

Microsoft Intune

Microsoft Intune (formerly **Windows Intune**) is a [Microsoft cloud-based unified endpoint management](#) service for both corporate and [BYOD](#) devices.^[1] It extends some of the "on-premises" functionality of [Microsoft Endpoint Configuration Manager](#) to the [Microsoft Azure](#) cloud.^[2]

Distribution[edit]

No on-premises infrastructure is required for clients to use Intune, and management is accomplished using a web-based portal.^{[3][4]} Distribution is through a subscription system in which a fixed monthly cost is incurred per user. It is also to use Endpoint Manager in co management with Microsoft Endpoint Configuration Manager.

It is included in Microsoft Enterprise Mobility + Security (EMS) suite^[5] and Microsoft Office 365 Enterprise E5,^[6] which were both succeeded by [Microsoft 365](#) in July 2017.^{[7][8]} Microsoft 365 Business Premium licenses also include Intune and EMS.

Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints. As organizations move to support hybrid and remote workforces, they face the challenge of managing devices to access organizational resources. Staff and students must collaborate, work across the board, and access and participate in these resources safely. Managers must protect organizational data, manage end-user access, and support users wherever they work.^[9]

Intune supports [Android](#), [iOS](#), [macOS](#) and [Windows](#) Operating Systems.^[10] Administration is done via a web browser. The administration console allows Intune to invoke remote tasks such as [malware](#) scans.^[11] Since version 2.0, installation of software packages in [.exe](#), [.msi](#) and [.msp](#) format are supported. Installations are encrypted and compressed on [Microsoft Azure Storage](#). Software installation can begin upon login. It can record and administer volume, retail and OEM licenses, and licenses which are administered by third parties.^[11] Upgrades to newer versions of the Intune software are also controlled.^[12]

Information about inventory is recorded automatically.^[13] Managed computers can be grouped together when problems occur. Intune notifies support staff as well as notifying an external dealer via e-mail.^[14]

Intune plans

Since March 2023 Microsoft Intune is available in 3 versions: Intune Plan 1, Intune Plan 2 and Intune Suite. Plan 2 or Suite do not include Plan 1. Microsoft Intune P1 is included with subscriptions to Microsoft 365 E3, E5, F1, F3, Enterprise Mobility + Security E3 and E5, and Business Premium plans.^[15]

Reception

Der Standard praised the application, saying "the cloud service Intune promises to be a simple PC Management tool via Web console. The interface provides a quick overview of the system of state enterprise."^[16] German *PC World* positively evaluated "usability" saying that it "kept the interface simple."^[13] *Business Computing World* criticized the program, saying "Although Windows Intune worked well in our tests and did everything expected of it, we didn't find it all that easy to get to grips with", blaming the unintuitive "deceptively simple" management interface.^[4] ITespresso rated it "good", but noted connection issues with the remote assistance feature and that changes to firewall settings could take upwards of a full day to push out to clients.^[17]

History

Microsoft Intune was originally introduced as Windows Intune in April 2010. ^[18] Microsoft announced plans to extend the service to other platforms and rename it to Microsoft Intune on 8 October 2014.^[19]

Microsoft Intune securely manages identities, manages apps, and manages devices

Feedback

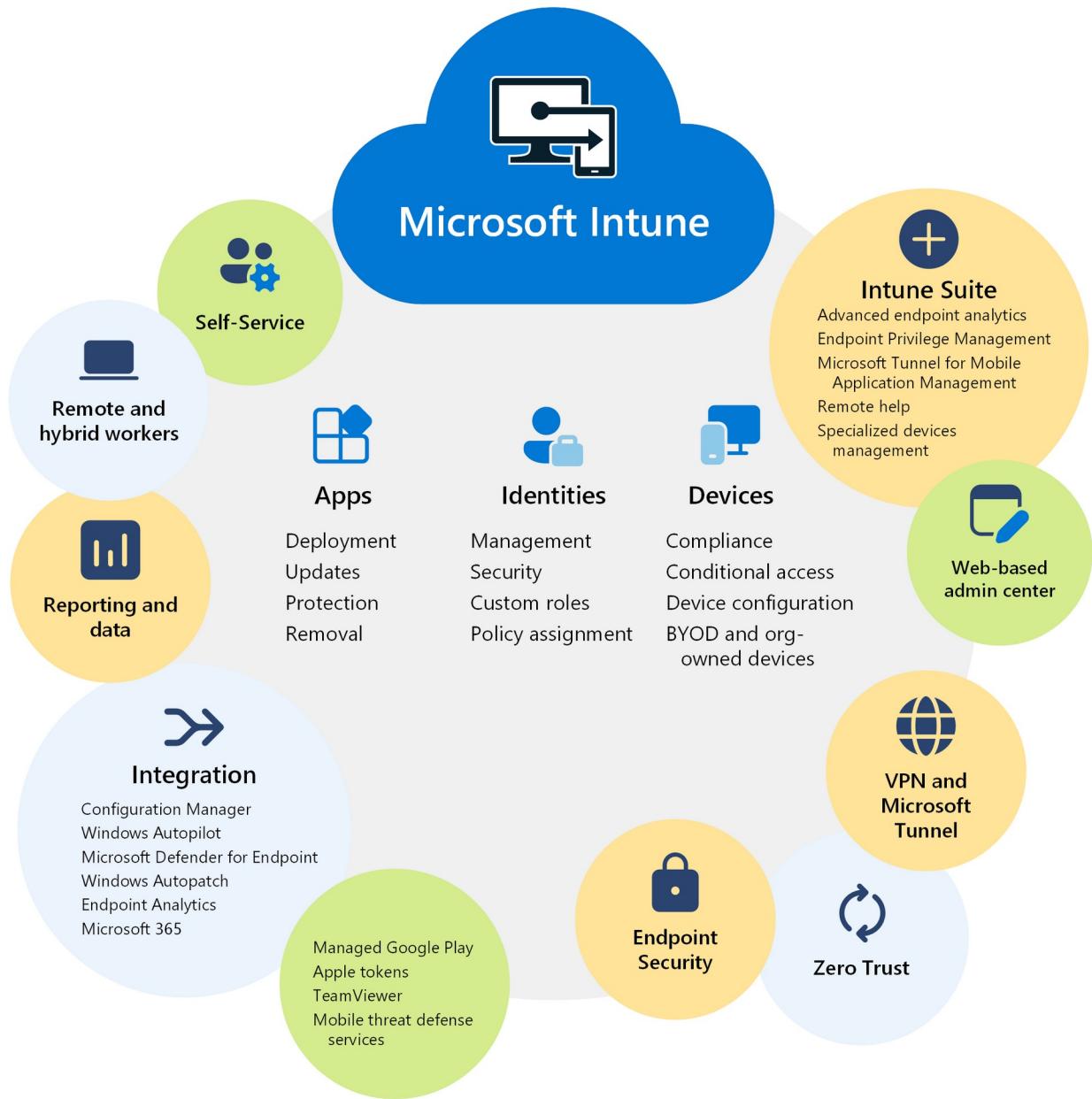
In this article

1. [Key features and benefits](#)
2. [Integrates with other Microsoft services and apps](#)
3. [Integrates with third party partner devices and apps](#)
4. [Enroll in device management, application management, or both](#)

Show 3 more

As organizations support hybrid and remote workforces, they're challenged with managing the different devices that access organization resources. Employees and students need to collaborate, work from anywhere, and securely access and connect to these resources. Admins need to protect organization data, manage end user access, and support users from wherever they work.

To help with these challenges and tasks, use [Microsoft Intune](#).



Microsoft Intune is a cloud-based endpoint management solution. It manages user access to organizational resources and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints.

You can protect access and data on organization-owned and users personal devices. And, Intune has compliance and reporting features that support the [Zero Trust security model](#).

This article lists some features and benefits of Microsoft Intune.

Tip

- To get Intune, go to [Licenses available for Microsoft Intune](#) and [Intune 30-day trial](#).
- For information on what it means to be cloud-native, go to [Learn more about cloud-native endpoints](#).

Key features and benefits

Some key features and benefits of Intune include:

- You can **manage users and devices**, including devices owned by your organization and personally owned devices. Microsoft Intune supports Android, Android Open Source Project (AOSP), iOS/iPadOS, Linux Ubuntu Desktop, macOS, and Windows client devices. With Intune, you can use these devices to securely access organization resources with policies you create.

For more information, go to:

- [Manage identities using Microsoft Intune](#)
- [Manage devices using Microsoft Intune](#)
- [Supported operating systems in Microsoft Intune](#)

Note

If you manage on-premises Windows Server, you can use Configuration Manager.

- Intune **simplifies app management** with a built-in app experience, including app deployment, updates, and removal. You can connect to and distribute apps from your private app stores, enable Microsoft 365 apps, deploy Win32 apps, create app protection policies, and manage access to apps & their data.

For more information, go to [Manage apps using Microsoft Intune](#).

- Intune **automates policy deployment** for apps, security, device configuration, compliance, conditional access, and more. When the policies are ready, you can deploy these policies to your user groups and device groups. To receive these policies, the devices only need internet access.

- Employees and students can **use the self-service features** in the Company Portal app to reset a PIN/password, install apps, join groups, and more. You can customize the Company Portal app to help reduce support calls.

For more information, go to [Configure the Intune Company Portal apps, Company Portal website, and Intune app](#).

- Intune **integrates with mobile threat defense** services, including Microsoft Defender for Endpoint and third party partner services. With these services, the focus is on endpoint security and you can create policies that respond to threats, do real-time risk analysis, and automate remediation.

For more information, go to [Mobile Threat Defense integration with Intune](#).

- You **use a web-based admin center** that focuses on endpoint management, including data-driven reporting. Admins can sign into the Intune admin center from any device that has internet access.

For more information, go to [Walkthrough the Intune admin center](#). To sign in to the admin center, go to [Microsoft Intune admin center](#).

This admin center uses [Microsoft Graph](#) REST APIs to programmatically access the Intune service. Every action in the admin center is a Microsoft Graph call. If you're not familiar with Graph, and want to learn more, go to [Graph integrates with Microsoft Intune](#).

- The Microsoft Intune Suite offers **advanced endpoint management and security**. The suite has optional add-on features, including Remote Help, Endpoint Privilege Management, Microsoft Tunnel for MAM, and more.

For more information, go to [Intune Suite add-on features](#)

Learn how you can [benefit from modern endpoint management](#) with Microsoft Intune.

Integrates with other Microsoft services and apps

Microsoft Intune integrates with other Microsoft products and services that focus on endpoint management, including:

- [**Configuration Manager**](#) for on-premises endpoint management and Windows Server, including deploying software updates and managing data centers

You can use Intune and Configuration Manager together in a co-management scenario, use tenant attach, or use both. With these options, you get the benefits of the web-based admin center and can use other cloud-based features available in Intune.

For more specific information, go to:

- [What is co-management](#)
- [Frequently asked questions about co-management](#)
- [How to enable tenant attach](#)
- [**Windows Autopilot**](#) for modern OS deployment and provisioning

With Windows Autopilot, you can provision new devices and send these devices directly to users from an OEM or device provider. For existing devices, you can reimagine these devices to use Windows Autopilot and deploy the latest Windows version.

For more specific information, go to:

- [Windows Autopilot overview](#)
- [Windows Autopilot deployment for existing devices](#)
- [**Endpoint analytics**](#) for visibility and reporting on end user experiences, including device performance and reliability

You can use Endpoint analytics to help identify policies or hardware issues that slow down devices. It also provides guidance that can help you proactively improve end user experiences and reduce help desk tickets.

For more specific information, go to:

- [What is Endpoint analytics](#)
- [Enroll Intune devices into Endpoint analytics](#)
- [**Microsoft 365**](#) for end user productivity Office apps, including Outlook, Teams, Sharepoint, OneDrive, and more

Using Intune, you can deploy Microsoft 365 apps to users and devices in your organization. You can also deploy these apps when users sign in for the first time.

For more specific information, go to:

- [Add Microsoft 365 Apps to Windows 10/11 devices with Microsoft Intune](#)
- [Microsoft 365 docs: Manage devices with Intune](#)
- **Microsoft Defender for Endpoint** to help enterprises prevent, detect, investigate, and respond to threats

In Intune, you can create a service-to-service connection between Intune and Microsoft Defender for Endpoint. When they're connected, you can create policies that scan files, detect threats, and report threat levels to Microsoft Defender for Endpoint. You can also create compliance policies that set an allowable level of risk. When combined with conditional access, you can block access to organization resources for devices that are noncompliant.

For more specific information, go to:

- [Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune](#)
- [Configure Microsoft Defender for Endpoint in Intune](#)
- **Windows Autopatch** for automatic patching of Windows, Microsoft 365 apps for enterprise, Microsoft Edge, and Microsoft Teams

Windows Autopatch is a cloud based service. It keeps software current, gives users the latest productivity tools, minimizes on-premises infrastructure, and helps free up your IT admins to focus on other projects. Windows Autopatch uses Microsoft Intune to manage patching for Intune-enrolled devices or devices using co-management (Intune + Configuration Manager).

For more specific information, go to:

- [What is Windows Autopatch?](#)
- [Frequently Asked Questions about Windows Autopatch](#)

Integrates with third party partner devices and apps

The Intune admin center makes it easy to connect to different partner services, including:

- **Managed Google Play:** When you connect to your Managed Google Play account, admins can access your organization's private store for Android apps, and deploy these apps to your devices.

For more information, go to [Add Managed Google Play apps to Android Enterprise devices with Intune](#).

- **Apple tokens and certificates:** When they're added, your iOS/iPadOS and macOS devices can enroll in Intune and receive policies from Intune. Admins can access your volume purchased iOS/iPad and macOS app licenses, and deploy these apps to your devices.

For more information, go to:

- [Get an Apple MDM push certificate](#)
- [Automatically enroll iOS/iPadOS devices by using Apple's Automated Device Enrollment](#)
- [Manage iOS and macOS apps purchased through Apple Business Manager with Microsoft Intune](#)
- **TeamViewer:** When you connect to your TeamViewer account, you can use TeamViewer to remotely assist devices.

For more information, go to [Use TeamViewer to remotely administer Intune devices](#).

With these services, Intune:

- Gives admins simplified access to third party partner app services.
- Can manage hundreds of third party partner apps.
- Supports public retail store apps, line of business (LOB) apps, private apps not available in the public store, custom apps, and more.

For more platform-specific requirements to enroll third party partner devices in Intune, go to:

- [Deployment guide: Enroll Android devices in Microsoft Intune](#)
- [Deployment guide: Enroll iOS and iPadOS devices in Microsoft Intune](#)
- [Deployment guide: Enroll Linux devices in Microsoft Intune](#)

- [Deployment guide: Enroll macOS devices in Microsoft Intune](#)

Enroll in device management, application management, or both

Organization-owned devices are enrolled in Intune for **mobile device management (MDM)**. MDM is device centric, so device features are configured based on who needs them. For example, you can configure a device to allow access to Wi-Fi, but only if the signed-in user is an organization account.

In Intune, you create policies that configure features & settings and provide security & protection. The devices are fully managed by your organization, including the user identities that sign in, the apps that are installed, and the data that's accessed.

When devices enroll, you can deploy your policies during the enrollment process. When enrollment completes, the device is ready to use.

For personal devices in bring-your-own-device (BYOD) scenarios, you can use Intune for **mobile application management (MAM)**. MAM is user centric, so the app data is protected regardless of the device used to access this data. There's a focus on apps, including securely accessing apps and protecting data within the apps.

With MAM, you can:

- Publish mobile apps to users.
- Configure apps and automatically update apps.
- View data reports that focus on app inventory and app usage.

You can also use MDM and MAM together. If your devices are enrolled and there are apps that need extra security, then you can also use MAM app protection policies.

For more information, go to:

- [What is device enrollment in Intune?](#)
- [App protection policies overview](#)
- [Create and assign app protection policies](#)

Protect data on any device

With Intune, you can **protect data on managed devices** (enrolled in Intune) and **protect data on unmanaged devices** (not enrolled in Intune). Intune can isolate organization data from personal data. The idea is to protect your company information by controlling the way users access and share information.

For organization-owned devices, you want full control over the devices, especially security. When devices enroll, they receive your security rules and settings.

On devices enrolled in Intune, you can:

- Create and deploy policies that configure security settings, set password requirements, deploy certificates, and more.
- Use mobile threat defense services to scan devices, detect threats, and remediate threats.
- View data and reports that measure compliance with your security settings and rules.
- Use conditional access to only allow managed and compliant devices access to organization resources, apps, and data.
- Remove organization data if a device is lost or stolen.

For personal devices, users might not want their IT admins to have full control. To support a hybrid work environment, give users options. For example, users enroll their devices if they want full access to your organization's resources. Or, if these users only want access to Outlook or Microsoft Teams, then use app protection policies that require multi-factor authentication (MFA).

On devices using application management, you can:

- Use mobile threat defense services to protect app data by scanning devices, detecting threats, and assessing risk.
- Prevent organization data from being copied and pasted into personal apps.
- Use app protection policies on apps and on unmanaged devices enrolled in a third party or partner MDM.
- Use conditional access to restrict the apps that can access organization email and files.
- Remove organization data within apps.

For more information, go to:

- [Protect data and devices with Microsoft Intune](#)
- [Mobile Threat Defense integration with Intune](#)

Simplify access

Intune helps organizations support employees who can work from anywhere. There are features you can configure that allow users to connect to an organization, wherever they might be.

This section includes some common features that you can configure in Intune.

Use Windows Hello for Business instead of passwords

Windows Hello for Business helps protect against phishing attacks and other security threats. It also helps users sign in to their devices and apps more quickly and easily.

Windows Hello for Business replaces passwords with a PIN or biometric, such as fingerprint or facial recognition. This biometric information is stored locally on the devices and is never sent to external devices or servers.

For more information, go to:

- [Windows Hello for Business Overview](#)
- [Manage Windows Hello for Business on devices when they enroll in Intune](#)
- [Manage identities using Microsoft Intune](#)

Create a VPN connection for remote users

VPN policies give users secure remote access to your organization network.

Using common VPN connection partners, including Check Point, Cisco, Microsoft Tunnel, NetMotion, Pulse Secure, and more, you can create a VPN policy with your network settings. When the policy is ready, you deploy this policy to your users and devices that need to connect to your network remotely.

In the VPN policy, you can use certificates to authenticate the VPN connection. When you use certificates, your end users don't need to enter usernames and passwords.

For more information, go to:

- [Create VPN profiles to connect to VPN servers in Intune](#)
- [Use certificates for authentication in Microsoft Intune](#)
- [Microsoft Tunnel for Microsoft Intune](#)
- [Microsoft Tunnel for MAM](#)

Create a Wi-Fi connection for on-premises users

For users who need to connect to your organization network on-premises, you can create a Wi-Fi policy with your network settings. You can connect to a specific SSID, select an authentication method, use a proxy, and more. You can also configure the policy to automatically connect to Wi-Fi when the device is in range.

In the Wi-Fi policy, you can use certificates to authenticate the Wi-Fi connection. When you use certificates, your end users don't need to enter usernames and passwords.

When the policy is ready, you deploy this policy to your on-premises users and devices that need to connect to your on-premises network.

For more information, go to:

- [Create Wi-Fi policy to connect to Wi-Fi networks in Intune](#)
- [Use certificates for authentication in Microsoft Intune](#)

Enable single sign-on (SSO) to your apps and services

When you enable SSO, users can automatically sign in to apps and services using their Microsoft Entra organization account, including some mobile threat defense partner apps.

Specifically:

- On Windows devices, SSO is automatically built in and used to sign in to apps and websites that use Microsoft Entra ID for authentication, including Microsoft 365 apps. You can also enable SSO on VPN and Wi-Fi policies.
- On iOS/iPadOS and macOS devices, you can use the Microsoft Enterprise SSO plug-in to automatically sign in to apps and websites that use Microsoft Entra ID for authentication, including Microsoft 365 apps.
- On Android devices, you can use the Microsoft Authentication Library (MSAL) to enable SSO to Android apps.

For more information, go to:

- [How SSO to on-premises resources works on Microsoft Entra joined devices](#)
- [Use the Microsoft Enterprise SSO plug-in on iOS/iPadOS and macOS devices in Microsoft Intune](#)
- [Enable cross-app SSO on Android using MSAL](#)

Next steps

- [Manage identities using Microsoft Intune](#)
- [Manage devices using Microsoft Intune](#)
- [Manage apps using Microsoft Intune](#)