post to discover information about available deployment resources such as the Windows Assessment and Deployment Kit (Windows ADK).

To learn more about the status of the update rollout, known issues, and new information, see Windows release health.

Features no longer under temporary enterprise control

Temporary enterprise feature control temporarily turns off certain features that were introduced during monthly cumulative updates for managed Windows 11 devices. For the purposes of temporary enterprise control, a system is considered managed if it's configured to get updates from Windows Update client policies or Windows Server Update Services (WSUS). Clients that get updates from Microsoft Configuration

Manager and Microsoft Intune are considered managed since their updates ultimately come from WSUS or Windows Updates for Business.

There aren't any features under temporary enterprise control between Windows 11, version 23H2 and Windows 11, version 24H2. For a list of features that were under temporary enterprise control between Windows 11, version 22H2 and Windows 11, version 23H2, see, Windows 11 features behind temporary enterprise feature control.

Checkpoint cumulative updates

Microsoft is introducing checkpoint cumulative updates, a new servicing model that enables devices running Windows 11, version 24H2 or later to save time, bandwidth and hard drive space when getting features and security enhancements via the latest cumulative update. Previously, the cumulative updates contained all changes to the binaries since the last release to manufacturing (RTM) version. The size of the cumulative updates could grow large over time since RTM was used as the baseline for each update.

With checkpoint cumulative updates, the update file level differentials are based on a previous cumulative update instead of the RTM release. Cumulative updates that serve as a checkpoint will be released periodically. Using a checkpoint rather than RTM means the subsequent update packages are smaller, which makes downloads and installations faster. Using a checkpoint also means that in order for a device to install the latest cumulative update, the installation of a prerequisite cumulative update might be required. For more information about checkpoint cumulative updates, see https://aka.ms/CheckpointCumulativeUpdates.

Features exclusive to Copilot+ PCs in 24H2

Copilot+ PCs are a new class of Windows 11 AI PCs that are powered by a neural processing unit (NPU) that can perform more than 40 trillion operations per second (TOPS). The following features are exclusive to Copilot+ PCs in Windows 11, version 24H2:

- Live Captions allow you to translate audio and video content into English subtitles from 44 languages. For more information, see Use live captions to better understand audio.
- Windows Studio Effects is the collective name of AI-powered video call and audio effects that are available on Copilot+ PCs and select Windows 11 devices with compatible NPUs. Windows Studio Effects automatically improves lighting and

cancels noises during video calls. For more information, see Windows Studio Effects.

- Cocreator in Paint allows you to create amazing artwork with the help of AI. Enter a text prompt, start drawing in Paint, and Cocreator generates artwork based on what you're drawing. For more information, see Cocreator in Paint
- Auto Super Resolution (Auto SR) is the first AI-powered super resolution solution built into an operating system, making games automatically play smoother with higher resolution details. For more information, see Automatic Super Resolution.
- Image Creator and Restyle Image in the Microsoft Photos app lets you reimagine your photos or create new images with the assistance of AI. For more information, see Microsoft Photos Restyle Image and Image Creator.

Features added to Windows 11 since version 23H2

New features and enhancements were introduced to Windows 11, version 23H2 periodically to provide continuous innovation for Windows 11. These features and enhancements use the normal update servicing channels you're already familiar with. At first, new features are introduced with an optional nonsecurity preview release and gradually rolled out to clients. These new features are released later as part of a monthly security update release. For more information about continuous innovation, see Update release cycle for Windows clients.

Some of the features were released within the past year's continuous innovation updates and carry forward into the 24H2 annual feature update include:

Server Message Block (SMB) protocol changes

SMB signing and encryption

The following changes were made for SMB signing and encryption:

- **SMB signing requirement changes**: In Windows 11, version 24H2 on the Home, Pro, Education, and Enterprise editions, SMB signing is now required by default for all connections. SMB signing ensures every message contains a signature generated using session key and cipher suite. The client puts a hash of the entire message into the signature field of the SMB header. If anyone changes the message itself later on the wire, the hash won't match and SMB knows that someone tampered with the data. It also confirms to sender and receiver that they

are who they say they are, breaking relay attacks. For more information about SMB signing being required by default, see https://aka.ms/SMBSigningOBD.

- **SMB client encryption**: SMB now supports requiring encryption on all outbound SMB client connections. Encryption of all outbound SMB client connections enforces the highest level of network security and brings management parity to SMB signing, which allows both client and server requirements. With this new option, administrators can mandate that all destination servers use SMB 3 and encryption, and if missing those capabilities, the client won't connect. For more information about this change, see https://aka.ms/SmbClientEncrypt.
- **SMB signing and encryption auditing**: Administrators can now enable auditing of the SMB server and client for support of SMB signing and encryption. This shows if a third-party client or server doesn't support SMB encryption or signing. The SMB signing and encryption auditing settings can be modified in Group Policy or through PowerShell.

SMB alternative client and server ports

The SMB client now supports connecting to an SMB server over TCP, QUIC, or RDMA using alternative network ports to the hardcoded defaults. However, you can only connect to alternative ports if the SMB server is configured to support listening on that port. Starting in Windows Server Insider build 26040, the SMB server now supports listening on an alternative network port for SMB over QUIC. Windows Server doesn't support configuring alternative SMB server TCP ports, but some third parties do. For more information about this change, see https://aka.ms/SMBAlternativePorts.

SMB NTLM blocking exception list

The SMB client now supports blocking NTLM for remote outbound connections. With this new option, administrators can intentionally block Windows from offering NTLM via SMB and specify exceptions for NTLM usage. An attacker who tricks a user or application into sending NTLM challenge responses to a malicious server will no longer receive any NTLM data and can't brute force, crack, or pass hashes. This change adds a new level of protection for enterprises without a requirement to entirely disable NTLM usage in the OS.

For more information about this change, see https://aka.ms/SmbNtlmBlock.

SMB dialect management

The SMB server now supports controlling which SMB 2 and 3 dialects it negotiates. With this new option, an administrator can remove specific SMB protocols from use in the organization, blocking older, less secure, and less capable Windows devices and third parties from connecting. For example, admins can specify to only use SMB 3.1.1, the most secure dialect of the protocol.

For more information about this change, see https://aka.ms/SmbDialectManage.

SMB over QUIC

SMB over QUIC, which introduced an alternative to TCP and RDMA, supplies secure connectivity to edge file servers over untrusted networks like the Internet. QUIC has significant advantages, the largest being mandatory certificate-based encryption instead of relying on passwords. SMB over QUIC client access control improves the existing SMB over QUIC feature.

Administrators now have more options for SMB over QUIC such as:

- Specifying which clients can access SMB over QUIC servers. This gives organizations more protection but doesn't change the Windows authentication used to make the SMB connection or the end user experience.
- Disabling SMB over QUIC for client with Group Policy and PowerShell
- Auditing client connection events for SMB over QUIC

For more information about these changes, see https://aka.ms/SmbOverQUICCAC.

SMB firewall rule changes

The Windows Firewall default behavior has changed. Previously, creating an SMB share automatically configured the firewall to enable the rules in the **File and Printer Sharing** group for the given firewall profiles. Now, Windows automatically configures the new **File and Printer Sharing (Restrictive)** group, which no longer contains inbound NetBIOS ports 137-139.

This change enforces a higher degree of default of network security and brings SMB firewall rules closer to the Windows Server **File Server** role behavior, which only opens the minimum ports needed to connect and manage sharing. Administrators can still configure the **File and Printer Sharing** group if necessary as well as modify this new firewall group, these are just default behaviors.

For more information about this change, see https://aka.ms/SMBfirewall. For more information about SMB network security, see Secure SMB Traffic in Windows Server.

Local Security Authority (LSA) protection enablement on upgrade

LSA protection helps protect against theft of secrets and credentials used for logon by preventing unauthorized code from running in the LSA process and by preventing dumping of process memory. An audit occurs for incompatibilities with LSA protection for a period of time, starting with this upgrade. If incompatibilities aren't detected, LSA protection is automatically enabled. You can check and change the enablement state of LSA protection in the Windows Security application under the **Device Security** > **Core Isolation** page. In the event log, LSA protection records whether programs are blocked from loading into LSA. If you would like to check if something was blocked, review the logging.

Remote Mailslot protocol disabled by default

Remote Mailslot protocol was deprecated in November 2023 and is now disabled by default starting in Windows 11, version 24H2. For more information on Remote Mailslots, see About Mailslots.

Local Administrator Password Solution (LAPS) improvements

LAPS has a new automatic account management feature. IT admins can configure Windows LAPS to:

- Automatically create the managed local account
- Configure name of account
- Enable or disable the account
- Randomize the name of the account

LAPS has the following policy improvements:

- Added passphrase settings for the PasswordComplexity policy
  - Use PassphraseLength to control the number of words in a new passphrase
- Added an improved readability setting for the PasswordComplexity policy, which generates passwords without using characters that are easily confused with another character. For example, the zero and the letter O aren't used in the password since the characters can be confused.
- Added the `Reset the password, logoff the managed account, and terminate any remaining processes` setting to the PostAuthenticationActions policy. The event logging messages that are emitted during post-authentication-action execution

were also expanded, to give insights into exactly what was done during the operation.

Image rollback detection was introduced for LAPS. LAPS can detect when a device was rolled back to a previous image. When a device is rolled back, the password in Active Directory might not match the password on the device that was rolled back. This new feature adds an Active Directory attribute, `msLAPS-CurrentPasswordVersion`, to the Windows LAPS schema. This attribute contains a random GUID that Windows LAPS writes every time a new password is persisted in Active Directory, followed by saving a local copy. During every processing cycle, the GUID stored in `msLAPS-CurrentPasswordVersion` is queried and compared to the locally persisted copy. If the GUIDs are different, the password is immediately rotated. To enable this feature, you need to run the latest version of the Update-LapsADSchema PowerShell cmdlet.

Rust in the Windows kernel

There's a new implementation of GDI region in `win32kbase_rs.sys`. Since Rust offers advantages in reliability and security over traditional programs written in C/C++, you'll continue to see more use of it in the kernel.

Personal Data Encryption for folders

Personal Data Encryption for folders is a security feature where the contents of the known Windows folders (Documents, Desktop and Pictures) are protected using a user authenticated encryption mechanism. Windows Hello is the user authentication used to provide the keys for encrypting user data in the folders. Personal Data Encryption for folders can be enabled from a policy in Intune. IT admins can select all of the folders, or a subset, then apply the policy to a group of users in their organization. Personal Data Encryption for Folders settings is available on Intune under **Endpoint Security** > **Disk encryption**.

For more information about Personal Data Encryption, see Personal Data Encryption overview

Windows protected print mode

Windows protected print mode enables devices to print using only the Windows modern print stack, which is designed for Morpia certified printers. With Morpia certified printers, there's no longer a need to rely on third-party software installers. To enable Windows protected print mode:

- Go to **Settings** > **Bluetooth & Devices** > **Printers & scanners**, then choose **Setup** under **Windows protected print mode**
- Enable the **Configure Windows protected print** policy in Group Policy under **Computer Configuration** > **Administrative Templates** > **Printers**

SHA-3 support

Support for the SHA-3 family of hash functions and SHA-3 derived functions (SHAKE, cSHAKE, KMAC) was added. The SHA-3 family of algorithms are the latest standardized hash functions by the National Institute of Standards and Technology (NIST). Support for these functions is enabled through the Windows CNG library.

- **Supported SHA-3 hash functions**: SHA3-256, SHA3-384, SHA3-512 (SHA3-224 isn't supported)
- **Supported SHA-3 HMAC algorithms**: HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512
- **Supported SHA-3 derived algorithms**: extendable-output functions (XOF) (SHAKE128, SHAKE256), customizable XOFs (cSHAKE128, cSHAKE256), and KMAC (KMAC128, KMAC256, KMACXOF128, KMACXOF256).

App Control for Business

Customers can now use App Control for Business (formerly called Windows Defender Application Control) and its next-generation capabilities to protect their digital property from malicious code. With App Control for Business, IT teams can configure what runs in a business environment through Microsoft Intune or other MDMs in the admin console, including setting up Intune as a managed installer. For more information, see Application Control for Windows.

Wi-Fi 7 support

Support for Wi-Fi 7 was added for consumer access points. Wi-Fi 7, also known as IEEE 802.11be Extremely High Throughput (EHT) is the latest Wi-Fi technology that offers unprecedented speed, reliability, and efficiency for your wireless devices. For more information about Wi-Fi 7, see the Wi-Fi Alliance announcement.

Bluetooth ® LE audio support for assistive devices

Customers who use these assistive hearing devices are now able to directly pair, stream audio, take calls, and control audio presets when they use an LE Audio-compatible PC. Users who have Bluetooth LE Audio capable assistive hearing devices can determine if their PC is LE Audio-compatible, set up, and manage their devices via **Settings** > **Accessibility** > **Hearing devices**. For more information, see Using hearing devices with your Windows 11 PC.

Windows location improvements

New controls were added to help manage which apps have access to the list of Wi-Fi networks around you, which could be used to determine your location.

- You can view and modify which apps can access the list of Wi-Fi networks from **Settings** > **Privacy & security** > **Location**.
- A new prompt appears the first time an app attempts to access your location or Wi-Fi information.
  - The prompt also notifies when an app unexpectedly requests access to location services so that you can deny it.
  - If you grant permission, apps that use location or Wi-Fi information now appear in **Recent activity** on the **Location** settings page, and the location icon is displayed in the taskbar while the app is in-use.
  - To hide these prompts when location has been turned off, turn off **Notify when apps request location** on the **Location** settings page.
- Developers can use the Changes to API behavior for Wi-Fi access and location article to learn about API surfaces impacted by this change.

Sudo for Windows

Sudo for Windows is a new way for users to run elevated commands (as an administrator) directly from an unelevated console session. The sudo command can be configured to run in three different modes:

- **In a new window**: The elevated command runs in a new window. This mode is similar to the behavior of the `runas /user:admin` command.
- **With input disabled**: Runs the elevated process in the current window, but with the input handle closed. This means that the elevated process won't be able to receive input from the current console window.
- **Inline**: Runs the elevated process in the current window and the process is able to receive input from the current console session. This mode is most similar to the sudo experience on other platforms.

It's recommended that you review the security considerations for each mode here before enabling the sudo command on your machine. For more information, see Sudo for Windows.

Enable optional updates

In addition to the monthly cumulative update, optional updates are available to provide new features and nonsecurity changes. Most optional updates are released on the fourth Tuesday of the month, known as optional nonsecurity preview releases. Optional updates can also include features that are gradually rolled out, known as controlled feature rollouts (CFRs). Installation of optional updates isn't enabled by default for devices that receive updates using Windows Update client policies. However, you can enable optional updates for devices by using the **Enable optional updates** policy. For more information about optional content, see Enable optional updates.

Remote Desktop Connection improvements

Remote Desktop Connection has the following improvements:

- The Remote Desktop Connection setup window (mstsc.exe) follows the text scaling settings under **Settings** > **Accessibility** > **Text size**.
- Remote Desktop Connection supports zoom options of 350, 400, 450, and 500%
- Improvements to the connection bar design

Additional features

- **File Explorer**: The following changes were made to File Explorer context menu:
  - Support for creating 7-zip and TAR archives
  - **Compress to** > **Additional options** allows you to compress individual files with gzip, BZip2, xz, or Zstandard
  - Labels were added to the context menu icons for actions like copy, paste, delete, and rename
- **OOBE improvement**: when you need to connect to a network and there's no Wi-Fi drivers, you're given an *Install drivers* option to install drivers that are already downloaded
- **Registry Editor**: The Registry Editor supports limiting a search to the currently selected key and its descendants
- **Task Manager**: The Task Manager settings page has Mica material and a redesigned icon

Developer APIs

The following developer APIs were added or updated:

- Introduced the Power Grid Forecast API. App developers can minimize environmental impact by shifting background workloads to times when renewable energy is available to the local grid. Forecast data isn't available globally and quality of data may vary by region.
- Added an energy saver notification callback setting GUID to represent the new energy saver experience. Apps can subscribe to the energy saver status by passing the appropriate GUID to the PowerSettingRegisterNotification API and can implement different behaviors to optimize energy or performance depending on the current energy saver status. For more information, see Power Setting GUIDs
- Extended the Effective Power Mode API to interpret the new energy saver levels when determining the returned effective power mode.

Features removed in Windows 11, version 24H2

The following deprecated features are removed in Windows 11, version 24H2:

- **NTLMv1**: NTLMv1 is removed starting in Windows 11, version 24H2 and Windows Server 2025.
- **WordPad**: WordPad is removed from all editions of Windows starting in Windows 11, version 24H2 and Windows Server 2025.
- **Alljoyn**: Microsoft's implementation of AllJoyn, which included the Windows.Devices.AllJoyn API namespace, a Win32 API, a management configuration service provider (CSP), and an Alljoyn Router Service is retired.

Feedback

What's new in Windows 11, version 23H2

Article • 07/09/2024 • Applies to: ✅ Windows 11, version 23H2

Windows 11, version 23H2 is a feature update for Windows 11. It includes all features and fixes in previous cumulative updates to Windows 11, version 22H2. This article lists the new and updated features IT Pros should know.

Windows 11, version 23H2 follows the Windows 11 servicing timeline:

- **Windows 11 Pro**: Serviced for 24 months from the release date.
- **Windows 11 Enterprise**: Serviced for 36 months from the release date.

Devices updating from Windows 11, version 22H2 use an enablement package. Most the files for the 23H2 update already exist on Windows 11, version 22H2 devices that have installed a recent monthly security update. Many of the new features have already been enabled on Windows 11, version 22H2 clients. However, some features are just in an inactive and dormant state because they are under temporary enterprise feature control. These new features remain dormant until they're turned on through the enablement package, a small, quick-to-install switch that activates all of the Windows 11, version 23H2 features.

Windows 11, version 23H2 is available through Windows Server Update Services (including Configuration Manager), Windows Update client policies, and the Volume Licensing Service Center (VLSC). For more information, see How to get the Windows 11, version 23H2 update. Review the Windows 11, version 23H2 Windows IT Pro blog post to discover information about available deployment resources such as the Windows Deployment Kit (Windows ADK).

To learn more about the status of the update rollout, known issues, and new information, see Windows release health.

Features no longer under temporary enterprise control

Temporary enterprise feature control temporarily turns off certain features that were introduced during monthly cumulative updates for managed Windows 11, version 22H2 devices. For the purposes of temporary enterprise control, a system is considered managed if it's configured to get updates from Windows Update client policies or Windows Server Update Services (WSUS). Clients that get updates from Microsoft Configuration Manager and Microsoft Intune are considered managed since their updates ultimately come from WSUS or Windows Updates for Business.

When a managed Windows 11, version 22H2 device installs version 23H2, the following features will no longer be under temporary enterprise feature control:

Expand table

Feature	KB article where the feature was introduced
Touch-optimized taskbar for 2-in-1 devices	February 28, 2023 - KB5022913
Selecting **Uninstall** for a Win32 app from the right-click menu uses the **Installed Apps** page in **Settings** rather than **Programs and Features** under the **Control Panel**	September 2023 - KB5030310
Windows Spotlight provides a minimized experience, opportunities to learn more about each image, and allows users to preview images at full screen.	September 2023 - KB5030310
Copilot in Windows	September 2023 - KB5030310
Dev Home	September 2023 - KB5030310
Dev Drive	September 2023 - KB5030310

Features added to Windows 11 since version 22H2

Starting with Windows 11, version 22H2, new features and enhancements were introduced periodically to provide continuous innovation for Windows 11. These features and enhancements use the normal update servicing channels you're already familiar with. At first, new features are introduced with an optional nonsecurity preview release and gradually rolled out to clients. These new features are released later as part of a monthly security update release. For more information about continuous innovation, see Update release cycle for Windows clients Some of the features were released within the past year's continuous innovation updates and carry forward into the 23H2 annual feature update include:

Passkeys in Windows

Windows provides a native experience for passkey management. You can use the Settings app to view and manage passkeys saved for apps or websites. For more information, see Support for passkeys in Windows.

Windows passwordless experience

Windows passwordless experience is a security policy that promotes a user experience without passwords on Microsoft Entra joined devices. When the policy is enabled, certain Windows authentication scenarios don't offer users the option to use a password, helping organizations and preparing users to gradually move away from passwords. For more information, see Windows passwordless experience.

Web sign-in for Windows

You can enable a web-based sign-in experience on Microsoft Entra joined devices, unlocking new sign-in options and capabilities. For more information, see Web sign-in for Windows.

Declared configuration protocol

Declared configuration protocol is a new protocol for device configuration management that's based on a desired state model and uses OMA-DM SyncML protocol. It allows the server to provide the device with a collection of settings for a specific scenario, and the device to handle the configuration request and maintain its state. For more information, see What is the declared configuration protocol.

Education themes

You can deploy education themes to your devices. The education themes are designed for students using devices in a school. For more information, see Configure education themes for Windows 11.

Temporary enterprise feature control

Controls were added to temporarily turn off certain features that were introduced during monthly cumulative updates for managed Windows 11, version 22H2 devices. For more information, see Temporary enterprise feature control.

Multi-app kiosk

You can configure a multi-app kiosk, which displays a customized start menu of allowed apps. For more information, see Set up a multi-app kiosk on Windows 11 devices.

Copilot in Windows

Copilot in Windows provides centralized generative AI assistance to your users right from the Windows desktop. For more information, see Manage Copilot in Windows.

Windows Hello for Business authentication improvement

Peripheral face and fingerprint sensors can be used for Windows Hello for Business authentication on devices where Enhanced Sign-in Security (Secure Biometrics) has been enabled at the factory. Previously this functionality was blocked. For more information, see Common questions about Windows Hello for Business.

LAPS native integration

Use Windows Local Administrator Password Solution (LAPS) to regularly rotate and manage local administrator account passwords. For more information, see Local Administrator Password Solution (LAPS)

Federated sign-in

You can sign into Windows using a federated identity, which simplifies the experience for students. For example, students and educators can use QR code badges to sign-in. This feature is designed specifically for Education editions of Windows. For more information, see Configure federated sign-in for Windows devices.

Customize Windows 11 taskbar buttons

Policies to customize Windows 11 taskbar buttons were added to provide you with more control over the taskbar search experience across your organization.

Braille displays

The compatibility of braille displays was expanded. Braille displays work seamlessly and reliably across multiple screen readers, improving the end user experience. We also added support for new braille displays and new braille input and output languages in Narrator. For more information, see Accessibility information for IT professionals.

Dev Drive

Dev Drive is a new form of storage volume available to improve performance for key developer workloads. For more information, see Set up a Dev Drive on Windows 11.

Additional features

- **Tabs for File Explorer**: File Explorer includes tabs to help you organize your File Explorer sessions.
- **Taskbar overflow menu**: The taskbar offers an entry point to a menu that shows all of your overflowed apps in one spot.
- **Suggested actions**: Copied text in certain formats, such as phone numbers or dates, offer suggested actions such as calling the number or adding the event to your calendar.
- **Task Manager enhancements**: Process filtering, theme settings, and the ability to opt out of efficiency mode notification were added to Task Manager.
- **Narrator improvements**: Scripting functionality was added to Narrator. Narrator includes more natural voices.

In-box apps

- **Microsoft Teams**: Chat is being removed from the Microsoft Teams in-box app. Teams will no longer be pinned to the taskbar for enterprise editions of Windows 11, version 23H2 or later. To identify the appx package: `Get-AppxPackage -Name MicrosoftTeams`
- **Dev Home**: Dev Home is a new app that provides a central location for developers to start building, testing, and deploying Windows apps. For more information, see Dev Home. To identify the appx package: `Get-AppxPackage -Name Microsoft.Windows.DevHome`

Feedback

What's new in Windows 11, version 22H2

Article • 07/09/2024 • Applies to: ✅ Windows 11, version 22H2

Windows 11, version 22H2 is a feature update for Windows 11. It includes all features and fixes in previous cumulative updates to Windows 11, version 21H2, the original Windows 11 release version. This article lists the new and updated features IT Pros should know.

Windows 11, version 22H2 follows the Windows 11 servicing timeline:

- **Windows 11 Pro**: Serviced for 24 months from the release date.
- **Windows 11 Enterprise**: Serviced for 36 months from the release date.

Windows 11, version 22H2 is available through Windows Server Update Services (including Configuration Manager), Windows Update client policies, and the Volume Licensing Service Center (VLSC). For more information, see How to get the Windows 11, version 22H2 update. Review the Windows 11, version 22H2 Windows IT Pro blog post to discover information about available deployment resources such as the Windows Deployment Kit (Windows ADK).

To learn more about the status of the update rollout, known issues, and new information, see Windows release health.

Microsoft Pluton

Microsoft Pluton security processor is a chip-to-cloud security technology built with Zero Trust principles at the core. Microsoft Pluton provides hardware-based root of trust, secure identity, secure attestation, and cryptographic services. Pluton technology is a combination of a secure subsystem, which is part of the System on Chip (SoC) and Microsoft authored software that runs on this integrated secure subsystem. Microsoft Pluton can be enabled on devices with Pluton capable processors running Windows 11, version 22H2.

For more information, see Microsoft Pluton security processor.

Enhanced Phishing Protection

Enhanced Phishing Protection in **Microsoft Defender SmartScreen** helps protect Microsoft school or work passwords against phishing and unsafe usage on websites and in applications. Enhanced Phishing Protection works alongside Windows security protections to help protect Windows 11 work or school sign-in passwords.

For more information, see Enhanced Phishing Protection in Microsoft Defender SmartScreen and Protect passwords with enhanced phishing protection in the Windows IT Pro blog.

Smart App Control

Smart App Control adds significant protection from malware, including new and emerging threats, by blocking apps that are malicious or untrusted. **Smart App Control** also helps to block potentially unwanted apps, which are apps that may cause your device to run slowly, display unexpected ads, offer extra software you didn't want, or do other things you don't expect.

For more information, see Smart App Control.

Credential Guard

Compatible Windows 11 Enterprise version 22H2 devices will have **Credential Guard** turned on by default. This changes the default state of the feature in Windows, though system administrators can still modify this enablement state.

For more information, see Manage Credential Guard.

Malicious and vulnerable driver blocking

The vulnerable driver blocklist is automatically enabled on devices for the following two new conditions:

- When Smart App Control is enabled
- For clean installs of Windows

For more information, see recommended block rules.

Security hardening and threat protection

Windows 11, version 22H2 supports additional protection for the Local Security Authority (LSA) process to prevent code injection that could compromise credentials.

For more information, see Configuring Additional LSA Protection.

Personal Data Encryption

Personal Data Encryption is a security feature introduced in Windows 11, version 22H2 that provides additional encryption features to Windows. Personal Data Encryption differs from BitLocker in that it encrypts individual files instead of whole volumes and disks. Personal Data Encryption occurs in addition to other encryption methods such as BitLocker.

Personal Data Encryption utilizes Windows Hello for Business to link data encryption keys with user credentials. This feature can minimize the number of credentials the user has to remember to gain access to files. For example, when using BitLocker with PIN, a user would need to authenticate twice - once with the BitLocker PIN and a second time with Windows credentials. This requirement requires users to remember two different credentials. With Personal Data Encryption, users only need to enter one set of credentials via Windows Hello for Business.

For more information, see Personal Data Encryption.

WebAuthn APIs support ECC

Elliptic-curve cryptography (ECC) is now supported by WebAuthn APIs for Windows 11, version 22H2 clients.

For more information, see WebAuthn APIs for passwordless authentication on Windows.

Stickers for Windows 11 SE, version 22H2

Starting in Windows 11 SE, version 22H2, **Stickers** is a new feature that allows students to decorate their desktop with digital stickers. Students can choose from over 500 cheerful, education-friendly digital stickers. Stickers can be arranged, resized, and customized on top of the desktop background. Each student's stickers remain, even when the background changes.

For more information, see Configure Stickers for Windows 11 SE.

Education themes

Starting in Windows 11, version 22H2, you can deploy education themes to your devices. The education themes are designed for students using devices in a school. Themes allow the end user to quickly configure the look and feel of the device, with preset wallpaper, accent color, and other settings. Students can choose their own themes, making it feel the device is their own.

For more information, see Configure education themes for Windows 11.

Windows Update notifications

The following items were added for Windows Update notifications:

- You can now block user notifications for Windows Updates during active hours. This setting is especially useful for educational organizations that want to prevent Windows Update notifications from occurring during class time. For more information, see Control restart notifications.
- The organization name now appears in the Windows Update notifications when Windows clients are associated with an Azure Active Directory tenant. For more information, see Display organization name in Windows Update notifications.

Start menu layout

Windows 11, version 22H2 now supports additional CSPs for customizing the start menu layout. These CSPs allow you to hide the app list and disable context menus.

For more information, see Supported configuration service provider (CSP) policies for Windows 11 Start menu.

Improvements to task manager

- A new command bar was added to each page to give access to common actions
- Task Manager will automatically match the system wide theme configured in **Windows Settings**
- Added an efficiency mode that allows you to limit the resource usage of a process
- Updated the user experience for Task Manager

Windows accessibility

Windows 11, version 22H2, includes additional improvements for people with disabilities: system-wide live captions, Focus sessions, voice access, and more natural voices for Narrator. For more information, see New accessibility features coming to Windows 11 and How inclusion drives innovation in Windows 11.

For more information, see Accessibility information for IT professionals.

High Efficiency Video Coding (HEVC) support

Starting in Windows 11, version 22H2, support for High Efficiency Video Coding (HEVC) is now available. You can play HEVC videos in any video app on your Windows 11 device. HEVC is designed to take advantage of hardware capabilities on some newer devices to support 4K and Ultra HD content. For devices that don't have hardware support for HEVC videos, software support is provided, but the playback experience might vary based on the video resolution and your devices performance.

Feedback

Was this page helpful? Yes No

Provide product feedback

Extended Security Updates (ESU) program for Windows 10

Article • 03/18/2025 • Applies to: ✅ Windows 10

The Windows 10 Extended Security Updates (ESU) program gives customers the option to receive security updates for PCs enrolled in the program. ESU is a paid program that provides individuals and organizations of all sizes with the option to extend the use of Windows 10 devices past the end of support date in a more secure manner. For more information about the Windows 10 lifecycle, see the Windows Lifecycle FAQ.

Individuals or organizations who elect to continue using Windows 10 after support ends on October 14, 2025, will have the option of enrolling their PCs into a paid ESU subscription. The ESU program enables PCs to continue to receive critical and important security updates through an annual subscription service after support ends. The Microsoft Security Response Center defines the severity rating for security updates.

Device prerequisites

To be eligible to install updates from the ESU program, devices must be running Windows 10, version 22H2.

Limitations

ESUs doesn't include the following items:

- New features
- Customer-requested nonsecurity updates
- Design change requests
- General support won't be provided for Windows versions past the end of support date. The Windows 10 ESU only includes support for the license activation, installation, and possible regressions of the ESU itself. To get technical support for the ESU, organizations must have an active support plan in place.

Frequently asked questions

The following are frequently asked questions about the ESU program for Windows 10:

How much does ESU cost?

Extended Security Updates for organizations and businesses on Windows 10 can be purchased today through the Microsoft Volume Licensing Program, at $61 USD per device for Year One. For more information, see When to use Windows 10 Extended Security Updates. The price doubles every consecutive year, for a maximum of three years. ESU is available at no additional cost for Windows 10 virtual machines running in Windows 365 or Azure Virtual Desktop. Additionally, Windows 10 endpoints connecting to Windows 365 Cloud PCs will be entitled to the ESU for up to three years, with an active Windows 365 subscription license. For more information about Windows 365, see What is Windows 365?.

For individuals or Windows 10 Home customers, Extended Security Updates for Windows 10 will be available for purchase at $30 for one year.

Is there a minimum license purchase requirement for Windows 10 ESU?

The minimum license purchase requirements for Windows 10 ESU is one license.

Can ESUs be purchased for a specific duration?

The Extended Security Update Program for Windows 10 must be purchased by year. Customers can't buy partial periods, for instance, only six months. Year One starts in November 2025. If you decide to purchase the program in Year Two, you'll have to pay for Year One too, as ESUs are cumulative.

When will the ESU offer be available for licensing?

Windows 10 ESU will be available in volume licensing starting about 12 months before the end of support date of Windows 10, or late 2024.

How long can I get security updates for?

Enrolled PCs belonging to a commercial or educational organization can receive security updates for a maximum of three years after end of support for Windows 10.

Is technical support included in ESU?

No, technical support isn't included in the ESU program. Microsoft will provide support for customers that encounter challenges related to the ESU.

Will Windows 10 PCs stop working without the ESU offering?

Windows 10 PCs will continue to work, but we recommend customers upgrade eligible PCs to Windows 11 using Windows Autopatch, Microsoft Intune, or transition to a new Windows 11 PC for the best, most secure computing experience. Customers also have the option to migrate to the cloud and subscribe to Windows 365 to make Windows 11 available to users on any device with a Cloud PC. Beginning October 14, 2025, Microsoft will no longer provide the following for versions of Windows 10 that reach end of support on that date:

- Technical support
- Feature updates or new features
- Quality updates (including security and reliability fixes)

Feedback

Was this page helpful? Yes No

Provide product feedback

What's new in Windows 10, version 22H2

Article • 03/31/2025 • Applies to: ✅ Windows 10, version 22H2

Windows 10, version 22H2 is a feature update for Windows 10. It's a scoped release focused on quality improvements to the overall Windows experience in existing feature areas. It includes all previous cumulative updates to Windows 10, version 21H2. This article is for IT professionals, it lists information about this release that you should know.

Windows 10, version 22H2 is an H2-targeted release, and has the following servicing schedule:

- **Windows 10 Professional**: Serviced for 18 months from the release date.
- **Windows 10 Enterprise**: Serviced for 30 months from the release date.

Windows 10, version 22H2 is available through Windows Server Update Services including Configuration Manager, Windows Update client policies, and the Volume Licensing Service Center (VLSC). For more information, see How to get the Windows 10 2022 Update.

Devices running earlier supported versions of Windows 10 can update to version 22H2 using an enablement package. For more information, see Feature update to Windows 10, version 22H2 by using an enablement package.

To learn more about the status of the Windows 10, version 22H2 rollout, known issues, and build information, see Windows 10 release information.

For more information about updated tools to support this release, see IT tools to support Windows 10, version 22H2.

The Windows 10, version 22H2 feature update is installed as part of the general availability channel. Quality updates are still installed monthly on the second Tuesday of the month.

For more information, see:

- Feature and quality update definitions
- Windows servicing channels

Feedback

Was this page helpful? Yes No

Provide product feedback

Windows Enterprise LTSC

Article • 10/01/2024 •

Applies to: ✅ Windows 10 Enterprise LTSC, ✅ Windows 11 Enterprise LTSC

This article provides general information about the Windows Enterprise long-term servicing channel (LTSC). For more information about the features in each available version of the Windows LTSC, see the following articles:

- What's New in Windows 11 Enterprise LTSC 2024
- What's New in Windows 10 Enterprise LTSC 2021
- What's New in Windows 10 Enterprise LTSC 2019
- What's New in Windows 10 Enterprise LTSC 2016
- What's New in Windows 10 Enterprise LTSC 2015

The long-term servicing channel (LTSC)

The following table summarizes equivalent feature update versions of Windows LTSC and general availability channel (GA channel) releases:

Expand table

LTSC release	Equivalent GA channel release	Availability date
Windows 11 Enterprise LTSC 2024	Windows 11, Version 24H2	10/01/2024
Windows 10 Enterprise LTSC 2021	Windows 10, Version 21H2	11/16/2021
Windows 10 Enterprise LTSC 2019	Windows 10, Version 1809	11/13/2018
Windows 10 Enterprise LTSC 2016	Windows 10, Version 1607	8/2/2016
Windows 10 Enterprise LTSC 2015	Windows 10, Version 1507	7/29/2015

> **Note**
>
> The long-term servicing channel was previously called the long-term servicing branch (LTSB). All references to LTSB are changed in this article to LTSC for consistency, even though the name of previous versions might still be displayed as LTSB.

With the LTSC servicing model, you can delay receiving *feature* updates and instead only receive monthly *quality* updates on devices. Features from Windows 10 and 11 that

could be updated with new functionality, including Microsoft Edge and in-box Windows apps, are also not included. Feature updates are offered in new LTSC releases every several years instead of every few months. You can choose to install them as in-place upgrades, or even skip releases, what's best for your business requirements. Microsoft is committed to providing bug fixes and security patches for each LTSC release during the extended LTSC servicing lifecycle. Always check your individual LTSC release to verify its servicing lifecycle. For more information, see release information, or search the product lifecycle information page.

> **Important**
>
> The long-term servicing channel isn't intended for deployment on most or all the PCs in an organization. The LTSC edition of Windows provides a deployment option for special-purpose devices and environments. These devices typically do a single important task and don't need feature updates as frequently as other devices in the organization. These devices are also typically not heavily dependent on support from external apps and tools. Since the feature set for LTSC doesn't change for the lifetime of the release, over time there might be some external tools that don't continue to provide legacy support. For more information, see **LTSC: What is it, and when it should be used**.

For more information about Windows 10 servicing, see Overview of Windows as a service.

See also

- What's new in Windows: See what's new in other versions of Windows.
- Windows release information: Current versions of Windows by servicing option.

Feedback

Was this page helpful? Yes No

Provide product feedback

What's new in Windows 11 Enterprise LTSC 2024

Article • 10/01/2024 • Applies to: ✅ Windows 11 Enterprise LTSC 2024

This article lists some of the new and updated features and content that is of interest to IT Pros for Windows 11 Enterprise long-term servicing channel (LTSC) 2024, compared to Windows 10 Enterprise LTSC 2021. For a brief description of the LTSC servicing channel and associated support, see Windows Enterprise LTSC.

Windows 11 Enterprise LTSC 2024 builds on Windows 10 Enterprise LTSC 2021, adding premium features such as advanced protection against modern security threats and comprehensive device management, app management, and control capabilities.

The Windows 11 Enterprise LTSC 2024 release includes the cumulative enhancements provided in Windows 11 versions 21H2, 22H2, 23H2, and 24H2. Details about these enhancements are provided below.

Lifecycle

Windows 11 Enterprise LTSC 2024 was first available on October 1, 2024. Features in Windows 11 Enterprise LTSC 2024 are similar to Windows 11, version 24H2.The LTSC release is intended for special use devices. Support for LTSC by apps and tools, such as in-box apps and Microsoft Store, that are designed for the general availability channel release of Windows might be limited.

> **Important**
>
> Windows 11 Enterprise LTSC 2024 has a 5 year lifecycle. (**IoT Enterprise LTSC** continues to have a **10 year lifecycle**). Windows 11 Enterprise LTSC 2024 follows the **Fixed Lifecycle Policy**.

Accessibility

Expand table

Feature [Release]	Description
Windows accessibility 22H2	Improvements for people with disabilities: system-wide live captions, Focus sessions, voice access, and more natural voices for Narrator. For more information, see: * New accessibility features coming to Windows 11 * How inclusion drives innovation in Windows 11 * Accessibility information for IT professionals.
Braille displays 23H2	Braille displays work seamlessly and reliably across multiple screen readers, improving the end user experience. We also added support for new braille displays and new braille input and output languages in Narrator. For more information, see Accessibility information for IT professionals.
Narrator improvements 23H2	Scripting functionality was added to Narrator. Narrator includes more natural voices. For more information, see Complete guide to Narrator.
Bluetooth ® LE audio support for assistive devices 24H2	Windows has taken a significant step forward in accessibility by supporting the use of assistive hearing devices equipped with the latest Bluetooth ® Low Energy Audio technology. For more information, see Using hearing devices with your Windows 11 PC.
Remote Desktop Connection improvements 24H2	The Remote Desktop Connection setup window (mstsc.exe) follows the text scaling settings under **Settings** > **Accessibility** > **Text size**. Remote Desktop Connection supports zoom options of 350, 400, 450, and 500%.

Applications

Expand table

Feature [Release]	Description
Internet Explorer	Internet Explorer (IE) is no longer available in Windows 11 Enterprise LTSC 2024. However, you can use IE Mode if a website needs Internet Explorer. For more information, see Internet Explorer (IE) Mode
Microsoft Edge 21H2	The Microsoft Edge browser is the default browser. For information about configuring Microsoft Edge on Windows, see Configure Microsoft Edge policy settings on Windows devices.
File Explorer 23H2/24H2	**Tabs**: File Explorer includes tabs to help you organize your File Explorer sessions. **Context menu**:

Feature [Release]	Description
	Support for creating 7-zip and TAR archives. **Compress to** > **Additional options** allows you to compress individual files with gzip, BZip2, xz, or Zstandard Labels were added to the context menu icons for actions like copy, paste, delete, and rename.
Registry Editor Search 24H2	The Registry Editor supports limiting a search to the currently selected key and its descendants
Remote Desktop Connection improvements 24H2	The Remote Desktop Connection setup window (mstsc.exe) follows the text scaling settings under **Settings** > **Accessibility** > **Text size**, provides zoom options of 350, 400, 450, and 500%, and improves the connection bar design
Sudo for Windows 24H2	Sudo for Windows is a new way for users to run elevated commands (as an administrator) directly from an unelevated console session. For more information, see Sudo for Windows.

Developer

Expand table

Feature [Release]	Description
Arm64EC (Emulation Compatible)	Code built as Arm64EC is interoperable with x64 code running under emulation within the same process. The Arm64EC code in the process runs with native performance, while any x64 code runs using emulation that comes built-in with Windows 11. For more information, see Arm64EC - Build and port apps for native performance on Arm
Power Grid Forecast 24H2	The Power Grid Forecast API was introduced. App developers can minimize environmental impact by shifting background workloads to times when renewable energy is available to the local grid. Forecast data isn't available globally and quality of data varies by region.
Energy saver notification callback 24H2	Added an energy saver notification callback setting GUID to represent the new energy saver experience. Apps can subscribe to the energy saver status and can implement different behaviors to optimize energy or performance depending on the current energy saver status. For more information, see Power Setting GUIDs
Effective Power Mode	Extended the Effective Power Mode API to interpret the new energy saver levels when determining the returned effective power mode.

Feature [Release]	Description
24H2	

Management

Expand table

Feature [Release]	Description
Microsoft Intune 21H2	Microsoft Intune is a mobile application management (MAM) and mobile device management (MDM) provider. It helps manage devices, and manage apps on devices in your organization. You configure policies, and then deploy these policies to users and groups. You can create and deploy policies that install apps, configure device features, enforce PIN requirements, block compromised devices, and more. If you use Group Policy to manage your Windows 10 devices, then you can also use Group Policy to manage Windows 11 devices. In Intune, there are administrative templates and the settings catalog that include many of the same policies. Group Policy analytics analyze your on-premises group policy objects.
Control Windows Update notifications 22H2	You can now block user notifications for Windows Updates during active hours. This setting is especially useful for organizations that want to prevent Windows Update notifications from occurring during business hours. For more information, see Control restart notifications.
Organization name in update notifications 22H2	The organization name now appears in the Windows Update notifications when Windows clients are associated with a Microsoft Entra ID tenant. For more information, see Display organization name in Windows Update notifications.
Start menu layout 22H2	New Configuration Service Providers (CSPs) for customizing the start menu layout. These CSPs allow you to hide the app list and disable context menus. For more information, see Supported configuration service provider (CSP) policies for Windows 11 Start menu.
Restricted User Experience 23H2	Restricted User Experience (formerly Multi-App Kiosk Mode) supports the creation of a controlled user experience while maintaining the familiar look and feel of the Windows 11 desktop. Ideal for shared devices that require access to more than one app, admins can configure a curated experience to limit distractions and potential tampering points while focusing the experience around the device's dedicated purpose.
Declared configuration	Declared configuration protocol is a new protocol for device configuration management based on a desired state model and uses OMA-DM SyncML

Feature [Release]	Description
protocol 23H2	protocol. It allows the server to provide the device with a collection of settings for a specific scenario, and the device to handle the configuration request and maintain its state. For more information, see What is the declared configuration protocol.
Control File Explorer Home Recommended section 23H2	Configure the Recommended section added to File Explorer Home for users signed into Windows with a Microsoft Entra ID account. For more information, see DisableGraphRecentItems. To configure using Local Group Policy Editor, see `Computer Configuration\Administrative Templates\Windows Components\File Explorer\Turn off files from Office.com in Quick Access View`.
Taskbar Button Policies 23H2	Policies to customize taskbar buttons were added to provide you with more control over the taskbar search experience across your organization. For more information, see Supported taskbar CSPs.
Control Start Menu Recommended section 23H2	Configure the Recommended section of the Start Menu, which displays personalized website recommendations. For more information, see HideRecoPersonalizedSites. To configure using Local Group Policy Editor, see `Computer Configuration\Administrative Templates\Start Menu and Taskbar\Remove Personalized Website Recommendations from the Recommended section in the Start Menu`.
Sudo for Windows 24H2	Sudo for Windows is a new way for users to run elevated commands (as an administrator) directly from an unelevated console session. For more information, see Sudo for Windows.

Networking

Expand table

Feature [Release]	Description
Wi-Fi 7 consumer access points 24H2	Support for Wi-Fi 7 consumer access points offers unprecedented speed, reliability, and efficiency for wireless devices. For more information, see the Wi-Fi 7 announcements from Wi-Fi Alliance and the Windows Insider.
Windows location improvements 24H2	New controls were added to help manage which apps have access to the list of Wi-Fi networks around you, which could be used to determine your location. You can view and modify which apps can access the list of Wi-Fi networks from **Settings** > **Privacy & security** > **Location**. A new prompt appears the first time an app attempts to access your location or Wi-Fi

Feature [Release]	Description
	information. Developers can use the Changes to API behavior for Wi-Fi access and location article to learn about API surfaces impacted by this change.

Security

The security and privacy features in Windows 11 are similar to Windows 10. Security for your devices starts with the hardware, and includes OS security, application security, and user & identity security. There are features available in the Windows OS to help in these areas. For a more comprehensive view, including Zero Trust, see Windows security.

Expand table

Feature [Release]	Description
Windows Security app 21H2	Windows Security app is an easy-to-use interface, and combines commonly used security features. For example, your get access to virus & threat protection, firewall & network protection, account protection, and more. For more information, see the Windows Security app.
Security baselines 21H2	Security baselines include security settings that are already configured, and ready to be deployed to your devices. If you don't know where to start, or it's too time consuming to go through all the settings, then you should look at Security Baselines. For more information, see Windows security baselines.
Microsoft Defender Antivirus 21H2	Microsoft Defender Antivirus helps protect devices using next-generation security. When used with Microsoft Defender for Endpoint, your organization gets strong endpoint protection, and advanced endpoint protection & response. If you use Intune to manage devices, then you can create policies based on threat levels in Microsoft Defender for Endpoint. For more information, see: * Microsoft Defender Antivirus * Microsoft Defender for Endpoint * Enforce compliance for Microsoft Defender for Endpoint
Application Security 21H2	The Application Security features help prevent unwanted or malicious code from running, isolate untrusted websites & untrusted Office files, protect against phishing or malware websites, and more. For more information, see Windows application security.
Microsoft Pluton 22H2	Pluton, designed by Microsoft and built by silicon partners, is a secure crypto-processor built into the CPU. Pluton provides security at the core to ensure code integrity and the latest protection with updates delivered by Microsoft through Windows Update. Pluton protects credentials, identities, personal data, and encryption keys. Information is harder to be removed even if an

Feature [Release]	Description
	attacker installed malware or has complete physical possession. For more information, see Microsoft Pluton security processor.
Enhanced Phishing Protection 22H2	Enhanced Phishing Protection in Microsoft Defender SmartScreen helps protect Microsoft passwords against phishing and unsafe usage. Enhanced Phishing Protection works alongside Windows security protections to help protect sign-in passwords. For more information, see: * Enhanced Phishing Protection in Microsoft Defender SmartScreen * Protect passwords with enhanced phishing protection in the Windows IT Pro blog.
Smart App Control 22H2	Smart App Control adds significant protection from malware, including new and emerging threats, by blocking apps that are malicious or untrusted. Smart App Control helps block unwanted apps that affect performance, display unexpected ads, offer extra software you didn't want, and other things you don't expect. For more information, see Smart App Control.
Credential Guard 22H2	Credential Guard, enabled by default, uses Virtualization-based security (VBS) to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks like pass the hash and pass the ticket. For more information, see Configure Credential Guard.
Malicious and vulnerable driver blocking 22H2	The vulnerable driver blocklist is automatically enabled on devices when Smart App Control is enabled and for clean installs of Windows. For more information, see recommended block rules.
Security hardening and threat protection 22H2	Enhanced support with Local Security Authority (LSA) to prevent code injection that could compromise credentials. For more information, see Configuring Additional LSA Protection.
Personal Data Encryption 22H2	Personal Data Encryption is a security feature that provides file-based data encryption capabilities to Windows. Personal Data Encryption utilizes Windows Hello for Business to link data encryption keys with user credentials. When a user signs in to a device using Windows Hello for Business, decryption keys are released, and encrypted data is accessible to the user.
Passkeys in Windows 23H2	Windows provides a native experience for passkey management. You can use the Settings app to view and manage passkeys saved for apps or websites. For more information, see Support for passkeys in Windows.
Windows passwordless experience 23H2	Windows passwordless experience is a security policy that promotes a user experience without passwords on Microsoft Entra joined devices. When the policy is enabled, certain Windows authentication scenarios don't offer users the option to use a password, helping organizations and preparing

Feature [Release]	Description
	users to gradually move away from passwords. For more information, see Windows passwordless experience.
Web sign-in for Windows 23H2	You can enable a web-based sign-in experience on Microsoft Entra joined devices, unlocking new sign-in options, and capabilities. For more information, see Web sign-in for Windows.
Federated sign-in 23H2	Federated sign-in is a great way to simplify the sign-in process for your users: instead of having to remember a username and password defined in Microsoft Entra ID, they can sign-in using their existing credentials from the federated identity provider. For more information, see Configure federated sign-in for Windows devices.
Windows Hello for Business authentication improvement 23H2	Peripheral face and fingerprint sensors can be used for Windows Hello for Business authentication on devices where Enhanced Sign-in Security (Secure Biometrics) enabled at the factory. For more information, see Common questions about Windows Hello for Business.
App Control for Business 24H2	Customers can now use App Control for Business (formerly called Windows Defender Application Control) and its next-generation capabilities to protect their digital property from malicious code. With App Control for Business, IT teams can configure what runs in a business environment through Microsoft Intune or other MDMs in the admin console, including setting up Intune as a managed installer. For more information, see Application Control for Windows.
Local Security Authority (LSA) protection enablement 24H2	An audit occurs for incompatibilities with LSA protection for a period of time, starting with this upgrade. If incompatibilities aren't detected, LSA protection is automatically enabled. You can check and change the enablement state of LSA protection in the Windows Security application under the **Device Security** > **Core Isolation** page. In the event log, LSA protection logs whether programs are blocked from loading into LSA.
Rust in the Windows kernel 24H2	There's a new implementation of GDI region in `win32kbase_rs.sys`. Since Rust offers advantages in reliability and security over traditional programs written in C/C++, you'll continue to see more use of it in the kernel.
SHA-3 support 24H2	Support for the SHA-3 family of hash functions and SHA-3 derived functions (SHAKE, cSHAKE, KMAC) was added. The SHA-3 family of algorithms is the latest standardized hash functions by the National Institute of Standards and Technology (NIST). Support for these functions is enabled through the Windows CNG library.
Windows Local Admin Password Solution (LAPS) 24H2	Windows Local Administrator Password Solution (Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on your Microsoft Entra joined or Windows Server Active Directory-joined devices. Windows LAPS is the successor for the now

Feature [Release]	Description
	deprecated legacy Microsoft LAPS product. For more information, see What is Windows LAPS?
Windows LAPS Automatic account management 24H2	Windows Local Administrator Password Solution (LAPS) has a new automatic account management feature. Admins can configure Windows LAPS to: * Automatically create the managed local account * Configure name of account * Enable or disable the account * Randomize the name of the account
Windows LAPS Policy improvements 24H2	* Added passphrase settings for the PasswordComplexity policy * Use PassphraseLength to control the number of words in a new passphrase * Added an improved readability setting for the PasswordComplexity policy, which generates passwords without using characters that are easily confused with another character. For example, the number `0` and the letter `O` aren't used in the password since the characters can be confused. * Added the `Reset the password, logoff the managed account, and terminate any remaining processes` setting to the PostAuthenticationActions policy. The event logging messages that are emitted during post-authentication-action execution were also expanded, to give insights into exactly what was done during the operation.
Windows LAPS Image rollback detection 24H2	Image rollback detection was introduced for LAPS. LAPS can detect when a device was rolled back to a previous image. When a device is rolled back, the password in Active Directory might not match the password on the device that was rolled back. This new feature adds an Active Directory attribute, `msLAPS-CurrentPasswordVersion`, to the Windows LAPS schema. This attribute contains a random GUID that Windows LAPS writes every time a new password is persisted in Active Directory, followed by saving a local copy. During every processing cycle, the GUID stored in `msLAPS-CurrentPasswordVersion` is queried and compared to the locally persisted copy. If the GUIDs are different, the password is immediately rotated. To enable this feature, you need to run the latest version of the Update-LapsADSchema PowerShell cmdlet.
Windows protected print mode 24H2	Windows protected print mode (WPP) enables a modern print stack which is designed to work exclusively with Mopria certified printers. For more information, see What is Windows protected print mode (WPP) and Windows Insider WPP announcement.
SMB signing requirement changes 24H2	SMB signing is now required by default for all connections. SMB signing ensures every message contains a signature generated using session key and cipher suite. The client puts a hash of the entire message into the signature field of the SMB header. If anyone changes the message itself later on the wire, the hash won't match and SMB knows that someone tampered with the data. It also confirms to sender and receiver that they are who they say they

Feature [Release]	Description
	are, breaking relay attacks. For more information about SMB signing being required by default, see https://aka.ms/SMBSigningOBD.
SMB client encryption 24H2	SMB now supports requiring encryption on all outbound SMB client connections. Encryption of all outbound SMB client connections enforces the highest level of network security and brings management parity to SMB signing, which allows both client and server requirements. With this new option, administrators can mandate that all destination servers use SMB 3 and encryption, and if missing those capabilities, the client won't connect. For more information about this change, see https://aka.ms/SmbClientEncrypt.
SMB signing and encryption auditing 24H2	Administrators can now enable auditing of the SMB server and client for support of SMB signing and encryption. This shows if a third-party client or server doesn't support SMB encryption or signing. The SMB signing and encryption auditing settings can be modified in Group Policy or through PowerShell.
SMB alternative client and server ports 24H2	The SMB client now supports connecting to an SMB server over TCP, QUIC, or RDMA using alternative network ports to the hardcoded defaults. However, you can only connect to alternative ports if the SMB server is configured to support listening on that port. Starting in Windows Server Insider build 26040, the SMB server now supports listening on an alternative network port for SMB over QUIC. Windows Server doesn't support configuring alternative SMB server TCP ports, but some third parties do. For more information about this change, see https://aka.ms/SMBAlternativePorts.
SMB NTLM blocking exception list 24H2	The SMB client now supports blocking NTLM for remote outbound connections. With this new option, administrators can intentionally block Windows from offering NTLM via SMB and specify exceptions for NTLM usage. An attacker who tricks a user or application into sending NTLM challenge responses to a malicious server will no longer receive any NTLM data and can't brute force, crack, or pass hashes. This change adds a new level of protection for enterprises without a requirement to entirely disable NTLM usage in the OS. For more information about this change, see https://aka.ms/SmbNtlmBlock.
SMB dialect management 24H2	The SMB server now supports controlling which SMB 2 and 3 dialects it negotiates. With this new option, an administrator can remove specific SMB protocols from use in the organization, blocking older, less secure, and less capable Windows devices and third parties from connecting. For example, admins can specify to only use SMB 3.1.1, the most secure dialect of the protocol. For more information about this change, see https://aka.ms/SmbDialectManage.

Feature [Release]	Description
SMB over QUIC client access control 24H2	SMB over QUIC, which introduced an alternative to TCP and RDMA, supplies secure connectivity to edge file servers over untrusted networks like the Internet. QUIC has significant advantages, the largest being mandatory certificate-based encryption instead of relying on passwords. SMB over QUIC client access control improves the existing SMB over QUIC feature. Administrators now have more options for SMB over QUIC such as: * Specifying which clients can access SMB over QUIC servers. This gives organizations more protection but doesn't change the Windows authentication used to make the SMB connection or the end user experience. * Disabling SMB over QUIC for client with Group Policy and PowerShell * Auditing client connection events for SMB over QUIC For more information about these changes, see https://aka.ms/SmbOverQUICCAC.
SMB firewall rule changes 24H2	The Windows Firewall default behavior has changed. Previously, creating an SMB share automatically configured the firewall to enable the rules in the **File and Printer Sharing** group for the given firewall profiles. Now, Windows automatically configures the new **File and Printer Sharing (Restrictive)** group, which no longer contains inbound NetBIOS ports 137-139. This change enforces a higher degree of default of network security and brings SMB firewall rules closer to the Windows Server **File Server** role behavior, which only opens the minimum ports needed to connect and manage sharing. Administrators can still configure the **File and Printer Sharing** group if necessary as well as modify this new firewall group, these are just default behaviors. For more information about this change, see https://aka.ms/SMBfirewall. For more information about SMB network security, see Secure SMB Traffic in Windows Server.

Servicing

Expand table

Feature [Release]	Description
Windows Updates and Delivery optimization 21H2	Delivery optimization helps reduce bandwidth consumption. It shares the work of downloading the update packages with multiple devices in your deployment. Windows 11 updates are smaller, as they only pull down source files that are different. You can create policies that configure delivery optimization settings. For example, set the maximum upload and download bandwidth, set caching sizes, and more. For more information, see: * Delivery Optimization for Windows updates

Feature [Release]	Description
	* Installation & updates * Manage updates in Windows
Control Windows Update notifications 22H2	You can now block user notifications for Windows Updates during active hours. This setting is especially useful for organizations that want to prevent Windows Update notifications from occurring during business hours. For more information, see Control restart notifications.
Organization name in update notifications	The organization name now appears in the Windows Update notifications when Windows clients are associated with a Microsoft Entra ID tenant. For more information, see Display organization name in Windows Update notifications.
Checkpoint cumulative updates 24H2	Windows quality updates are provided as cumulative updates throughout the life cycle of a Windows release. Checkpoint cumulative updates introduce periodic baselines that reduce the size of future cumulative updates making the distribution of monthly quality updates more efficient. For more information, see https://aka.ms/CheckpointCumulativeUpdates.

User Experience

Expand table

Feature [Release]	Description
High Efficiency Video Coding (HEVC) support 22H2	HEVC is designed to take advantage of hardware capabilities on some newer devices to support 4K and Ultra HD content. For devices that don't have hardware support for HEVC videos, software support is provided, but the playback experience might vary based on the video resolution and your devices performance.
Task Manager 22H2/23H2	A new command bar was added to each page to give access to common actions. Task Manager matches the system wide theme configured in Windows Settings. Added an efficiency mode that allows you to limit the resource usage of a process. Process filtering, theme settings, and the ability to opt out of efficiency mode notification were added to Task Manager.
Taskbar overflow menu 23H2	The taskbar offers an entry point to a menu that shows all of your overflowed apps in one spot.
Taskbar Optimize for	Taskbar touch optimization is available for devices that can be used as a tablet. Once enabled, the user can switch between a collapsed taskbar, saving screen

Feature [Release]	Description
touch 23H2	space, and an expanded taskbar, optimized for touch. The taskbar changes to this optimized version when you disconnect or fold back the keyboard on a 2-in-1 device. To enable or disable this feature on a tablet capable device, go to Settings > Personalization > Taskbar > Taskbar behaviors. See also February 28, 2023 - KB5022913
Windows Ink as input 23H2	Windows Ink allows users to handwrite directly onto most editable fields
Uninstall Win32 app 23H2	Selecting Uninstall for a Win32 app from the right-click menu uses the Installed Apps page in Settings rather than Programs and Features in Control Panel. For more information, see September 2023 - KB5030310
Dev Drive 23H2	Dev Drive is a new form of storage volume available to improve performance for key developer workloads. For more information, see Set up a Dev Drive on Windows 11 and September 2023 - KB5030310.

Features Removed

Each version of Windows client adds new features and functionality. Occasionally, features and functionality are removed, often because a newer option was added. For a list of features no longer in active development that might be removed in a future release, see deprecated features. The following features are removed in Windows 11 Enterprise LTSC 2024:

Expand table

Feature	Description
WordPad 24H2	WordPad is removed from all editions of Windows starting in Windows 11, version 24H2 and Windows Server 2025.
Alljoyn 24H2	Microsoft's implementation of AllJoyn, which included the Windows.Devices.AllJoyn API namespace, a Win32 API, a management configuration service provider (CSP), and an Alljoyn Router Service is retired.

Related links

- Windows Enterprise LTSC overview
- Windows 11 requirements
- Plan for Windows 11

- Prepare for Windows 11
- Release information

Feedback

Was this page helpful? Yes No

Provide product feedback

What's new in Windows 10 Enterprise LTSC 2021

Article • 07/09/2024 • Applies to: ✅ Windows 10 Enterprise LTSC 2021

This article lists new and updated features and content that is of interest to IT Pros for Windows 10 Enterprise LTSC 2021, compared to Windows 10 Enterprise LTSC 2019 (LTSB). For a brief description of the LTSC servicing channel and associated support, see Windows 10 Enterprise LTSC.

> **Note**
>
> Windows 10 Enterprise LTSC 2021 was first available on November 16, 2021. Features in Windows 10 Enterprise LTSC 2021 are equivalent to Windows 10, version 21H2.
>
> The LTSC release is intended for special use devices. Support for LTSC by apps and tools that are designed for the general availability channel release of Windows 10 might be limited.

Windows 10 Enterprise LTSC 2021 builds on Windows 10 Enterprise LTSC 2019, adding premium features such as advanced protection against modern security threats and comprehensive device management, app management, and control capabilities.

The Windows 10 Enterprise LTSC 2021 release includes the cumulative enhancements provided in Windows 10 versions 1903, 1909, 2004, 21H1, and 21H2. Details about these enhancements are provided below.

Lifecycle

> **Important**
>
> Windows 10 Enterprise LTSC 2021 has a 5 year lifecycle. (IoT Enterprise LTSC continues to have a 10 year lifecycle). Thus, the LTSC 2021 release is not a direct replacement for LTSC 2019, which has a 10 year lifecycle.

For more information about the lifecycle for this release, see The next Windows 10 long-term servicing channel (LTSC) release.

Hardware security

System Guard

System Guard has improved a feature in this version of Windows called **SMM Firmware Protection**. This feature is built on top of System Guard Secure Launch to reduce the firmware attack surface and ensure that the System Management Mode (SMM) firmware on the device is operating in a healthy manner - specifically, SMM code can't access the OS memory and secrets.

In this release, Windows Defender System Guard enables an even *higher* level of System Management Mode (SMM) Firmware Protection that goes beyond checking the OS memory and secrets to other resources like registers and IO.

With this improvement, the OS can detect a higher level of SMM compliance, enabling devices to be even more hardened against SMM exploits and vulnerabilities. Based on the platform, the underlying hardware and firmware, there are three versions of SMM Firmware Protection (one, two and three), with each subsequent versions offering stronger protections than the preceding ones.

There are already devices in the market today that offer SMM Firmware Protection versions one and two. SMM Firmware Protection version three This feature is currently forward-looking and requires new hardware that will be made available soon.

Operating system security

System security

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.

Encryption and data protection

BitLocker and Mobile Device Management (MDM) with Microsoft Entra ID work together to protect your devices from accidental password disclosure. Now, a new key-rolling feature securely rotates recovery passwords on MDM-managed devices. The feature is activated whenever Microsoft Intune/MDM tools or a recovery password is used to

unlock a BitLocker protected drive. As a result, the recovery password will be better protected when users manually unlock a BitLocker drive.

Network security

Windows Defender Firewall

Windows Defender Firewall now offers the following benefits:

Reduce risk: Windows Defender Firewall reduces the attack surface of a device with rules to restrict or allow traffic by many properties, such as IP addresses, ports, or program paths. Reducing the attack surface of a device increases manageability and decreases the likelihood of a successful attack.

Safeguard data: With integrated Internet Protocol Security (IPsec), Windows Defender Firewall provides a simple way to enforce authenticated, end-to-end network communications. It provides scalable, tiered access to trusted network resources, helping to enforce integrity of the data, and optionally helping to protect the confidentiality of the data.

Extend value: Windows Defender Firewall is a host-based firewall that is included with the operating system, so there's no other hardware or software required. Windows Defender Firewall is also designed to complement existing non-Microsoft network security solutions through a documented application programming interface (API).

The Windows Defender Firewall is also now easier to analyze and debug. IPsec behavior has been integrated with Packet Monitor (pktmon), an in-box cross-component network diagnostic tool for Windows.

Additionally, the Windows Defender Firewall event logs have been enhanced to ensure an audit can identify the specific filter that was responsible for any given event. This enhancement enables analysis of firewall behavior and rich packet capture without relying on other tools.

Windows Defender Firewall also now supports Windows Subsystem for Linux (WSL); You can add rules for WSL process, just like for Windows processes. For more information, see Windows Defender Firewall now supports Windows Subsystem for Linux (WSL).

Virus and threat protection

Attack surface area reduction - IT admins can configure devices with advanced web protection that enables them to define allowlists and blocklists for specific URLs 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 Microsoft Defender for Endpoint security capabilities away from the OS and attackers. Platform support - In addition to Windows 10, Microsoft Defender for Endpoint'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.

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 that 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 and configurable retention policies.

Improved support for non-ASCII file paths for Microsoft Defender Advanced Threat Protection (ATP) Auto Incident Response (IR).

> **Note**
>
> The DisableAntiSpyware parameter is deprecated in this release.

Application security

App isolation

Windows Sandbox: Isolated desktop environment where you can run untrusted software without the fear of lasting impact to your device.

Microsoft Defender Application Guard

Microsoft Defender Application Guard enhancements include:

- 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.

- Application Guard is now an extension in Google Chrome and Mozilla Firefox. Many users are in a hybrid browser environment, and would like to extend Application Guard's browser isolation technology beyond Microsoft Edge. In the latest release, users can install the Application Guard extension in their Chrome or Firefox browsers. This extension will redirect untrusted navigation to the Application Guard Edge browser. There's also a companion app to enable this feature in the Microsoft Store. Users can quickly launch Application Guard 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 Application Guard 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 of the other configuration steps on the extension setup page.
  4. Reboot the device.
  5. Navigate to an untrusted site in Chrome and Firefox.

Dynamic navigation: Application Guard now allows users to navigate back to their default host browser from the Application Guard Microsoft Edge. Previously, users browsing in Application Guard 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 Application Guard Edge. This feature is also available in Windows 10, version 1803 or later with the latest updates.

Application Guard performance is improved with optimized document opening times:

- An issue is fixed that could cause a one-minute-or-more delay when you open a Microsoft Defender Application Guard (Application Guard) Office document. This issue can occur when you try to open a file using a Universal Naming Convention (UNC) path or Server Message Block (SMB) share link.

- A memory issue is fixed that could cause an Application Guard container to use almost 1 GB of working set memory when the container is idle.
- The performance of Robocopy is improved when copying files over 400 MB in size.

Application Control

Application Control for Windows: In Windows 10, version 1903, Windows Defender Application Control (WDAC) added many new features that light up key scenarios and provide feature parity with AppLocker.

- Multiple Policies: Windows Defender Application Control 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 aren't user-writeable is executed. When code tries to execute at runtime, the directory is scanned and files will be checked for write permissions for unknown admins. If a file is found to be user writeable, the executable is blocked from running unless it's authorized by something other than a path rule like a signer or hash rule.
  This functionality brings WDAC to 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 isn't available with AppLocker.
- Allow COM Object Registration: Previously, Windows Defender Application Control (WDAC) enforced a built-in allowlist for COM object registration. While this mechanism works for most common application usage scenarios, customers have provided feedback that there are cases where more 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.

Identity and privacy

Secured identity

Windows Hello enhancements include:

- Windows Hello is now supported as Fast Identity Online 2 (FIDO2) authenticator across all major browsers including Chrome and Firefox.
- You can now enable passwordless sign-in for Microsoft accounts on your Windows 10 device by going to **Settings** > **Accounts** > **Sign-in options**, and selecting **On** under **Make your device passwordless**. Enabling passwordless sign-in will switch all Microsoft accounts on your Windows 10 device to modern authentication with Windows Hello Face, Fingerprint, or PIN.
- Windows Hello PIN sign-in support is added to Safe mode.
- Windows Hello for Business now has Microsoft Entra hybrid support and phone number sign-in (Microsoft account). FIDO2 security key support is expanded to Microsoft Entra hybrid environments, enabling enterprises with hybrid environments to take advantage of passwordless authentication. For more information, see Expanding Azure Active Directory support for FIDO2 preview to hybrid environments.
- With specialized hardware and software components available on devices shipping with Windows 10, version 20H2 configured out of factory, Windows Hello now offers added support for virtualization-based security with supporting fingerprint and face sensors. This feature isolates and secures a user's biometric authentication data.
- Windows Hello multi-camera support is added, allowing users to choose an external camera priority when both external and internal Windows Hello-capable cameras are present.
- Windows Hello FIDO2 certification: Windows Hello is now a FIDO2 Certified authenticator and enables password-less sign-in for websites supporting FIDO2 authentication, such as Microsoft account and Entra ID.
- 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.
- Remote Desktop with Biometrics: Microsoft Entra ID and Active Directory users using Windows Hello for Business can use biometrics to authenticate to a remote desktop session.

Credential protection

Credential Guard

Credential Guard is now available for ARM64 devices, for extra protection against credential theft for enterprises deploying ARM64 devices in their organizations, such as Surface Pro X.

Privacy controls

Microphone privacy settings: A microphone icon appears in the notification area letting you see which apps are using your microphone.

Cloud Services

Microsoft Intune

Microsoft Intune supports Windows 10 Enterprise LTSC 2021 with the following exception:

- Update rings can't be used for feature updates since Windows 10 LTSC versions don't receive feature updates. Update rings can be used for quality updates for Windows 10 Enterprise LTSC 2021 clients.

A new Intune remote action: **Collect diagnostics**, lets you collect the logs from corporate devices without interrupting or waiting for the end user. For more information, see Collect diagnostics remote action.

Intune has also added capabilities to Role-based access control (RBAC) that can be used to further define profile settings for the Enrollment Status Page (ESP). For more information, see Create Enrollment Status Page profile and assign to a group.

For a full list of what's new in Microsoft Intune, see What's new in Microsoft Intune.

Mobile Device Management

Mobile Device Management (MDM) policy is extended with new Local Users and Groups settings that match the options available for devices managed through Group Policy.

For more information about what's new in MDM, see What's new in mobile device enrollment and management

Windows Management Instrumentation (WMI) Group Policy Service (GPSVC) has a performance improvement to support remote work scenarios:

- An issue is fixed that caused changes by an Active Directory (AD) administrator to user or computer group memberships to propagate slowly. Although the access token eventually updates, these changes might not appear when the administrator uses gpresult /r or gpresult /h to create a report.

Key-rolling and Key-rotation

This release also includes two new features called key-rolling and key-rotation enables secure rolling of recovery passwords on MDM-managed Microsoft Entra ID devices on demand from Microsoft Intune/MDM tools or when a recovery password is used to unlock the BitLocker protected drive. This feature will help prevent accidental recovery password disclosure as part of manual BitLocker drive unlock by users.

Deployment

SetupDiag

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 log files are being searched, 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.

Windows Assessment and Deployment Toolkit (ADK)

A new Windows ADK is available for Windows 11 that also supports Windows 10, version 21H2.

Microsoft Deployment Toolkit (MDT)

For the latest information about MDT, see the MDT release notes.

Windows Setup

Windows Setup answer files (unattend.xml) have improved language handling.

Improvements in Windows Setup with this release also include:

- Reduced offline time during feature updates
- Improved controls for reserved storage
- Improved controls and diagnostics
- New recovery options

For more information, see Windows Setup enhancements in the Windows IT Pro Blog.

Microsoft Edge

Microsoft Edge Browser support is now included in-box.

Microsoft Edge kiosk mode

Microsoft Edge kiosk mode is available for LTSC releases starting in Windows 10 Enterprise 2021 LTSC and Windows 10 IoT Enterprise 2021 LTSC.

Microsoft Edge kiosk mode offers two lockdown experiences of the browser so organizations can create, manage, and provide the best experience for their customers. The following lockdown experiences are available:

- Digital/Interactive Signage experience - Displays a specific site in full-screen mode.
- Public-Browsing experience - Runs a limited multi-tab version of Microsoft Edge.
- Both experiences are running a Microsoft Edge InPrivate session, which protects user data.

Windows Subsystem for Linux

Windows Subsystem for Linux (WSL) is available in-box.

Networking

WPA3 H2E standards are supported for enhanced Wi-Fi security.

See Also

Windows 10 Enterprise LTSC: A short description of the LTSC servicing channel with links to information about each release.

Feedback

Was this page helpful? Yes No

Provide product feedback

What's new in Windows 10 Enterprise LTSC 2019

Article • 07/09/2024 • Applies to: ✅ Windows 10 Enterprise LTSC 2019

This article lists new and updated features and content that are of interest to IT Pros for Windows 10 Enterprise LTSC 2019, compared to Windows 10 Enterprise LTSC 2016 (LTSB). For a brief description of the LTSC servicing channel and associated support, see Windows 10 Enterprise LTSC.

> **Note**
>
> Windows 10 Enterprise LTSC 2019 was first available on November 13, 2018. Features in Windows 10 Enterprise LTSC 2019 are equivalent to Windows 10, version 1809.

Windows 10 Enterprise LTSC 2019 builds on Windows 10 Pro, version 1809 adding premium features designed to address the needs of large and mid-size organizations (including large academic institutions), such as:

- Advanced protection against modern security threats
- Full flexibility of OS deployment
- Updating and support options
- Comprehensive device and app management and control capabilities

The Windows 10 Enterprise LTSC 2019 release is an important release for LTSC users because it includes the cumulative enhancements provided in Windows 10 versions 1703, 1709, 1803, and 1809. Details about these enhancements are provided below.

> **Important**
>
> The LTSC release is intended for special use devices. Support for LTSC by apps and tools that are designed for the general availability channel release of Windows 10 might be limited.

Microsoft Intune

Microsoft Intune supports Windows 10 Enterprise LTSC 2019 with the following exception:

- Update rings can't be used for feature updates since Windows 10 LTSC versions don't receive feature updates. Update rings can be used for quality updates for Windows 10 Enterprise LTSC 2019 clients.

Security

This version of Windows 10 includes security improvements for threat protection, information protection, and identity protection.

Threat protection

Microsoft Defender for Endpoint

The Microsoft Defender for Endpoint platform includes multiple security pillars. In this version of Windows, Defender for Endpoint includes powerful analytics, security stack integration, and centralized management for better detection, prevention, investigation, response, and management.

Attack surface reduction

Attack surface reduction includes host-based intrusion prevention systems such as controlled folder access.

- This feature 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. Select **Allow an app through Controlled folder access**. After the prompt, select 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.

Windows Defender Firewall

Windows Defender Firewall now supports Windows Subsystem for Linux (WSL) processes. You can add specific rules for a WSL process 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 behavior was first introduced in Build 17627.

Windows Defender Device Guard

Device Guard has always been a collection of technologies that can be combined to lock down a PC, including:

- Software-based protection provided by code integrity policies
- Hardware-based protection provided by Hypervisor-protected code integrity (HVCI)

But these protections can also be configured separately. And, unlike HVCI, code integrity policies don't require virtualization-based security (VBS). To help underscore the distinct value of these protections, code integrity policies have been rebranded as Windows Defender Application Control.

Next-gen protection

Endpoint detection and response

Endpoint detection and response are improved. Enterprise customers can now take advantage of the entire Windows security stack with Microsoft Defender Antivirus **detections** and Device Guard **blocks** being surfaced in the Microsoft Defender for Endpoint portal.

Windows Defender is now called Microsoft Defender Antivirus and now shares detection status between Microsoft 365 services and interoperates with Microsoft Defender for Endpoint. Other 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 Microsoft Defender Antivirus through cloud-delivered protection.

We've also 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 Microsoft Defender AV and Deployment guide for Microsoft Defender AV in a virtual desktop infrastructure environment.

New features for Microsoft Defender AV in Windows 10 Enterprise LTSC 2019 include:

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

We've invested heavily in helping to protect against ransomware, and we continue that investment with updated behavior monitoring and always-on real-time protection.

Endpoint detection and response is also enhanced. New **detection** capabilities include:

- Custom detection. With custom detections, you can create custom queries to monitor events for any kind of behavior such as suspicious or emerging threats. You can use advanced hunting through the creation of custom detection rules.
- 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.

Threat response is improved when an attack is detected, enabling immediate action by security teams 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 capabilities have been added to help you gain a holistic view on **investigations** include:

- Threat analytics - Threat Analytics is a set of interactive reports published by the Microsoft Defender for Endpoint research team as soon as emerging threats and outbreaks are identified. The reports help security operations teams assess the effect to their environment. They also provide recommended actions to contain, increase organizational resilience, and prevent specific threats.

- Query data using Advanced hunting in Microsoft Defender for Endpoint
- Use Automated investigations to investigate and remediate threats
- 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 Microsoft Defender for Endpoint.

Other enhanced security features include:

- Check sensor health state - Check an endpoint's ability to provide sensor data and communicate with the Microsoft Defender for Endpoint service and fix known issues.
- Managed security service provider (MSSP) support - Microsoft Defender for Endpoint 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 Defender - Microsoft Defender for Endpoint integrates with Azure Defender to provide a comprehensive server protection solution. With this integration, Azure Defender can use Defender for Endpoint to provide improved threat detection for Windows Servers.
- Integration with Microsoft Cloud App Security - Microsoft Cloud App Security uses Microsoft Defender for Endpoint signals to allow direct visibility into cloud application usage including the use of unsupported cloud services (shadow IT) from all Defender for Endpoint monitored machines.
- Onboard Windows Server 2019 - Microsoft Defender for Endpoint 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 Microsoft Defender for Endpoint sensor.
- Enable conditional access to better protect users, devices, and data

We've also added a new assessment for the Windows time service to the **Device performance & health** section. If we detect that your device's time isn't 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. Select **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 improvement 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.

Also see New capabilities of Microsoft Defender for Endpoint further maximizing the effectiveness and robustness of endpoint security

Get a quick, but in-depth overview of Microsoft Defender for Endpoint for Windows 10: Defender for Endpoint.

Information protection

Improvements have been added to Windows Information Protection and BitLocker.

Windows Information Protection

Windows Information Protection is now designed to work with Microsoft Office and Azure Information Protection.

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 more information, see How to collect Windows Information Protection (WIP) audit event logs.

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.

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.

Silent enforcement on fixed drives

Through a modern device management (MDM) policy, BitLocker can be enabled silently for standard Microsoft Entra ID joined users. In Windows 10, version 1803 automatic BitLocker encryption was enabled for standard Entra ID 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 change is an update to the BitLocker CSP and used by Intune and others.

Identity protection

Improvements have been added are to Windows Hello for Business and Credential Guard.

Windows Hello for Business

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 aren't present.

New features in Windows Hello for Business include:

- You can now reset a forgotten PIN without deleting company managed data or apps on devices managed by Microsoft Intune.
- For Windows desktops, users are able to reset a forgotten PIN through **Settings** > **Accounts** > **Sign-in options**. For more information, see What if I forget my PIN?.

Windows Hello for Business now supports FIDO 2.0 authentication for Entra ID-joined Windows 10 devices and has enhanced support for shared devices, as described in Kiosk configuration.

- 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 device Bluetooth is off.
- You can set up Windows Hello from lock screen for Microsoft 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's easier to set up Dynamic lock, and WD SC actionable alerts have been added when Dynamic lock stops working (ex: device Bluetooth is off).

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

Credential Guard

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's designed to protect against well-known threats such as Pass-the-Hash and credential harvesting.

Credential Guard has always been an optional feature, but Windows 10 in S mode turns on this functionality by default when the machine has been Entra ID-joined. This feature provides an added level of security when connecting to domain resources not normally present on devices running Windows 10 in S mode.

> **Note**
>
> Credential Guard is available only to S mode devices or Enterprise and Education Editions.

For more information, see Credential Guard overview.

Other security improvements

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 effect. 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.

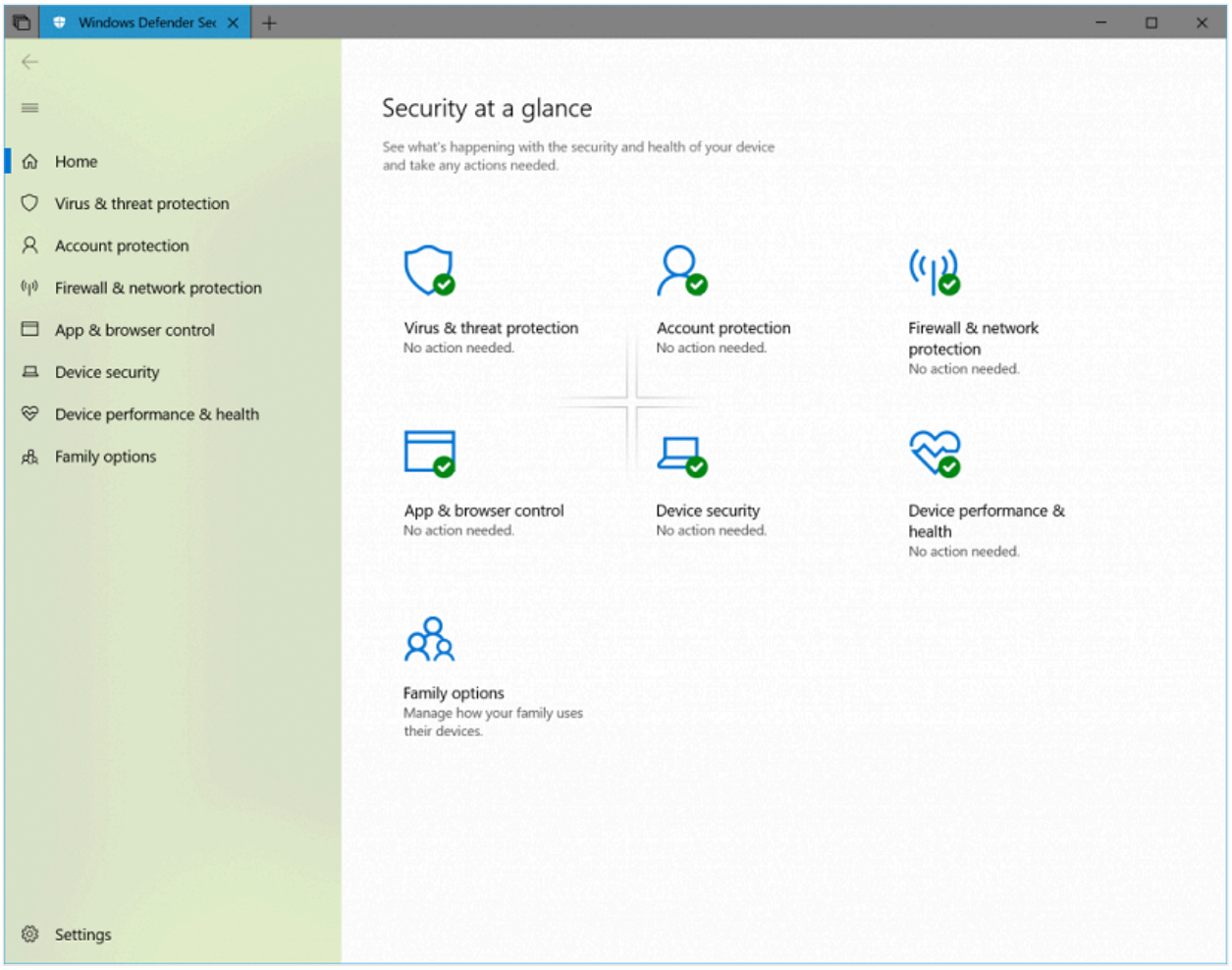
Windows Security Center

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

You can still get to the app in all the usual ways. WSC lets you manage all your security needs, including **Microsoft Defender Antivirus** and **Windows Defender Firewall**.

The WSC service now requires antivirus products to run as a protected process to register. Products that haven't yet implemented this functionality won't appear in the Windows Security Center user interface, and Microsoft 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've enabled that option in **Color Settings**.



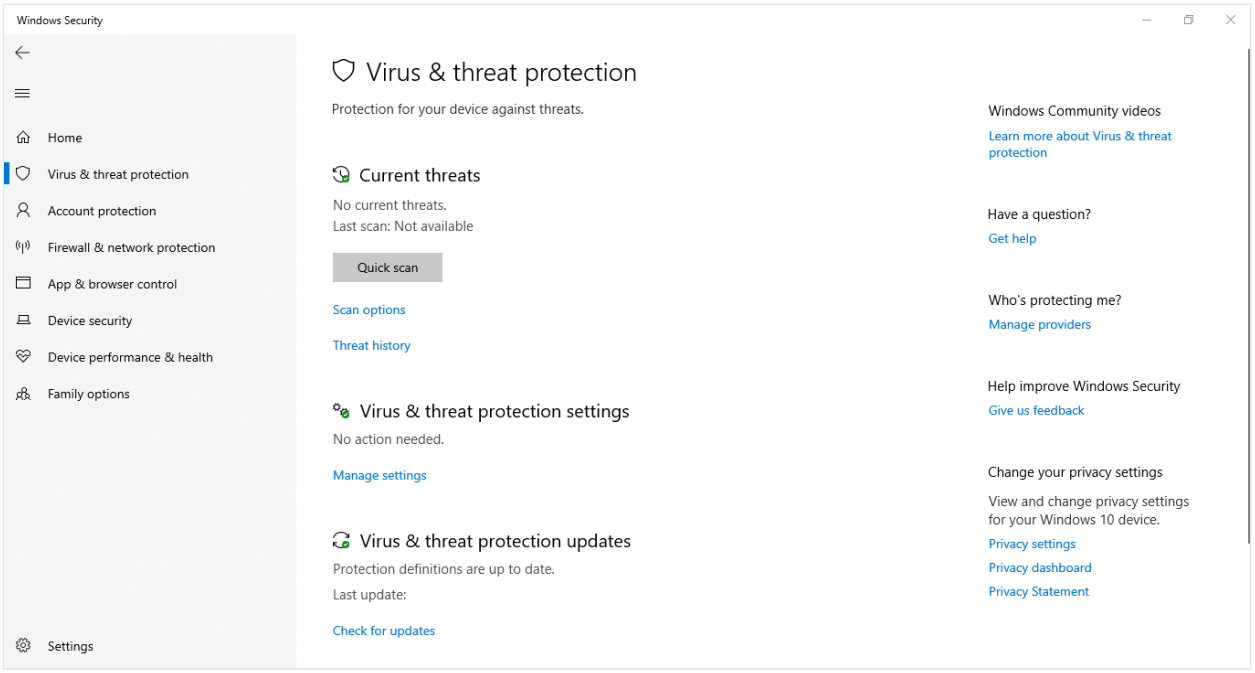
Group policy security options

The security setting **Interactive logon: Display user information when the session is locked** has been updated to work 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 Enterprise LTSC 2019. This security policy setting determines whether the username is displayed during sign-in. It works with the **Privacy** setting in **Settings** > **Accounts** > **Sign-in options**. The setting only affects the **Other user** tile.

Windows 10 in S mode

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:



Deployment

MBR2GPT.EXE

MBR2GPT.EXE is a new command-line tool introduced with Windows 10, version 1703 and also available in Windows 10 Enterprise LTSC 2019 (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 runs from a Windows Preinstallation Environment (Windows PE) command prompt, but can also run from the full Windows 10 operating system.

The GPT partition format is newer and enables the use of larger and more disk partitions. It also provides added data reliability, supports other 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.

Other 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 more information, see MBR2GPT.EXE.

DISM

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

- `DISM /Online /Initiate-OSUninstall`: Initiates an 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 Windows 10 Enterprise LTSC 2019, or later.
- Windows 10 Enterprise or Pro

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

It's 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 doesn't work, then suspend BitLocker and complete the upgrade.
- `Setup.exe /BitLocker ForceKeepActive`: Enable upgrade without suspending BitLocker, but if upgrade doesn't work, fail the upgrade.

For more information, see Windows Setup Command-Line Options.

Feature update improvements

Portions of the work done during the offline phases of a Windows update have been moved to the online phase. This change results in a significant reduction of offline time when installing updates.

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 it searches 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.

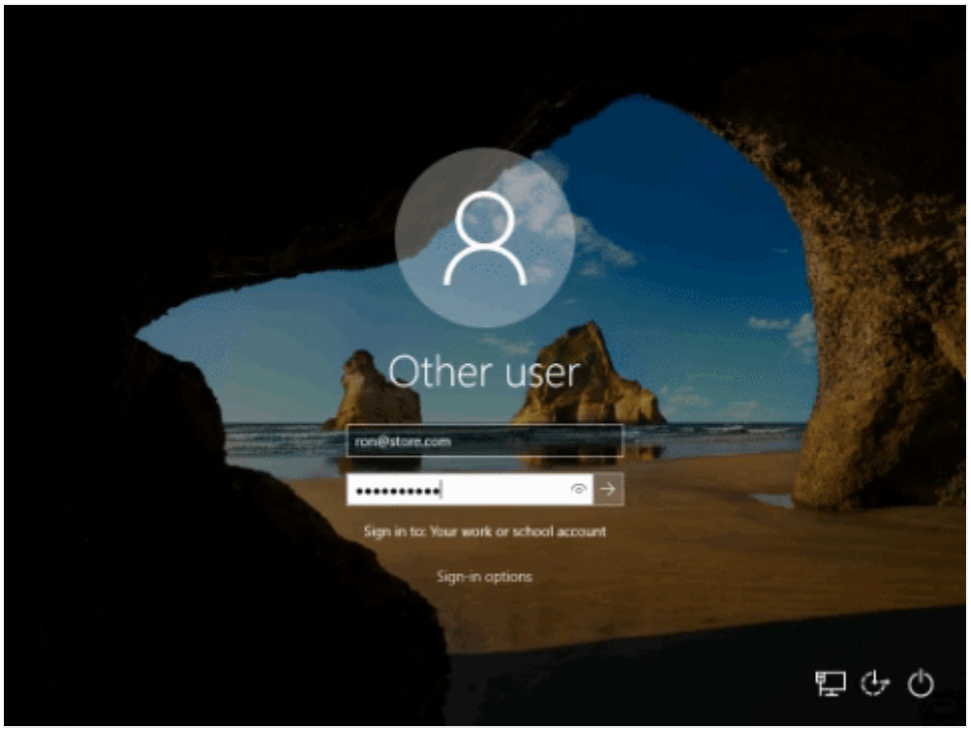
Sign-in

Faster sign-in to a Windows 10 shared pc

If you have shared devices deployed in your work place, **Fast sign-in** enables users to quickly sign in to a shared Windows 10 PC.

To enable fast sign-in

1. Set up a shared or guest device with Windows 10, version 1809 or Windows 10 Enterprise LTSC 2019.
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.

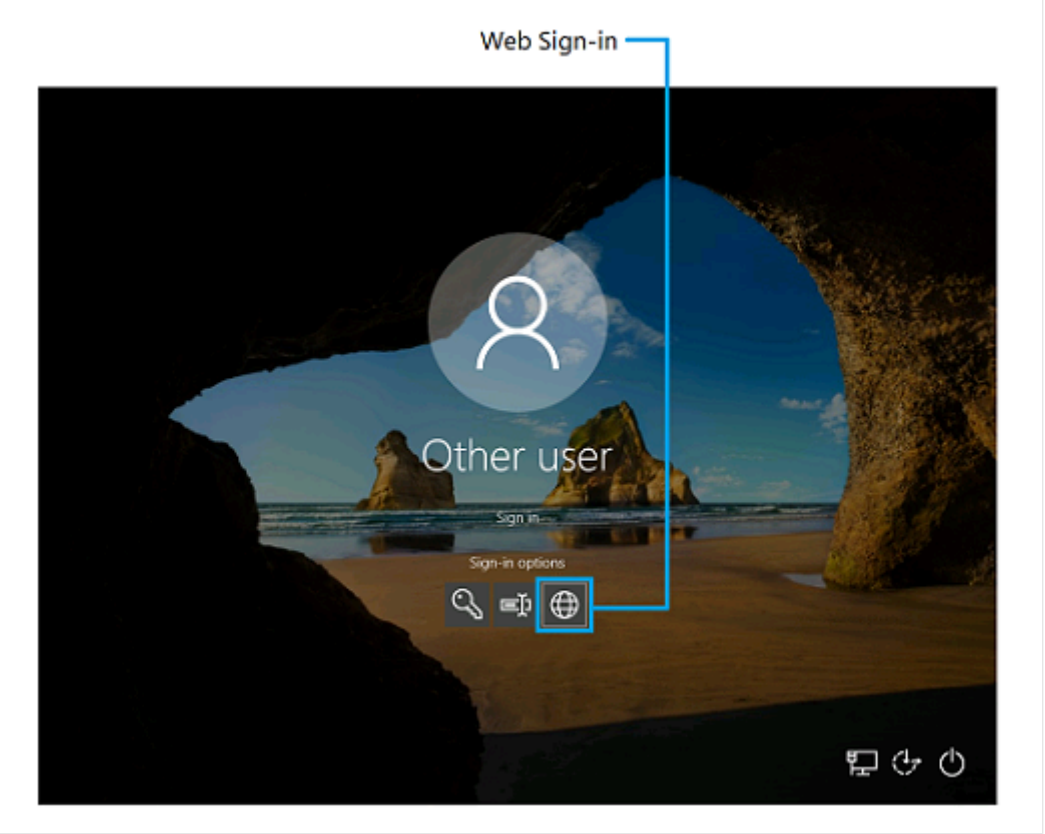


Web sign-in to Windows 10

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

Try out web sign-in

1. Entra ID join your Windows 10 PC. (Web sign-in is only supported on Entra ID-joined PCs).
2. Set the Policy CSP, and the Authentication and EnableWebSignIn policies to enable web sign-in.
3. On the lock screen, select web sign-in under sign-in options.
4. Select "Sign in" to continue.



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.

New capabilities in Update Compliance let you monitor Windows Defender protection status, compare compliance with industry peers, and optimize bandwidth for deploying updates.

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 What's new in the Windows 10 April 2018 Update.

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.

Configuration

Kiosk configuration

The new chromium-based Microsoft Edge has many improvements targeted to kiosks. However, it's not included in the LTSC release of Windows 10. You can download and install Microsoft Edge separately. For more information, see Download and deploy Microsoft Edge for business.

Internet Explorer is included in Windows 10 LTSC releases as its feature set isn't changing, and it will continue to get security fixes for the life of a Windows 10 LTSC release.

If you wish to take advantage of kiosk capabilities in Microsoft Edge, consider Kiosk mode with a semi-annual release channel.

Co-management

Intune and Microsoft Configuration Manager policies have been added to enable hybrid Entra ID-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.

Microsoft Entra ID join in bulk

Using the new wizards in Windows Configuration Designer, you can create provisioning packages to enroll devices in Entra ID. Entra ID 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**

For more information, see Configure Windows Spotlight on the lock screen.

Start and taskbar layout

Previously, the customized taskbar could only be deployed using Group Policy or provisioning packages. Windows 10 Enterprise LTSC 2019 adds support for customized taskbars to MDM.

More 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**
- Other new settings: **Start/HideFrequentlyUsedApps**, **Start/HideRecentlyAddedApps**, **AllowPinnedFolder**, **ImportEdgeAssets**, **Start/HideRecentJumplists**, **Start/NoPinningToTaskbar**, **Settings/PageVisibilityList**, and **Start/HideAppsList**.

Windows Update

Windows Insider for Business

We recently added the option to download Windows 10 Insider Preview builds using your corporate credentials in Microsoft Entra ID. By enrolling devices in Entra ID, 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.

You can now register your Entra ID domains to the Windows Insider Program. For more information, see Windows Insider Program for Business.

Optimize update delivery

With changes delivered in Windows 10 Enterprise LTSC 2019, express updates are now fully supported with Configuration Manager. It's also supported with other third-party updating and management products that implement this new functionality. This support is in addition to current express support on Windows Update, Windows Update client policies, 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 other 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

For more information, see Configure Delivery Optimization for Windows updates.

Uninstalled in-box apps no longer automatically reinstall

Starting with Windows 10 Enterprise LTSC 2019, 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 Enterprise LTSC 2019 machines will stay de-provisioned after future feature update installations. This behavior won't apply to the update from Windows 10 Enterprise LTSC 2016 (or earlier) to Windows 10 Enterprise LTSC 2019.

Management

New MDM capabilities

Windows 10 Enterprise LTSC 2019 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. For more information, 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/region to avoid roaming charges, or the wireless network can be disabled when the device isn't 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.

For more information, see What's new in mobile device enrollment and management.

MDM has been expanded to include domain joined devices with Microsoft Entra ID 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.

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 Enterprise LTSC 2019.

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

MDM diagnostics

In Windows 10 Enterprise LTSC 2019, 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're introducing Microsoft Message Analyzer as another 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 Enterprise LTSC 2019 introduces two new PowerShell cmdlets, **New-AppVSequencerVM** and **Connect-AppvSequencerVM**. These cmdlets 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 clean up your unpublished packages after a device restart.

For more information, see the following articles:

- 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 Enterprise LTSC 2019.

- Group policy settings reference for Windows and Windows Server

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.

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.

Miracast over Infrastructure

In this version of Windows 10, 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).

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 and multicast DNS (mDNS). If the name isn't resolvable via either DNS method, Windows 10 will fall back to establishing the Miracast session using the standard Wi-Fi direct connection.

Miracast over Infrastructure offers many 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 don't 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 isn't optimized for Miracast over Wi-Fi Direct.
- It uses an existing connection that reduces the time to connect and provides a stable stream.

Enabling Miracast over Infrastructure

If you have a device that has been updated to Windows 10 Enterprise LTSC 2019, then you automatically have this new feature. To take advantage of it in your environment, you need to make sure the following requirement exist within your deployment:

- The device (PC or Surface Hub) needs to be running Windows 10, version 1703, Windows 10 Enterprise LTSC 2019, or a later OS.

- A Windows PC or Surface Hub can act as a Miracast over Infrastructure *receiver*. A Windows device 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. For example, 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 device must be connected to the same enterprise network via Ethernet or a secure Wi-Fi connection.

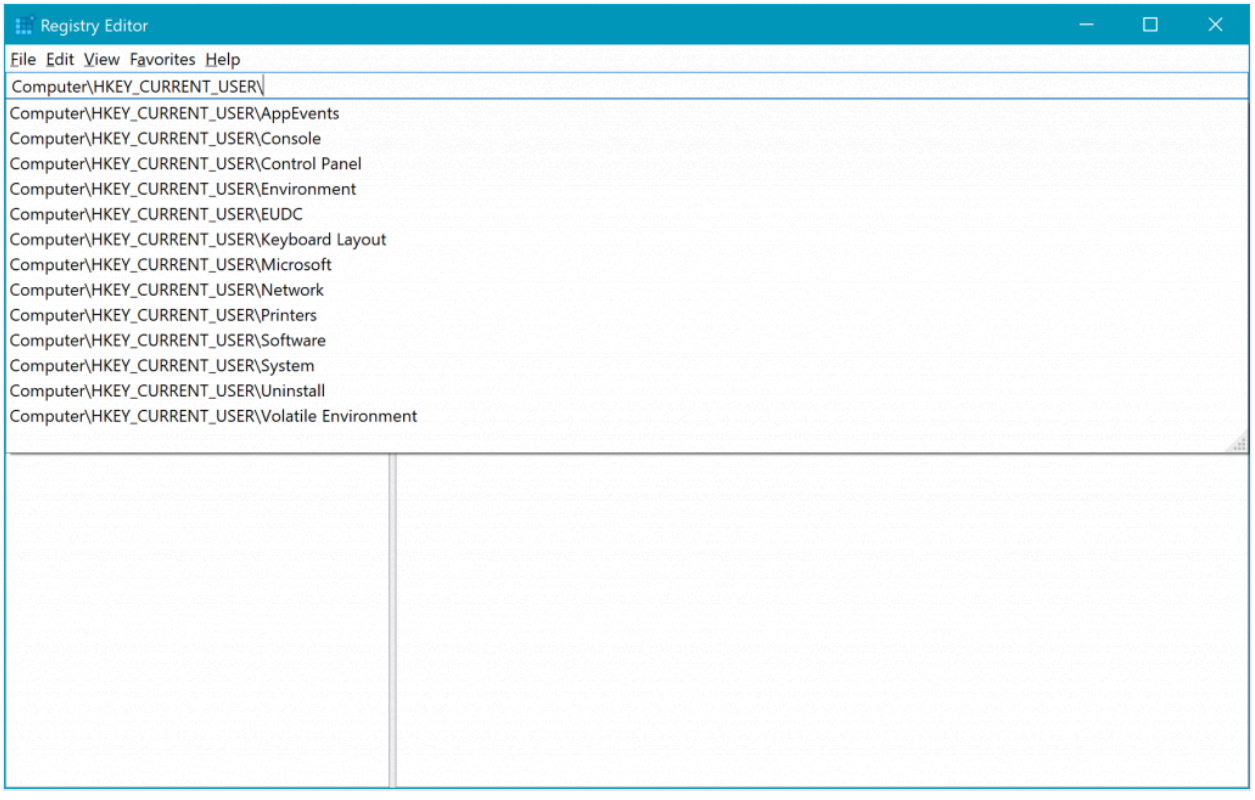
- The DNS Hostname (device name) of the device needs to be resolvable via your DNS servers. You can achieve this configuration by either allowing your device to register automatically via Dynamic DNS, or by manually creating an A or AAAA record for the device's hostname.

- Windows 10 PCs must be connected to the same enterprise network via Ethernet or a secure Wi-Fi connection.

> **ⓘ Important**
>
> 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.

Registry editor improvements

We added a dropdown that displays while 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.



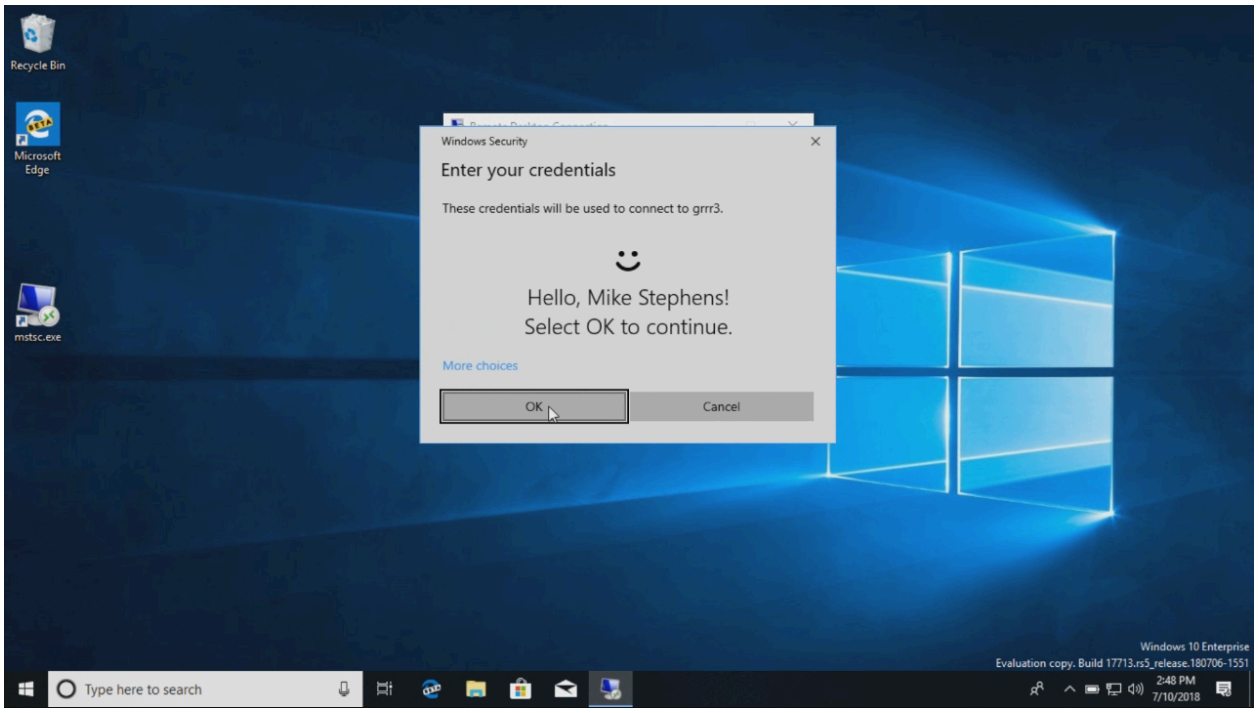
Remote Desktop with Biometrics

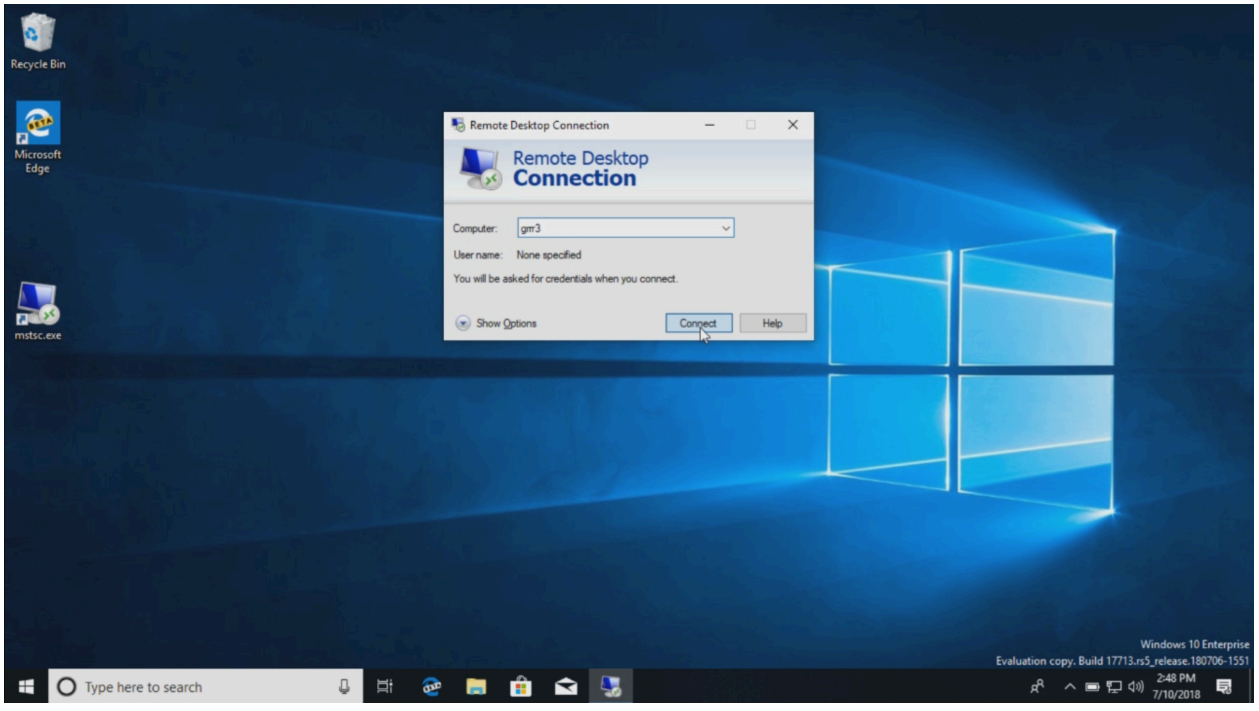
Microsoft Entra ID and Active Directory users using Windows Hello for Business can use biometrics to authenticate to a remote desktop session.

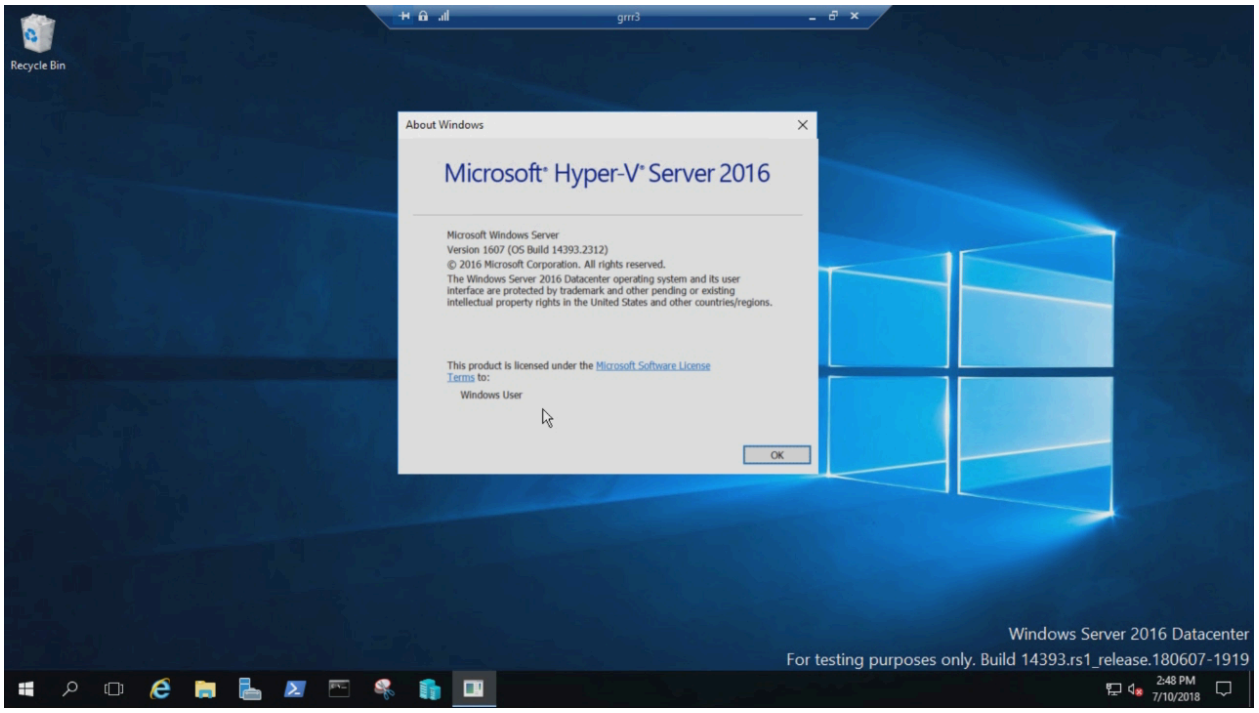
To get started, sign into your device using Windows Hello for Business. Bring up **Remote Desktop Connection** (mstsc.exe), type the name of the computer you want to connect to, and select **Connect**.

- 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 select **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:


Recycle Bin
Microsoft Edge
mstsc.exe
Windows Security
Enter your credentials
These credentials will be used to connect to grrr3.
Hello, Mike Stephens!
Select OK to continue.
More choices
OK
Cancel
Windows 10 Enterprise
Evaluation copy. Build 17713.rs5_release.180706-1551
Type here to search
2:48 PM
7/10/2018


Recycle Bin
Microsoft Edge
mstsc.exe
Remote Desktop Connection
Remote Desktop Connection
Computer: grrr3
User name: None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help
Windows 10 Enterprise
Evaluation copy. Build 17713.rs5_release.180706-1551
Type here to search
2:48 PM
7/10/2018



See also

Windows 10 Enterprise LTSC: A short description of the LTSC servicing channel with links to information about each release.

Feedback

Was this page helpful? Yes No

Provide product feedback

What's new in Windows 10 Enterprise LTSC 2016

Article • 07/17/2024 • Applies to: ✅ Windows 10 Enterprise LTSC 2016

This article lists new and updated features and content that are of interest to IT pros for Windows 10 Enterprise LTSC 2016 (LTSB), compared to Windows 10 Enterprise LTSC 2015 (LTSB). For a brief description of the LTSC servicing channel, see Windows 10 Enterprise LTSC.

> **Note**
>
> Windows 10 Enterprise LTSC 2016 was first available on August 2, 2016. Features in Windows 10 Enterprise LTSC 2016 are equivalent to Windows 10, version 1607.

Deployment

Windows Imaging and Configuration Designer (ICD)

In previous versions of the Windows 10 Assessment and Deployment Kit (ADK), you had to install more features for Windows ICD to run. Starting in this version of Windows 10, 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.

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 was first shipped, it included Microsoft Passport and Windows Hello, which worked together to provide multifactor authentication. To simplify deployment and improve supportability, Microsoft has combined these technologies into a single solution under the Windows Hello name in this version of Windows 10. Customers who have already deployed Microsoft Passport for Work won't 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.

Other changes for Windows Hello in Windows 10 Enterprise LTSC 2016:

- Personal (Microsoft account) and corporate (Active Directory or Entra ID) 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 this version of Windows 10, Windows Hello as a convenience PIN is disabled by default on all domain-joined computers. To enable a convenience PIN, enable the Group Policy setting **Turn on convenience PIN sign-in**.

Learn more about Windows Hello for Business.

BitLocker

New BitLocker features

- **XTS-AES encryption algorithm**. BitLocker now supports the XTS-AES encryption algorithm. XTS-AES provides extra 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.

Security auditing

New Security auditing features

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

Trusted Platform Module

New TPM features

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

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.

Learn more about Windows Information Protection (WIP).

Windows Defender

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

- 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 use 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.

Microsoft Defender for Endpoint

With the growing threat from more sophisticated targeted attacks, a new security solution is imperative in securing an increasingly complex network ecosystem. Microsoft Defender for Endpoint 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 Microsoft Defender for Endpoint.

VPN security

- The VPN client can integrate with the Conditional Access Framework, a cloud-based policy engine built into Microsoft Entra ID, to provide a device compliance option for remote clients.
- The VPN client can integrate with Windows Information Protection (WIP) policy to provide extra 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 VPNv2 CSP
- Microsoft Intune: *VPN* profile template includes support for native VPN plug-ins. For more information, see Create VPN profiles to connect to VPN servers in Intune.

Management

Use Remote Desktop Connection for PCs joined to Microsoft Entra ID

From its release, Windows 10 has supported remote connections to PCs that are joined to Active Directory. Starting in this version of Windows 10, you can also connect to a remote PC that is joined to Microsoft Entra ID. 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 this version of Windows 10, see What's new in MDM enrollment and management.

Shared PC mode

This version of Windows 10, 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 this version of Windows 10, App-V is included with the Windows 10 for Enterprise edition. If you're 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 sign in, their personalized settings are applied to their work session, regardless of which device or virtual desktop infrastructure (VDI) sessions they sign in to.

With the release of this version of Windows 10, UE-V is included with the Windows 10 for Enterprise edition. If you're 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.

Microsoft Edge

The new chromium-based Microsoft Edge isn't included in the LTSC release of Windows 10. However, you can download and install it separately. For more information, see Download and configure Microsoft Edge for Business.

See Also

Windows 10 Enterprise LTSC: A description of the LTSC servicing channel with links to information about each release.

Feedback

What's new in Windows 10 Enterprise LTSC 2015

Article • 07/09/2024 • Applies to: ✅ Windows 10 Enterprise LTSC 2015

This article lists new and updated features and content that are of interest to IT pros for Windows 10 Enterprise LTSC 2015 (LTSB). For a brief description of the LTSC servicing channel, see Windows 10 Enterprise LTSC.

> **Note**
>
> Windows 10 Enterprise LTSC 2015 was first available on July 29, 2015. Features in Windows 10 Enterprise LTSC 2015 are equivalent to Windows 10, version 1507.

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. An IT administrator who uses Windows Provisioning can easily specify the configuration and settings required to enroll devices into management using a wizard-driven user interface, and then apply this configuration to target devices in a matter of minutes. It's 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

AppLocker was available for Windows 8.1, and is improved with Windows 10. See Requirements to use AppLocker for a list of operating system requirements.

Enhancements to AppLocker in Windows 10 include:

- 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 parameter, set the **ServiceEnforcement** to **Enabled**.
- A new AppLocker configuration service provider was added to allow you to enable AppLocker rules by using an MDM server.

Learn how to manage AppLocker within your organization.

BitLocker

Enhancements to AppLocker in Windows 10 include:

- **Encrypt and recover your device with Microsoft Entra**. In addition to using a Microsoft Account, automatic device encryption can now encrypt your devices that are joined to a Microsoft Entra domain. When the device is encrypted, the BitLocker recovery key is automatically escrowed to Microsoft Entra. This escrow 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 information, see BitLocker preboot recovery screen.

Learn how to deploy and manage BitLocker within your organization.

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.

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 Entra ID 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

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 sign-in 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 sign-in. 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 can't 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 don't 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 is 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 information 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 setting 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 process under **Advanced Audit Policy Configuration\Object Access\Audit Kernel Object**. This process-when enabled-can help identify attacks that steal credentials from the memory of a process.

New fields in the sign-in event

The sign-in 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 signed in to the PC is a computer account, this field will be yes. Otherwise, the field is no.
2. **ElevatedToken** String: yes or no If an account has signed in to the PC through the "administrative sign-in" method, this field will be yes. Otherwise, the field is no. Additionally, if this field is part of a split token, the linked sign-in 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.

New fields in the process creation event

The sign-in 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 sign-in 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.

Trusted Platform Module

New TPM features in Windows 10

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 shouldn't turn off UAC because such a setting isn't supportive of devices running Windows 10. If you do turn off UAC, all Universal Windows Platform apps stop working. You must always set the **HKLM\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 **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin** registry value to 0, which is the same as setting the UAC slider Never Notify. This setting isn't recommended for devices running Windows 10.

For more info about how to manage UAC, see UAC group policy settings and registry key settings.

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

- **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 Entra ID 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.

Expand table

Area	Choices
Identity	Active Directory; Azure AD
Grouping	Domain join; Workgroup; Azure AD join
Device management	Group Policy; Microsoft 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.

Start layout

A standard 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.

Updates

Windows Update client policies enable 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 client policies are an easily established and implemented system that 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 efficient.
- **Use with existing tools** such as Microsoft Intune and Configuration Manager.

Together, these Windows Update client policies features help reduce device management costs, provide controls over update deployment, offer quicker access to security updates, and provide access to the latest innovations from Microsoft on an ongoing basis. Windows Update client policies are 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 Microsoft Configuration Manager.

Learn more about Windows Update client policies.

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

Microsoft Edge

The new chromium-based Microsoft Edge isn't included in the LTSC release of Windows 10. However, you can download and install it separately here.

See Also

Windows 10 Enterprise LTSC: A description of the LTSC servicing channel with links to information about each release.

Feedback

Was this page helpful? Yes No

Provide product feedback

Windows Commercial Licensing overview

Article • 12/02/2024 • Applies to: ✅ Windows 11

This document provides an overview of the products and use rights available through Microsoft Commercial Licensing, information about the products that are eligible for upgrades, and the key choices you have for using Windows in your organization.

> **Note**
>
> The content of this article doesn't replace or override other licensing documentation, such as the Windows 11 End User License Agreement or Commercial Licensing Product Terms.

Windows 11 editions

The following table lists the editions of Windows 11 available through each Microsoft distribution channel:

Expand table

Full Packaged Product (Retail)	Preinstalled on device (OEM)	Commercial Licensing
Windows 11 Home Windows 11 Pro	Windows 11 Home Windows 11 Pro	Windows 11 Pro Windows 11 Enterprise Windows 11 Enterprise LTSC

Windows desktop offerings available through Commercial Licensing

The following offerings are available for purchase through Microsoft Commercial Licensing:

Expand table

Product	Description	Availability
Windows 11 Pro Upgrade	Windows 11 Pro is designed for small and medium businesses. Windows 11 Pro enables organizations	The Windows 11 Pro Upgrade in Commercial

Product	Description	Availability
	to manage devices and apps, protect their data, facilitate remote and mobile scenarios, while taking advantage of the cloud technologies that support their business. Windows 11 Pro devices are a good choice for organizations that support *choose your own device (CYOD)* programs and *prosumer* customers.	Licensing upgrades a device from a previous version of Windows Pro.
Windows 11 Enterprise E3	Windows 11 Enterprise E3 is intended for large and medium-sized organizations. It includes Windows Enterprise edition with cloud-powered capabilities and subscription use rights. Examples include advanced identity protection, the broadest range of options for operating system deployment, update control, and device management.	Windows 11 Enterprise E3 is available **per-user** in Commercial Licensing programs. It requires Windows Pro as qualifying operating systems.
Windows 11 Enterprise E5	Windows 11 Enterprise E5 is for organizations that want to take advantage of everything in Windows 11 Enterprise E3 with the addition of **Microsoft Defender for Endpoint Plan 2**, a service that helps enterprises detect, investigate, and respond to advanced cybersecurity attacks on their endpoints and networks.	Windows 11 Enterprise E5 is available **per-user** in Commercial Licensing programs. It requires Windows Pro as qualifying operating systems.
Windows 10 Enterprise LTSC	Windows 10 Enterprise LTSC is designed for devices that have strict change-management policies with only security and critical bug fixes. By using a Long-Term Servicing Channel edition, you can apply monthly Windows 10 security updates for specialized devices while holding back new-feature updates for an extended period of time, up to five years.	Windows Enterprise LTSC is available in the **per-user** and **per-device** model, depending on the Volume Licensing program through which it's acquired.
Windows Virtual Desktop Access (VDA) Subscription License	The Windows VDA subscription license provides the right to access virtual Windows desktop environments from devices that aren't covered by a Commercial Licensing offer that includes VDA rights, such as thin clients.	Windows VDA is available on a **per-device** and **per-user** basis.

Windows 11 Pro Upgrade license

Windows 11 Pro is designed for small and medium businesses. Windows 11 Pro enables you to manage your devices and apps, protect your business data, facilitate remote and mobile scenarios, and take advantage of the cloud technologies for your organization.

The Windows 11 Pro Upgrade license is recommended if you want to:

- Upgrade a Windows 10 Pro device to Windows 11 Pro
- Upgrade Windows 7/8/8.1 Pro devices to Windows 10 Pro

Windows 11 Enterprise

There are two core Windows 11 Enterprise offers: **Windows 11 Enterprise E3** and **Windows 11 Enterprise E5**. These offers can be purchased on a **per-user basis**, and are only available through **Commercial Licensing**, including the **Cloud Solution Provider** program.

Windows 11 Enterprise E3

Windows 11 Enterprise E3 builds on Windows 11 Pro by adding more advanced features designed to address the needs of large and mid-size organizations. Examples include advanced protection against modern security threats, the broadest range of options for operating system deployment and update, and comprehensive device and app management.

> **Note**
>
> Windows Enterprise E3 is a **per user subscription**, intended for organizations. It includes **Windows Enterprise edition** with cloud-powered capabilities and **subscription use rights**. Windows Enterprise E3 is usually licensed through Volume Licensing programs and is an upgrade from Windows Pro.

Windows 11 Enterprise features

The following table describes the unique Windows Enterprise edition features:

Expand table

OS-based feature	Description
Credential Guard	Protects against user credential harvesting and pass-the-hash attacks or pass the token attacks.
Managed Microsoft Defender Application Guard (MDAG) for Microsoft Edge	Isolates enterprise-defined untrusted sites with virtualization-based security from Windows, protecting your organization while users browse the Internet.
Modern BitLocker Management	Allows you to eliminate on-premises tools to monitor and support BitLocker recovery scenarios.

OS-based feature	Description
Personal Data Encryption	Encrypts individual's content using Windows Hello for Business to link the encryption keys to user credentials.
Direct Access	Connect remote users to the organization network without the need for traditional VPN connections.
Always-On VPN device tunnel	Advanced security capabilities to restrict the type of traffic and which applications can use the VPN connection.
Windows Experience customization	Settings to lock down the user experience of corporate desktops and Shell Launcher with Unified Write Filter for frontline workers devices or public kiosks.

Windows 11 Enterprise cloud-based capabilities

The following table describes the unique Windows Enterprise cloud-based features:

Expand table

Cloud-based feature	Description
Windows subscription activation	Enables you to *step-up* from **Windows Pro edition** to **Enterprise edition**. You can eliminate license key management and the deployment of Enterprise edition images.
Windows Autopatch	Cloud service that puts Microsoft in control of automating updates to Windows, Microsoft 365 Apps for enterprise, Microsoft Edge, and Microsoft Teams.
Universal Print	Removes the need for on-premises print servers and enables any endpoint to print to cloud registered printers.
Microsoft Connected Cache	A software solution that caches app and OS updates on the local network to save Internet bandwidth in locations with limited connectivity.
Endpoint analytics proactive remediation	Helps you fix common support issues before end-users notice them.
Organizational messages	Keeps employees informed with organizational messages directly inserted in Windows UI surfaces.

Windows 11 Enterprise licensing use rights

The following table describes the Windows Enterprise licensing use rights:

Expand table

Licensing use rights	Description
Five Windows instances per licensed user	Allows your employees to simultaneously use a Windows laptop, a cloud PC and a specialized device with Windows LTSC, and more.
36 months (3 years) support on annual feature releases	Get extra time to deploy feature releases.
Azure Virtual Desktop, Windows 365 Enterprise and Virtual Desktop Access	Empower flexible work styles and smarter work with the included virtualization access rights. Includes FSLogix for a consistent experience of
Windows user profiles in virtual desktop environments.	
Windows release health in the Microsoft 365 admin center	Gives you essential information about monthly quality and feature updates in the Microsoft 365 admin center.
Windows feature update device readiness report	Provides per-device information about compatibility risks that are associated with an upgrade or update to a chosen version of Windows.
Windows feature update compatibility risks reports	Provides a summary view of the top compatibility risks, so you understand which compatibility risks impact the greatest number of devices in your organization.
Windows LTSC Enterprise	Intended for highly specialized devices that require limited changes due to regulations and certification
Microsoft Desktop Optimization Pack (MDOP)	Help improve compatibility and management, reduce support costs, improve asset management, and improve policy control.

Learn more about Windows 11 Enterprise E3 .

Windows 11 Enterprise E5

Windows 11 Enterprise E5 is for organizations that want to take advantage of everything in Windows 11 Enterprise E3 with the addition of **Microsoft Defender for Endpoint Plan 2**, a cloud service that helps enterprises detect, investigate, and respond to advanced cybersecurity attacks on their endpoints and networks.

Building on the existing security defenses in Windows 11, Microsoft Defender for Device provides a post-breach layer of protection to the Windows 11 security stack. With a combination of client technology built into Windows 11 and a robust cloud service, it

can help detect threats that have made it past other defenses, provide enterprises with information to investigate the breach across endpoints, and offer response recommendations.

> **Note**
>
> Windows 11 Enterprise E5 is available per user in Commercial Licensing programs.

Windows Enterprise E3 in Microsoft 365 F3

Windows Enterprise E3 subscription license in Microsoft 365 F3 has all the OS features, and most of the cloud services and use rights, included with regular Windows Enterprise E3. Windows Enterprise E3 in Microsoft 365 F3 does not include some use rights previously included in Software Assurance benefits that come with the regular E3 user subscription license. F3 does not come with:

- Microsoft Desktop Optimization Pack (MDOP)
- Windows LTSC Enterprise
- Windows Autopatch

Use a Windows Pro device with the Windows Enterprise user subscription license

In most cases, the Windows Pro edition comes pre-installed on a business-class device. Microsoft recommends upgrading your Windows Pro devices to Enterprise edition when you have acquired a user subscription license for Windows. However, there are cases that require to keep devices on the Pro edition and not upgrade them to Enterprise edition. With Windows 11 Enterprise E3, you can take advantage of features, services and use rights not licensed to the Windows Pro license bound to the device. It includes Windows Enterprise edition with cloud-powered capabilities and subscription use rights, and these capabilities are not always technically enforced. Some scenarios that may require to not upgrade to Windows Enterprise edition:

- Devices not properly provisioned that don't automatically upgrade to Windows Enterprise edition
- Devices may have been acquired for a business process that was not under control of a central IT department or outside of the IT department's knowledge
- Devices may be used temporarily for a project by vendors and added to the IT infrastructure, but not upgraded to Enterprise edition

- A developer that is developing applications that must be tested and certified on Pro, as that is how it will be delivered to customers
- A Windows Pro device that was pre-configured for a specific purpose and is certified on Pro only

In these cases, you want the PC to be configured, secured, monitored, and updated with the enterprise management and security tools that come with the Windows Enterprise user subscription. Your Windows Enterprise E3 subscription doesn't block these scenarios.

The following table lists the Windows 11 Enterprise features and their Windows edition requirements:

Expand table

OS-based feature	Windows Pro	Windows Enterprise
Credential Guard	✗	Yes
Microsoft Defender Application Guard (MDAG) for Microsoft Edge	Yes	Yes
Modern BitLocker Management	Yes	Yes
Personal Data Encryption	✗	Yes
Direct Access	Yes	Yes
Always On VPN	Yes	Yes
Windows Experience customization	✗	Yes

The following table lists the Windows 11 Enterprise cloud-based features and their Windows edition requirements:

Expand table

Cloud-based feature	Windows Pro	Windows Enterprise
Windows subscription activation	Yes	Yes
Windows Autopatch	Yes	Yes
Universal Print	Yes	Yes
Microsoft Connected Cache	Yes	Yes

Cloud-based feature	Windows Pro	Windows Enterprise
Endpoint analytics proactive remediation	Yes	Yes
Organizational messages	✗	Yes

The following table lists the Windows 11 Enterprise E3 licensing use rights and their Windows edition requirements:

Expand table

Licensing use rights	Windows Pro	Windows Enterprise
Five Windows instances per licensed user	n/a	n/a
36 months (3 years) support on annual feature releases	✗	Yes
Azure Virtual Desktop, Windows 365 Enterprise and Virtual Desktop Access	n/a	n/a
Windows release health in the Microsoft 365 admin center	n/a	n/a
Windows feature update device readiness report	Yes	Yes
Windows feature update compatibility risks reports	Yes	Yes
Windows LTSC Enterprise	n/a	n/a
Microsoft Desktop Optimization Pack (MDOP)	Yes	Yes

Next steps

To learn more about Windows 11 Enterprise E3 and E5 licensing, download the Windows 11 licensing guide. The guide provides additional information to complement the information in this article, including:

- Description of qualifying operating systems
- Availability of Windows desktop operating system products in licensing programs
- Deciding between per-device and per-user licensing
- Windows 11 downgrade rights
- Volume license activation methods
- How to acquire licenses through Commercial Licensing

Feedback

Was this page helpful? Yes No

Provide product feedback

Windows client features lifecycle

Article • 07/09/2024 • Applies to: ✅ Windows 11, ✅ Windows 10

Each release of Windows 10 and Windows 11 contains many new and improved features. Occasionally we also remove features and functionality, usually because there's a better option.

Windows 11 features

For information about features that are impacted when you upgrade from Windows 10 to Windows 11, see Feature deprecations and removals.

Features no longer being developed

The following article lists features that are no longer being developed. These features might be removed in a future release.

Deprecated Windows features

Features removed

The following article has details about features that have been removed from Windows 10 or Windows 11. This includes features that are present in Windows 10, but are removed in Windows 11.

Removed Windows features

Terminology

The following terms can be used to describe the status that might be assigned to a feature during its lifecycle:

- **Deprecation**: The stage of the product lifecycle when a feature or functionality is no longer in active development and may be removed in future releases of a product or online service.
- **End of support**: The stage of the product lifecycle when support and servicing are no longer available for a product.
- **Retirement**: The stage of the product lifecycle when a service is shut down so that it's no longer available for use.

- **Remove or retire a feature**: The stage of the product lifecycle when a feature or functionality is taken out of a service after it has been marked as deprecated. The feature is removed from newer versions of Windows, but still exists in older versions and is supported until those versions reach **end of support** stage.
- **Replace a feature**: The stage of the product lifecycle when a feature or functionality in a service is replaced with a different feature or functionality.

Also see

Windows release information

Feedback

Was this page helpful? Yes No

Provide product feedback

Deprecated features for Windows client

Article • 02/19/2025 • Applies to: ✅ Windows 11, ✅ Windows 10

Each version of Windows client adds new features and functionality. Occasionally, new versions also remove features and functionality, often because they added a newer option. This article provides details about the features and functionalities that are no longer being developed in Windows client. For more information about features that were removed, see Windows features removed.

- To understand the distinction between *deprecation* and *removal*, see Windows client features lifecycle.
- For more information about how deprecation fits into the Windows lifecycle, see Deprecation: What it means in the Windows lifecycle.
- For more information about features removed on upgrade to Windows 11 from Windows 10, see Feature deprecations and removals.

The features in this article are no longer being actively developed, and might be removed in a future update. Some features were replaced with other features or functionality and some are now available from other sources.

> **Tip**
>
> You can use RSS to be notified when this page is updated. For example, the following RSS link includes this article:
>
> url
>
> ```
> https://learn.microsoft.com/api/search/rss?
> search=%22details+about+the+features+and+functionalities+that+are+no+lo
> nger+being+developed+in+Windows%22&locale=en-
> us&%24filter=%28category+eq+%27Documentation%27%29
> ```
>
> This example includes the `&locale=en-us` variable. The `locale` variable is required, but you can change it to another supported locale. For example, `&locale=ja-jp`.
>
> For more information on using RSS for notifications, see How to use the docs in the Intune documentation.

Deprecated features

The following list is subject to change and might not include every affected feature or functionality.

> **Note**
>
> If you have feedback about the proposed replacement of any of these features, you can use the Feedback Hub app.

Expand table

Feature	Details and mitigation	Deprecation announced
Line printer daemon (LPR/LPD)	Deprecation reminder: The line printer daemon protocol (LPR/LPD) was deprecated starting in Windows Server 2012. As removal of the line printer daemon protocol nears, we'd like to remind customers to ensure their environments are prepared for removal. When these features are eventually removed, clients that print to a server using this protocol, such as UNIX clients, will not be able to connect or print. Instead, UNIX clients should use IPP. Windows clients can connect to UNIX shared printers using the Windows Standard Port Monitor.	Original announcement: Windows Server 2012 Courtesy reminder: February 2025
Location History	We are deprecating and removing the Location History feature, an API that allowed Cortana to access 24 hours of device history when location was enabled. With the removal of the Location History feature, location data will no longer be saved locally and the corresponding settings will also be removed from the **Privacy & Security** > **Location** page in **Settings**.	February 2025
Suggested actions	Suggested actions that appear when you copy a phone number or future date in Windows 11 are deprecated and will be removed in a future Windows 11 update.	December 2024
Legacy DRM services	Legacy DRM services, used by either Windows Media Player, Silverlight clients, Windows 7, or Windows 8 clients are deprecated. The following functionality won't work when these services are fully retired: • Playback of protected content in the legacy Windows Media Player on Windows 7	September 2024

Feature	Details and mitigation	Deprecation announced
	• Playback of protected content in a Silverlight client and Windows 8 clients • In-home streaming playback from a Silverlight client or Windows 8 client to an Xbox 360 • Playback of protected content ripped from a personal CD on Windows 7 clients using Windows Media Player	
Paint 3D	Paint 3D is deprecated and will be removed from the Microsoft Store on November 4, 2024. To view and edit 2D images, you can use Paint or Photos. For viewing 3D content, you can use 3D Viewer. For more information, see Resources for deprecated features.	August 2024
Adobe Type1 fonts	Adobe PostScript Type1 fonts are deprecated and support will be removed in a future release of Windows. In January 2023, Adobe announced the end of support for PostScript Type1 fonts for their latest software offerings. Remove any dependencies on this font type by selecting a supported font type. To display currently installed fonts, go to **Settings** > **Personalization** > **Fonts**. Application developers and content owners should test their apps and data files with the Adobe Type1 fonts removed. For more information, contact the application vendor or Adobe.	August 2024
DirectAccess	DirectAccess is deprecated and will be removed in a future release of Windows. We recommend migrating from DirectAccess to Always On VPN.	June 2024
NTLM	All versions of NTLM, including LANMAN, NTLMv1, and NTLMv2, are no longer under active feature development and are deprecated. Use of NTLM will continue to work in the next release of Windows Server and the next annual release of Windows. Calls to NTLM should be replaced by calls to Negotiate, which tries to authenticate with Kerberos and only falls back to NTLM when necessary. For more information, see, Resources for deprecated features. **[Update - November 2024]**: NTLMv1 is removed	June 2024

Feature	Details and mitigation	Deprecation announced
	starting in Windows 11, version 24H2 and Windows Server 2025.	
Driver Verifier GUI (verifiergui.exe)	Driver Verifier GUI, verifiergui.exe, is deprecated and will be removed in a future version of Windows. You can use the Verifier Command Line (verifier.exe) instead of the Driver Verifier GUI.	May 2024
NPLogonNotify and NPPasswordChangeNotify APIs	Starting in Windows 11, version 24H2, the inclusion of password payload in MPR notifications is set to `disabled` by default through group policy in NPLogonNotify and NPPasswordChangeNotify APIs. The APIs may be removed in a future release. The primary reason for disabling this feature is to enhance security. When enabled, these APIs allow the caller to retrieve a user's password, presenting potential risks for password exposure and harvesting by malicious users. To include password payload in MPR notifications, set the EnableMPRNotifications policy to `enabled`.	March 2024
TLS server authentication certificates using RSA keys with key lengths shorter than 2048 bits	Support for certificates using RSA keys with key lengths shorter than 2048 bits is deprecated. Internet standards and regulatory bodies disallowed the use of 1024-bit keys in 2013, recommending specifically that RSA keys should have a key length of 2048 bits or longer. For more information, see Transitioning of Cryptographic Algorithms and Key Sizes - Discussion Paper (nist.gov). This deprecation focuses on ensuring that all RSA certificates used for TLS server authentication must have key lengths greater than or equal to 2048 bits to be considered valid by Windows. TLS certificates issued by enterprise or test certification authorities (CA) aren't impacted with this change. However, we recommend that they be updated to RSA keys greater than or equal to 2048 bits as a security best practice. This change is necessary to preserve security of Windows customers using certificates for authentication and cryptographic purposes.	March 2024
Test Base	Test Base for Microsoft 365, an Azure cloud service for application testing, is deprecated. The service	March 2024

Feature	Details and mitigation	Deprecation announced
	will be retired in the future and will be no longer available for use after retirement.	
Windows Mixed Reality	Windows Mixed Reality is deprecated and will be removed in Windows 11, version 24H2. This deprecation includes the Mixed Reality Portal app, Windows Mixed Reality for SteamVR, and Steam VR Beta. Existing Windows Mixed Reality devices will continue to work with Steam through November 2026, if users remain on their current released version of Windows 11, version 23H2. After November 2026, Windows Mixed Reality will no longer receive security updates, nonsecurity updates, bug fixes, technical support, or online technical content updates.	December 2023
Microsoft Defender Application Guard for Edge	Microsoft Defender Application Guard, including the Windows Isolated App Launcher APIs, is deprecated for Microsoft Edge for Business and will no longer be updated. To learn more about Edge for Business security capabilities, see Microsoft Edge security for your business. **[Update - October 2024]**: Starting with Windows 11, version 24H2, Microsoft Defender Application Guard, including the Windows Isolated App Launcher APIs, is no longer available. **[Update - April 2024]**: Because Application Guard is deprecated there won't be a migration to Edge Manifest V3. The corresponding extensions and associated Windows Store app won't be available after May 2024. This change affects the following browsers: *Application Guard Extension - Chrome* and *Application Guard Extension - Firefox*. If you want to block unprotected browsers until you're ready to retire MDAG usage in your enterprise, we recommend using AppLocker policies or Microsoft Edge management service. For more information, see Microsoft Edge and Microsoft Defender Application Guard.	December 2023
Legacy console mode	The legacy console mode is deprecated and no longer being updated. In future Windows releases, it will be available as an optional Feature on Demand. This feature won't be installed by default.	December 2023

Feature	Details and mitigation	Deprecation announced
Windows speech recognition	Windows speech recognition is deprecated and is no longer being developed. This feature is being replaced with voice access. Voice access is available for Windows 11, version 22H2, or later devices. Currently, voice access supports five English locales: English - US, English - UK, English - India, English - New Zealand, English - Canada, and English - Australia. For more information, see Setup voice access.	December 2023
Microsoft Defender Application Guard for Office	Microsoft Defender Application Guard for Office, including the Windows Isolated App Launcher APIs, is being deprecated and will no longer be updated. We recommend transitioning to Microsoft Defender for Endpoint attack surface reduction rules along with Protected View and Windows Defender Application Control.	November 2023
Steps Recorder (psr.exe)	Steps Recorder is no longer being updated and will be removed in a future release of Windows. For screen recording, we recommend the Snipping Tool, Xbox Game Bar, or Microsoft Clipchamp.	November 2023
Tips	The Tips app is deprecated and will be removed in a future release of Windows. Content in the app will continue to be updated with information about new Windows features until the app is removed.	November 2023
Computer Browser	The Computer Browser driver and service are deprecated. The browser (browser protocol and service) is a dated and insecure device location protocol. This protocol, service, and driver were first disabled by default in Windows 10 with the removal of the SMB1 service. For more information on Computer Browser, see MS-BRWS Common Internet File System.	November 2023
Webclient (WebDAV) Service	The Webclient (WebDAV) service is deprecated. The Webclient service isn't started by default in Windows. For more information on WebDAV, see WebDAV - Win32 apps.	November 2023
Remote Mailslots	Remote Mailslots are deprecated. The Remote Mailslot protocol is a dated, simple, unreliable, insecure IPC method first introduced in MS DOS. This protocol was first disabled by default in	November 2023

Feature	Details and mitigation	Deprecation announced
	Windows 11 Insider Preview Build. For more information on Remote Mailslots, see About Mailslots and [MS-MAIL]: Remote Mailslot Protocol.	
Timeline for Microsoft Entra accounts	Cross-device syncing of Microsoft Entra user activity history will stop starting in January 2024. Microsoft will stop storing this data in the cloud, aligning with the previous change for Microsoft accounts (MSA) in 2021. The timeline user experience was retired in Windows 11, although it remains in Windows 10. The timeline user experience and all your local activity history still remains on Windows 10 devices. Users can access web history using their browser and access recent files through OneDrive and Office.	October 2023
VBScript	VBScript is deprecated. In future releases of Windows, VBScript will be available as a feature on demand before its removal from the operating system. For more information, see Resources for deprecated features.	October 2023
WordPad	WordPad is no longer being updated and will be removed in a future release of Windows. We recommend Microsoft Word for rich text documents like .doc and .rtf and Windows Notepad for plain text documents like .txt. **[Update - March 2024]**: WordPad will be removed from all editions of Windows starting in Windows 11, version 24H2 and Windows Server 2025. If you're a developer and need information about the affected binaries, see Resources for deprecated features.	September 1, 2023
AllJoyn	Microsoft's implementation of AllJoyn, which included the Windows.Devices.AllJoyn API namespace, a Win32 API, a management configuration service provider (CSP), and an Alljoyn Router Service is deprecated. AllJoyn, sponsored by AllSeen Alliance, was an open source discovery and communication protocol for Internet of Things scenarios such as turning on/off lights or reading temperatures.AllSeen Alliance promoted the AllJoyn project from 2013 until 2016 when it merged with the Open Connectivity Foundation	August 17, 2023

Feature	Details and mitigation	Deprecation announced
	(OCF), the sponsors of Iotivity.org, another protocol for Internet of Things scenarios. Customers should refer to the Iotivity.org website for alternatives such as Iotivity Lite or Iotivity.	
TLS 1.0 and 1.1	Over the past several years, internet standards and regulatory bodies have deprecated or disallowed TLS versions 1.0 and 1.1 due to various security issues. Starting in Windows 11 Insider Preview builds for September 2023 and continuing in future Windows OS releases, TLS 1.0 and 1.1 will be disabled by default. This change increases the security posture of Windows customers and encourages modern protocol adoption. For organizations that need to use these versions, there's an option to re-enable TLS 1.0 or TLS 1.1. For more information, see Resources for deprecated features.	August 1, 2023
Cortana in Windows	Cortana in Windows as a standalone app is deprecated. This change only impacts Cortana in Windows, and your productivity assistant, Cortana, will continue to be available in Outlook mobile, Teams mobile, Microsoft Teams display, and Microsoft Teams rooms.	June 2023
Microsoft Support Diagnostic Tool (MSDT)	MSDT is deprecated and will be removed in a future release of Windows. MSDT is used to gather diagnostic data for analysis by support professionals. For more information, see Resources for deprecated features	January 2023
Universal Windows Platform (UWP) Applications for 32-bit Arm	This change is applicable only to devices with an Arm processor, for example Snapdragon processors from Qualcomm. If you have a PC built with a processor from Intel or AMD, this content isn't applicable. If you aren't sure which type of processor you have, check **Settings** > **System** > **About**. Support for 32-bit Arm versions of applications will be removed in a future release of Windows 11. After this change, for the small number of applications affected, app features might be different and you might notice a difference in performance. For more technical details about this	January 2023

Feature	Details and mitigation	Deprecation announced
	change, see Update app architecture from Arm32 to Arm64.	
Update Compliance	Update Compliance, a cloud-based service for the Windows client, is no longer being developed. This service was replaced with Windows Update for Business reports, which provides reporting on client compliance with Microsoft updates from the Azure portal.	November 2022
Windows Information Protection	Windows Information Protection will no longer be developed in future versions of Windows. For more information, see Announcing sunset of Windows Information Protection (WIP). For your data protection needs, Microsoft recommends that you use Microsoft Purview Information Protection and Microsoft Purview Data Loss Prevention. Windows Information Protection is removed starting in Windows 11, version 24H2.	July 2022
BitLocker To Go Reader	**Note: BitLocker to Go as a feature is still supported.** Reading of BitLocker-protected removable drives (BitLocker To Go) from Windows XP or Windows Vista in later operating systems is deprecated and might be removed in a future release of Windows client. The following items might not be available in a future release of Windows client: - ADMX policy: **Allow access to BitLocker-protected removable data drives from earlier versions of Windows** - Command line parameter: manage-bde -DiscoveryVolumeType (-dv) - Catalog file: **c:\windows\BitLockerDiscoveryVolumeContents** - BitLocker 2 Go Reader app: **bitlockertogo.exe** and associated files	21H1
Personalization roaming	Roaming of Personalization settings (including wallpaper, slideshow, accent colors, and lock screen images) is no longer being developed and might be removed in a future release.	21H1

Feature	Details and mitigation	Deprecation announced
Windows Management Instrumentation command-line (WMIC) utility.	The WMIC utility is deprecated in Windows 10, version 21H1 and the 21H1 General Availability Channel release of Windows Server. This utility is superseded by Windows PowerShell for WMI. Note: This deprecation applies to only the command-line management utility. WMI itself isn't affected. **[Update - January 2024]**: Currently, WMIC is a Feature on Demand (FoD) that's preinstalled by default in Windows 11, versions 23H2 and 22H2. In the next release of Windows, the WMIC FoD will be disabled by default.	21H1
Timeline	Starting in July 2021, if you have your activity history synced across your devices through your Microsoft account (MSA), you can't upload new activity in Timeline. For more information, see Get help with timeline.	20H2
Microsoft Edge	The legacy version of Microsoft Edge is no longer being developed.	2004
Companion Device Framework	The Companion Device Framework is no longer under active development.	2004
Dynamic Disks	The Dynamic Disks feature is no longer being developed. This feature will be fully replaced by Storage Spaces in a future release.	2004
Microsoft Desktop Optimization Pack (MDOP)	The Microsoft Desktop Optimization Pack (MDOP) is no longer being developed. End of extended support is April 14, 2026. This end of support includes the User Experience Virtualization (UE-V) client in Windows. As of November 2024, the Application Virtualization (App-V) client in Windows is no longer deprecated and persists with a fixed extended support lifecycle.	September 2019
Language Community tab in Feedback Hub	The Language Community tab will be removed from the Feedback Hub. The standard feedback process: Feedback Hub - Feedback is the recommended way to provide translation feedback.	1909

Feature	Details and mitigation	Deprecation announced
My People / People in the Shell	My People is no longer being developed. It may be removed in a future update.	1909
Package State Roaming (PSR)	PSR will be removed in a future update. PSR allows non-Microsoft developers to access roaming data on devices, enabling developers of UWP applications to write data to Windows and synchronize it to other instantiations of Windows for that user. The recommended replacement for PSR is Azure App Service. Azure App Service is widely supported, well documented, reliable, and supports cross-platform/cross-ecosystem scenarios such as iOS, Android and web. PSR was removed in Windows 11.	1909
XDDM-based remote display driver	The Remote Desktop Services uses a Windows Display Driver Model (WDDM) based Indirect Display Driver (IDD) for a single session remote desktop. The support for Windows 2000 Display Driver Model (XDDM) based remote display drivers will be removed in a future release. Independent Software Vendors that use an XDDM-based remote display driver should plan a migration to the WDDM driver model. For more information on implementing remote display indirect display driver, check out Updates for IddCx versions 1.4 and later.	1903
Taskbar settings roaming	Roaming of taskbar settings is no longer being developed and we plan to remove this capability in a future release.	1903
Wi-Fi WEP and TKIP	Since the 1903 release, a warning message has appeared when connecting to Wi-Fi networks secured with WEP or TKIP (which aren't as secure as those using WPA2 or WPA3). In a future release, any connection to a Wi-Fi network using these old ciphers will be disallowed. Wi-Fi routers should be updated to use AES ciphers, available with WPA2 or WPA3.	1903
Print 3D app	3D Builder is the recommended 3D printing app. To 3D print objects on new Windows devices,	1903

Feature	Details and mitigation	Deprecation announced
	customers must first install 3D Builder from the Store.	
Companion device dynamic lock APIS	The companion device framework (CDF) APIs enable wearables and other devices to unlock a PC. In Windows 10, version 1709, we introduced Dynamic Lock, including an inbox method using Bluetooth to detect whether a user is present and lock or unlock the PC. Because of this reason, and because non-Microsoft partners didn't adopt the CDF method, we're no longer developing CDF Dynamic Lock APIs.	1809
OneSync service	The OneSync service synchronizes data for the Mail, Calendar, and People apps. We added a sync engine to the Outlook app that provides the same synchronization.	1809
Software Restriction Policies in Group Policy	Instead of using the Software Restriction Policies through Group Policy, you can use AppLocker or Windows Defender Application Control to control which apps users can access and what code can run in the kernel.	1803
Offline symbol packages (Debug symbol MSIs)	We're no longer making the symbol packages available as a downloadable MSI. Instead, the Microsoft Symbol Server is moving to be an Azure-based symbol store. If you need the Windows symbols, connect to the Microsoft Symbol Server to cache your symbols locally or use a manifest file with SymChk.exe on a computer with internet access.	1803
Windows Help Viewer (WinHlp32.exe)	All Windows help information is available online. The Windows Help Viewer is no longer supported in Windows 10. For more information, see Error opening Help in Windows-based programs: "Feature not included" or "Help not supported".	1803
MBAE service metadata	The MBAE app experience is replaced by an MO UWP app. For more information, see Developer guide for creating service metadata	1803
Contacts feature in File Explorer	We're no longer developing the Contacts feature or the corresponding Windows Contacts API. Instead, you can use the People app in Windows 10 to maintain your contacts.	1803

Feature	Details and mitigation	Deprecation announced
Phone Companion	Use the **Phone** page in the Settings app. In Windows 10, version 1709, we added the new **Phone** page to help you sync your mobile phone with your PC. It includes all the Phone Companion features.	1803
IPv4/6 Transition Technologies (6to4, ISATAP, Teredo, and Direct Tunnels)	6to4 has been disabled by default since Windows 10, version 1607 (the Anniversary Update), ISATAP has been disabled by default since Windows 10, version 1703 (the Creators Update), Teredo has been disabled since Windows 10, version 1803. The Direct Tunnels feature has always been disabled by default. Use native IPv6 support instead.	1803
Layered Service Providers	Layered Service Providers haven't been developed since Windows 8 and Windows Server 2012. Use the Windows Filtering Platform instead. When you upgrade from an older version of Windows, any layered service providers you're using aren't migrated; you'll need to reinstall them after upgrading.	1803
Business Scanning	This feature is also called Distributed Scan Management (DSM) **(Added 05/03/2018)** The Scan Management functionality was introduced in Windows 7 and enabled secure scanning and the management of scanners in an enterprise. We're no longer investing in this feature, and there are no devices available that support it.	1803
IIS 6 Management Compatibility*	We recommend that users use alternative scripting tools and a newer management console.	1709
IIS Digest Authentication	We recommend that users use alternative authentication methods.	1709
RSA/AES Encryption for IIS	We recommend that users use CNG encryption provider.	1709
Screen saver functionality in Themes	Disabled in Themes. Screen saver functionality in Group Policies, Control Panel, and Sysprep continues to be functional. Lock screen features and policies are preferred.	1709

Feature	Details and mitigation	Deprecation announced
Sync your settings (updated: July, 30, 2024)	Back-end changes: In future releases, the back-end storage for the current sync process will change. A single cloud storage system will be used for Enterprise State Roaming and all other users. As part of this change, we will stop supporting the Device Syncing Settings and App Data report. All other **Sync your settings** options will continue to work provided your clients are running an up-to-date version of: - Windows 11 - Windows 10, version 21H2, or later	1709
System Image Backup (SIB) Solution	This feature is also known as the **Backup and Restore (Windows 7)** legacy control panel. For full-disk backup solutions, look for a third-party product from another software publisher. You can also use OneDrive to sync data files with Microsoft 365.	1709
TLS RC4 Ciphers	To be disabled by default. For more information, see TLS (Schannel SSP) changes in Windows 10 and Windows Server 2016	1709
Trusted Platform Module (TPM) Owner Password Management	This functionality within TPM.msc will be migrated to a new user interface.	1709
Trusted Platform Module (TPM): TPM.msc and TPM Remote Management	To be replaced by a new user interface in a future release.	1709
Trusted Platform Module (TPM) Remote Management	This functionality within TPM.msc will be migrated to a new user interface.	1709
Windows Hello for Business deployment that uses Microsoft Configuration Manager	Windows Server 2016 Active Directory Federation Services - Registration Authority (ADFS RA) deployment is simpler and provides a better user experience and a more deterministic certificate enrollment experience.	1709
Windows PowerShell 2.0	Applications and components should be migrated to PowerShell 5.0+.	1709
Apndatabase.xml	Apndatabase.xml is being replaced by the COSA database. Therefore, some constructs will no longer function. This replacement includes Hardware ID, incoming SMS messaging rules in	1703

Feature	Details and mitigation	Deprecation announced
	mobile apps, a list of privileged apps in mobile apps, autoconnect order, APN parser, and CDMAProvider ID.	
Tile Data Layer	The Tile Data Layer database stopped development in Windows 10, version 1703.	1703
TLS DHE_DSS ciphers DisabledByDefault	TLS RC4 Ciphers will be disabled by default in this release.	1703
TCPChimney	TCP Chimney Offload is no longer being developed. See Performance Tuning Network Adapters.	1703
IPsec Task Offload	IPsec Task Offload versions 1 and 2 are no longer being developed and shouldn't be used.	1703
`wusa.exe /uninstall /kb:####### /quiet`	The `wusa` tool usage to quietly uninstall an update is deprecated. The uninstall command with `/quiet` switch fails with event ID 8 in the Setup event log. Uninstalling updates quietly could be a security risk because malicious software could quietly uninstall an update in the background without user intervention.	1507 Applies to Windows Server 2016 and Windows Server 2019.

Feedback

Was this page helpful? Yes No

Provide product feedback

Resources for deprecated features

Article • 03/24/2025 • Applies to: ✅ Windows 11, ✅ Windows 10

This article provides additional resources about deprecated features for Windows client that may be needed by IT professionals. The following information is provided to help IT professionals plan for the removal of deprecated features:

Paint 3D

Paint 3D is deprecated and will be removed from the Microsoft Store on November 4, 2024. Existing installations of Paint 3D will continue to work, but the app will no longer be available for download from the Microsoft Store. If you remove the app, you can reinstall it from the Microsoft Store until November 4, 2024. After that date, Paint 3D will no longer be available for download. Paint 3D was preinstalled on some Windows 10 devices, but wasn't preinstalled on Windows 11 devices. Some alternatives to Paint 3D include:

- View and edit 2D images: Paint or Photos
- View 3D content: 3D Viewer.

NTLM

Customers concerned about NTLM usage in their environments are encouraged to utilize NTLM auditing to investigate how NTLM is being used.

In many cases, applications should be able to replace NTLM with Negotiate using a one-line change in their `AcquireCredentialsHandle` request to the SSPI. One known exception is for applications that have made hard assumptions about the maximum number of round trips needed to complete authentication. In most cases, Negotiate will add at least one additional round trip. Some scenarios may require additional configuration. For more information, see Kerberos authentication troubleshooting guidance.

Negotiate's built-in fallback to NTLM is preserved to mitigate compatibility issues during this transition. For updates on NTLM deprecation, see https://aka.ms/ntlm.

NTLM v1 is removed starting in Windows 11, version 24H2 and Windows Server 2025. Some situations still use NTLMv1 primitives for legacy reasons. MSCHAPv2 uses the same response function as NTLMv1 and is vulnerable to the same attacks against the weak crypto. MSCHAPv2 is only disabled by enabling Credential Guard.

WordPad

WordPad is removed from all editions of Windows starting in Windows 11, version 24H2 and Windows Server 2025. As a result, Windows will no longer have a built-in, default RTF reader. We recommend Microsoft Word for rich text documents like .doc and .rtf and Notepad for plain text documents like .txt. The following binaries will be removed as a result of WordPad removal:

- wordpad.exe
- wordpadfilter.dll
- write.exe

Avoid taking a direct dependency on these binaries and Wordpad in your product. Instead, for trying to open a text file, rely on Microsoft Word or Notepad.

VBScript

VBScript will be available as a feature on demand before being retired in future Windows releases. Initially, the VBScript feature on demand will be preinstalled to allow for uninterrupted use while you prepare for the retirement of VBScript.

TLS versions 1.0 and 1.1 disablement resources

Over the past several years, internet standards and regulatory bodies have deprecated or disallowed TLS versions 1.0 and 1.1 due to various security issues. Starting in Windows 11 Insider Preview builds for September 2023 and continuing in future Windows OS releases, TLS 1.0 and 1.1 are disabled by default. This change increases the security posture of Windows customers and encourages modern protocol adoption. For organizations that need to use these versions, there's an option to re-enable TLS 1.0 or TLS 1.1.

The following information can help IT professionals to:

- Identify issues related to TLS 1.0 and 1.1 disablement
- Re-enable TLS 1.0 and 1.1, if needed

For developer guidance and for a list of common applications known to rely on TLS 1.0 or 1.1, see the Announcing the disablement of TLS 1.0 and TLS 1.1 in Windows blog post.

TLS diagnostic events

Applications that fail when TLS 1.0 and 1.1 are disabled can be identified by reviewing the event logs. In the System Event Log, SChannel EventID 36871 may be logged with the following description:

```
A fatal error occurred while creating a TLS <client/server> credential. The internal error state is 10013. The SSPI client process is <process ID>.
```

TLS 1.0 and 1.1 guidance for IT professionals

The impact of disabling TLS versions 1.0 and 1.1 depends on the Windows applications using TLS. For example, TLS 1.0 and TLS 1.1 are already disabled by Microsoft 365 products as well as WinHTTP and WinINet API surfaces. Most newer versions of applications support TLS 1.2 or higher protocol versions. If an application starts failing after this change, the first step is to discover if a newer version of the application has TLS 1.2 or TLS 1.3 support.

Using the system default settings for the best balance of security and performance is recommended. Organizations that limit TLS cipher suites using Group Policy or PowerShell cmdlets should also verify that cipher suites needed for TLS 1.3 and TLS 1.2 are enabled.

If there are no alternatives available and TLS 1.0 or TLS 1.1 is needed, the protocol versions can be re-enabled with a system registry setting. To override a system default and set a (D)TLS or SSL protocol version to the **Enabled** state:

- **TLS 1.0**:

  registry

  ```
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
        "Enabled" = dword:00000001
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
        "Enabled" = dword:00000001
  ```

- **TLS 1.1**:

  registry

  ```
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
        "Enabled" = dword:00000001
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\
  ```

```
SCHANNEL\Protocols\TLS 1.1\Server]
      "Enabled" = dword:00000001
```

Re-enabling TLS 1.0 or TLS 1.1 on machines should only be done as a last resort, and as a temporary solution until incompatible applications can be updated or replaced. Support for these legacy TLS versions may be completely removed in the future.

Microsoft Support Diagnostic Tool resources

The Microsoft Support Diagnostic Tool (MSDT) gathers diagnostic data for analysis by support professionals. MSDT is the engine used to run legacy Windows built-in troubleshooters. There are currently 28 built-in troubleshooters for MSDT. Half of the built-in troubleshooters have already been redirected to the Get Help platform, while the other half will be retired.

If you're using MSDT to run custom troubleshooting packages, it will be available as a feature on demand before the tool is fully retired in 2025. This change allows you to continue to use MSDT to run custom troubleshooting packages while transitioning to a new platform. Contact Microsoft support for Windows if you require more assistance.

Redirected MSDT troubleshooters

The following troubleshooters are automatically redirected when you access them from **Start** > **Settings** > **System** > **Troubleshoot**:

- Background Intelligent Transfer Service (BITS)
- Bluetooth
- Camera
- Internet Connections
- Network Adapter
- Playing Audio
- Printer
- Program Compatibility Troubleshooter
- Recording Audio
- Video Playback
- Windows Network Diagnostics
- Windows Media Player DVD
- Windows Media Player Library
- Windows Media Player Settings
- Windows Update

Retired MSDT troubleshooters

The following troubleshooters will be removed in a future release of Windows:

- Connection to a Workplace using DirectAccess
- Devices and Printers
- Hardware and Devices
- HomeGroup
- Incoming Connections
- Internet Explorer Performance
- Internet Explorer Safety
- Keyboard
- Power
- Search and Indexing
- Speech
- System Maintenance
- Shared Folders
- Windows Store Apps

Next steps

- Windows feature lifecycle
- Deprecated Windows features
- Removed Windows features

Feedback

Features and functionality removed in Windows client

Article • 03/11/2025 • Applies to: ✅ Windows 11, ✅ Windows 10

Each version of Windows client adds new features and functionality. Occasionally, new versions also remove features and functionality, often because they've added a newer option. This article provides details about the features and functionality that have been removed in Windows client.

For more information about features that might be removed in a future release, see Deprecated features for Windows client.

> **Note**
>
> To get early access to new Windows builds and test these changes yourself, join the Windows Insider program.

For more information about features in Windows 11, see Feature deprecations and removals.

To understand the distinction between *deprecation* and *removal*, see Windows client features lifecycle.

Removed features and functionality

The following features and functionalities have been removed from the installed product image for Windows client. Applications or code that depend on these features won't function in the release when it was removed, or in later releases.

The following list is subject to change and might not include every affected feature or functionality.

Expand table

Feature	Details and mitigation	Support removed
Location History	We are removing the Location History feature, an API that allowed Cortana to access 24 hours of device history when location was enabled. With the removal of the Location History feature, location data will no	March 25, 2025

Feature	Details and mitigation	Support removed
	longer be saved locally and the corresponding settings will also be removed from the **Privacy & Security** > **Location** page in **Settings**. This feature is being gradually removed from devices using a controlled feature rollout (CFR).	
Data Encryption Standard (DES)	DES, the symmetric-key block encryption cipher, is considered nonsecure against modern cryptographic attacks, and replaced by more robust encryption algorithms. DES was disabled by default starting with Windows 7 and Windows Server 2008 R2. It's removed from Windows 11, version 24H2 and later, and Windows Server 2025 and later.	September 2025
NTLMv1	NTLMv1 is removed starting in Windows 11, version 24H2 and Windows Server 2025.	24H2
Windows Information Protection	Windows Information Protection is removed starting in Windows 11, version 24H2.	24H2
Microsoft Defender Application Guard for Edge	Microsoft Defender Application Guard, including the Windows Isolated App Launcher APIs, is deprecated for Microsoft Edge for Business and is no longer available starting with Windows 11, version 24H2.	24H2
WordPad	WordPad is removed from all editions of Windows starting in Windows 11, version 24H2 and Windows Server 2025. We recommend Microsoft Word for rich text documents like .doc and .rtf and Windows Notepad for plain text documents like .txt. If you're a developer and need information about the affected binaries, see Resources for deprecated features.	October 1, 2024
Alljoyn	Microsoft's implementation of AllJoyn, which included the Windows.Devices.AllJoyn API namespace, a Win32 API, a management configuration service provider (CSP), and an Alljoyn Router Service is retired. AllJoyn, sponsored by AllSeen Alliance, was an open source discovery and communication protocol for Internet of Things scenarios such as turning on/off lights or reading temperatures. AllSeen Alliance promoted the AllJoyn project from 2013 until 2016 when it merged with the Open Connectivity Foundation (OCF), the sponsors of Iotivity.org, another protocol for Internet of Things scenarios. Customers should refer	October 1, 2024

Feature	Details and mitigation	Support removed
	to the Iotivity.org website for alternatives such as Iotivity Lite or Iotivity.	
Update Compliance	Update Compliance, a cloud-based service for the Windows client, is retired. This service has been replaced with Windows Update for Business reports, which provides reporting on client compliance with Microsoft updates from the Azure portal.	March 31, 2023
Store uploader tool	Support has been removed for the store uploader tool. This tool is included in the Windows SDK only. The endpoint for the tool has been removed from service and the files will be removed from the SDK in the next release.	November 2022
Internet Explorer 11	The Internet Explorer 11 desktop application is retired and out of support as of June 15, 2022 for certain versions of Windows 10. You can still access older, legacy sites that require Internet Explorer with Internet Explorer mode in Microsoft Edge. Learn how. The Internet Explorer 11 desktop application will progressively redirect to the faster, more secure Microsoft Edge browser, and will ultimately be disabled via Windows Update. Disable IE today.	June 15, 2022
XDDM-based remote display driver	Support for Windows 2000 Display Driver Model (XDDM) based remote display drivers is removed in this release. Software publishers that use an XDDM-based remote display driver should plan a migration to the WDDM driver model. For more information on implementing remote display indirect display driver, see Updates for IddCx versions 1.4 and later.	21H1
Microsoft Edge	The legacy version of Microsoft Edge is no longer supported after March 9, 2021. For more information, see End of support reminder for Microsoft Edge Legacy.	21H1
MBAE service metadata	The MBAE app experience is replaced by an MO UWP app. Metadata for the MBAE service is removed.	20H2
Connect app	The **Connect** app for wireless projection using Miracast is no longer installed by default, but is available as an optional feature. To add the feature, select **Settings** > **System** > **Optional features** > **Add a feature** (Windows 10) or **Settings** > **System** > **Optional features** > **Add an optional feature**	2004

Feature	Details and mitigation	Support removed
	(Windows 11), and then add the **Wireless Display** feature.	
Rinna and Japanese Address suggestion	The Rinna and Japanese Address suggestion service for Microsoft Japanese Input Method Editor (IME) ended on August 13, 2020. For more information, see Rinna and Japanese Address suggestion will no longer be offered	2004
Windows To Go	Windows To Go was announced as deprecated in Windows 10, version 1903 and is removed in this release.	2004
Mobile Plans and Messaging apps	Both apps are still supported, but are now distributed in a different way. OEMs can now include these apps in Windows images for cellular enabled devices. The apps are removed for noncellular devices.	2004
PNRP APIs	The Peer Name Resolution Protocol (PNRP) cloud service was shut down in Windows 10, version 1809. We're planning to complete the removal process by removing the corresponding APIs. **[Update - February 2024]**: The corresponding Windows APIs will be removed in Windows 11, version 24H2. DNS-SD and mDNS are recommended alternatives for implementing service discovery scenarios.	1909
Taskbar settings roaming	Roaming of taskbar settings is removed in this release. This feature was announced as no longer being developed in Windows 10, version 1903.	1909
Desktop messaging app doesn't offer messages sync	The messaging app on Desktop has a sync feature that can be used to sync SMS text messages received from Windows Mobile and keep a copy of them on the Desktop. The sync feature has been removed from all devices. Due to this change, you'll only be able to access messages from the device that received the message.	1903
Business Scanning also called Distributed Scan Management (DSM)	We're removing this secure scanning and scanner management capability - there are no devices that support this feature.	1809
FontSmoothing setting in unattend.xml	The FontSmoothing setting lets you specify the font antialiasing strategy to use across the system. We've	1809

Feature	Details and mitigation	Support removed
	changed Windows 10 to use ClearType by default, so we're removing this setting as it is no longer necessary. If you include this setting in the unattend.xml file, it will be ignored.	
Hologram app	We've replaced the Hologram app with the Mixed Reality Viewer. If you would like to create 3D word art, you can still do that in Paint 3D and view your art in VR or HoloLens with the Mixed Reality Viewer.	1809
limpet.exe	We're releasing the limpet.exe tool, used to access TPM for Azure connectivity, as open source.	1809
Phone Companion	When you update to Windows 10, version 1809, the Phone Companion app will be removed from your PC. Use the **Phone** page in the Settings app to sync your mobile phone with your PC. It includes all the Phone Companion features.	1809
Future updates through Windows Embedded Developer Update for Windows Embedded Standard 7-SP1 (WES7-SP1) and Windows Embedded Standard 8 (WES8)	We're no longer publishing new updates to the WEDU server. Instead, download any new updates from the Microsoft Update Catalog. Learn how to get updates from the catalog.	1809
Groove Music Pass	We ended the Groove streaming music service and music track sales through the Microsoft Store in 2017. The Groove app is being updated to reflect this change. You can still use Groove Music to play the music on your PC. You can use Spotify or other music services to stream music on Windows 10, or to buy music to own.	1803
People - Suggestions will no longer include unsaved contacts for non-Microsoft accounts	Manually save the contact details for people you send mail to or get mail from.	1803
Language control in the Control Panel	Use the Settings app to change your language settings.	1803
HomeGroup	We're removing HomeGroup but not your ability to share printers, files, and folders. When you update to Windows 10, version 1803, you won't see HomeGroup in File Explorer, the Control	1803

Feature	Details and mitigation	Support removed
	Panel, or Troubleshoot (**Settings** > **Update & Security** > **Troubleshoot**). Any printers, files, and folders that you shared using HomeGroup **will continue to be shared**. Instead of using HomeGroup, you can now share printers, files and folders by using features that are built into Windows 10: - Share your network printer - Share files in File Explorer	
Connect to suggested open hotspots option in Wi-Fi settings	We previously disabled the **Connect to suggested open hotspots** option and are now removing it from the Wi-Fi settings page. You can manually connect to free wireless hotspots with **Network & Internet** settings, from the taskbar or Control Panel, or by using Wi-Fi Settings (for mobile devices).	1803
XPS Viewer	We're changing the way you get XPS Viewer. In Windows 10, version 1709 and earlier versions, the app is included in the installation image. If you have XPS Viewer and you update to Windows 10, version 1803, there's no action required. You'll still have XPS Viewer. However, if you install Windows 10, version 1803, on a new device (or as a clean installation), you can install XPS Viewer from **Apps and Features** in the Settings app or through Features on Demand. If you had XPS Viewer in Windows 10, version 1709, but manually removed it before updating, you'll need to manually reinstall it.	1803
3D Builder app	No longer installed by default. Consider using Print 3D and Paint 3D in its place. However, 3D Builder is still available for download from the Windows Store.	1709
Apndatabase.xml	For more information about the replacement database, see the following Hardware Dev Center articles: MO Process to update COSA COSA FAQ	1709
Enhanced Mitigation Experience Toolkit (EMET)	Use of this feature will be blocked. Consider using Exploit Protection as a replacement.	1709
Outlook Express	This legacy application will be removed due to lack	1709

Feature	Details and mitigation	Support removed
	of functionality.	
Reader app	Functionality to be integrated into Microsoft Edge.	1709
Reading List	Functionality to be integrated into Microsoft Edge.	1709
Screen saver functionality in Themes	This functionality is disabled in Themes, and classified as **Removed** in this table. Screen saver functionality in Group Policies, Control Panel, and Sysprep continues to be functional. Lock screen features and policies are preferred.	1709
Syskey.exe	Removing this nonsecure security feature. We recommend that users use BitLocker instead. For more information, see 4025993 Syskey.exe utility is no longer supported in Windows 10 RS3 and Windows Server 2016 RS3.	1709
TCP Offload Engine	Removing this legacy code. This functionality was previously transitioned to the Stack TCP Engine. For more information, see Why Are We Deprecating Network Performance Features?	1709
Tile Data Layer	To be replaced by the Tile Store.	1709
Resilient File System (ReFS) (added: August 17, 2017)	Creation ability will be available in the following editions only: Windows 10 Enterprise and Windows 10 Pro for Workstations. Creation ability will be removed from all other editions. All other editions will have Read and Write ability.	1709
By default, Flash autorun in Microsoft Edge is turned off.	Use the Click-to-Run (C2R) option instead. (This setting can be changed by the user.)	1703
Interactive Service Detection Service	See Interactive Services for guidance on how to keep software up to date.	1703
Microsoft Paint	This application won't be available for languages that aren't on the full localization list.	1703
NPN support in TLS	This feature is superseded by Application-Layer Protocol Negotiation (ALPN).	1703
Windows Information Protection "AllowUserDecryption" policy	Starting in Windows 10, version 1703, AllowUserDecryption is no longer supported.	1703

Feature	Details and mitigation	Support removed
WSUS for Windows Mobile	Updates are being transitioned to the new Unified Update Platform (UUP)	1703

Feedback

Was this page helpful? Yes No

Provide product feedback