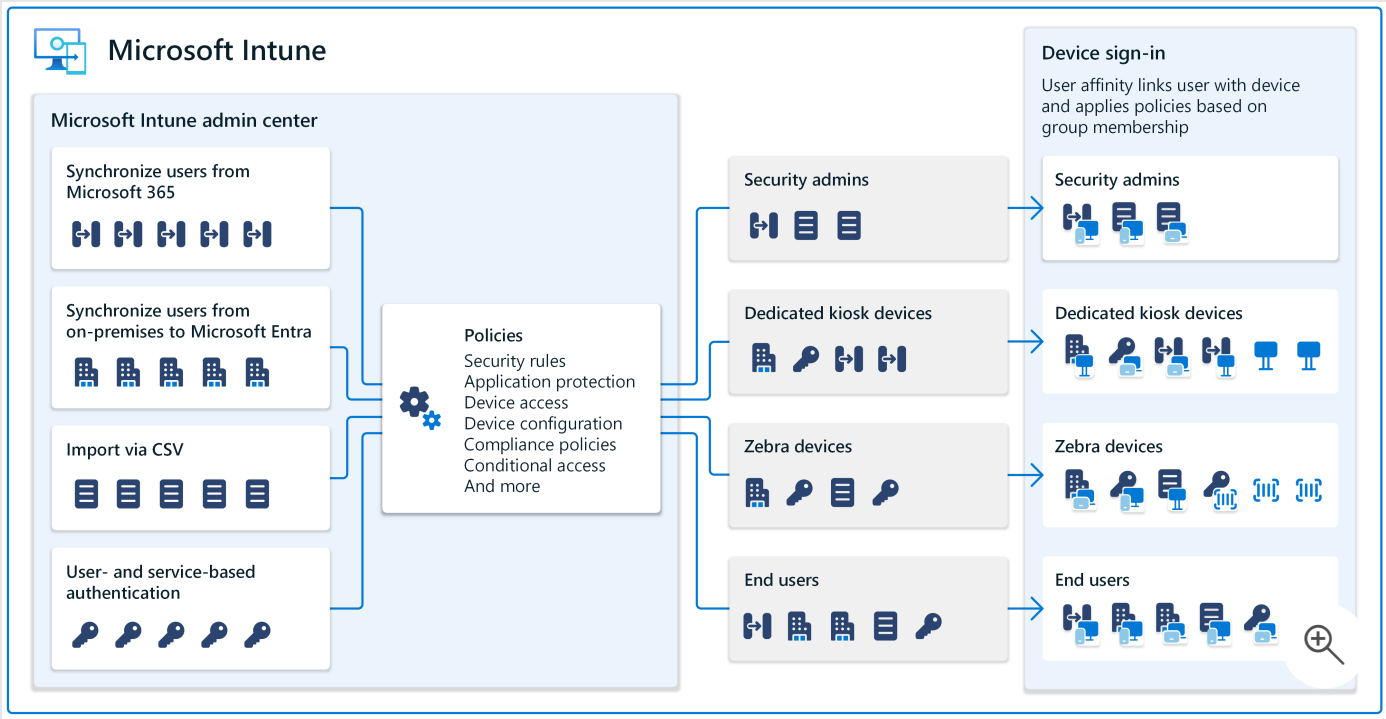
Learn about managing user and group identities in Microsoft Intune

Summarize this article for me

Managing and protecting user identities is a significant part of any endpoint management strategy and solution. Identity management includes the user accounts and groups that access your organization resources.



Admins have to manage account membership, authorize and authenticate access to resources, manage settings that affect user identities, and secure & protect the identities from malicious intent.

Microsoft Intune can do all these tasks, and more. Intune is a cloud-based service that can manage user identities through policy, including security and authentication policies.

From a service perspective, Intune uses Microsoft Entra ID for identity storage and permissions. Using the Microsoft Intune admin center, you can manage these tasks in a central location designed for endpoint management.

This article discusses concepts and features you should consider when managing your identities.

> **Important**
>
> On October 14, 2025, Windows 10 reached end of support and won't receive quality and feature updates. Windows 10 is an **allowed** version in Intune. Devices running this version can still enroll in Intune and use eligible features, but functionality won't be guaranteed and can vary.

Use your existing users and groups

A large part of managing endpoints is managing users and groups. If you have existing users and groups or will create new users and groups, Intune can help.

In on-premises environments, user accounts and groups are created and managed in on-premises Active Directory. You can update these users and groups using any domain controller in the domain.

It's a similar concept in Intune.

The Intune admin center includes a central location to manage users and groups. The admin center is web-based and can be accessed from any device that has an internet connection. Admins just need to sign into the admin center with their Intune administrator account.

An important decision is to determine how to get the user accounts and groups into Intune. Your options:

- If you **currently use Microsoft 365** and have your users and groups in the Microsoft 365 admin center, then these users and groups are also available in the Intune admin center.

  Microsoft Entra ID and Intune use a **tenant**, which is your organization, like Contoso or Microsoft. If you have multiple tenants, sign into the Intune admin center in the same Microsoft 365 tenant as your existing users and groups. Your users and groups are automatically shown and available.

  For more information on what a tenant is, go to Quickstart: Set up a tenant.

- If you **currently use on-premises Active Directory**, then you can use Microsoft Entra

Connect to synchronize your on-premises AD accounts to Microsoft Entra ID. When these accounts are in Microsoft Entra ID, then they're also available in the Intune admin center.

For more specific information, go to What is Microsoft Entra Connect Sync?.

- You can also **import existing users and groups** from a CSV file into the Intune admin center, or create the users and groups from scratch. When adding groups, you can add users and devices to these groups to organize them by location, department, hardware, and more.

  For more information on group management in Intune, go to Add groups to organize users and devices.

By default, Intune automatically creates the **All users** and **All devices** groups. When your users and groups are available to Intune, then you can assign your policies to these users and groups.

Move from machine accounts

When a Windows endpoint, like a Windows device, joins an on-premises Active Directory (AD) domain, a computer account is automatically created. The computer/machine account can be used to authenticate on-premises programs, services, and apps.

These machine accounts are local to the on-premises environment and can't be used on devices that are joined to Microsoft Entra ID. In this situation, you need to switch to user-based authentication to authenticate to on-premises programs, services, and apps.

For more information and guidance, go to Known issues and limitations with cloud-native endpoints.

Roles and permissions control access

For the different admin-type of tasks, Intune uses role-based access control (RBAC). The roles you assign determine the resources an admin can access in the Intune admin center, and what they can do with those resources. There are some built-in roles that focus on endpoint management, like Application Manager, and Policy and Profile Manager.

Since Intune uses Microsoft Entra ID, you also have access to the built-in Microsoft Entra roles, like the Intune Service Administrator.

Each role has its own create, read, update, or delete permissions as needed. You can also create custom roles if your admins need a specific permission. When you add or create your administrator-type of users and groups, you can assign these accounts to the different roles. The Intune admin center has this information in a central location and can be easily updated.

For more information, go to Role-based access control (RBAC) with Microsoft Intune

Create user affinity when devices enroll

When users sign into their devices the first time, the device becomes associated with that user. This feature is called **user affinity**.

Any policies assigned or deployed to the user identity go with the user to all of their devices. When a user is associated with the device, they can access their email accounts, their files, their apps, and more.

When you don't associate a user with a device, then the device is considered user-less. This scenario is common for kiosks devices dedicated to a specific task, and devices that are shared with multiple users.

In Intune, you can create policies for both scenarios on Android, iOS/iPadOS, macOS, and Windows. When getting ready to manage these devices, be sure you know the intended purpose of the device. This information helps in the decision making process when devices are being enrolled.

For more specific information, go to the enrollment guides for your platforms:

- Enrollment guide: Enroll Android devices in Microsoft Intune
- Enrollment guide: Enroll iOS and iPadOS devices in Microsoft Intune
- Enrollment guide: Enroll Linux desktop devices in Microsoft Intune
- Enrollment guide: Enroll macOS devices in Microsoft Intune
- Enrollment guide: Enroll Windows devices in Microsoft Intune

Assign policies to users and groups

On-premises, you work with domain accounts and local accounts, and then deploy group policies and permissions to these accounts at the local, site, domain, or OU level (LSDOU). An OU policy overwrites a domain policy, a domain policy overwrites a site policy, and so on.

Intune is cloud-based. Policies created in Intune include settings that control device features, security rules, and more. These policies are assigned to your users and groups. There isn't a traditional hierarchy like LSDOU.

The settings catalog in Intune includes thousands of settings to manage iOS/iPadOS, macOS, and Windows devices. If you currently use on-premises Group Policy Objects (GPOs), then using the settings catalog is a natural transition to cloud-based policies.

For more information on policies in Intune, go to:

- Use the settings catalog to configure settings on Windows, iOS/iPadOS, and macOS devices
- Common questions and answers with device policies and profiles in Microsoft Intune

Secure your user identities

Your user and group accounts access organization resources. You need to keep these identities secure and prevent malicious access to the identities. Here are some things to consider:

- **Windows Hello for Business** replaces username and password sign-in and is part of a password-less strategy.

  Passwords are entered on a device and then transmitted over the network to the server. They can be intercepted and used by anyone and anywhere. A server breach can reveal stored credentials.

  With Windows Hello for Business, users sign in and authenticate with a PIN or biometric, like facial and fingerprint recognition. This information is stored locally on the device and isn't sent to external devices or servers.

When Windows Hello for Business is deployed to your environment, you can use Intune to create Windows Hello for Business policies for your devices. These policies can configure PIN settings, allowing biometric authentication, use security keys, and more.

For more information, go to:

- Windows Hello for Business Overview
- Manage Windows Hello for Business on devices when devices enroll with Intune

To manage Windows Hello for Business, you use one of the following options:

- During device enrollment: Configure tenant-wide policy that applies Windows Hello settings to devices at the time the device enrolls with Intune.
- Security baselines: Some settings for Windows Hello can be managed through Intune's security baselines, like the **Microsoft Defender for Endpoint security** or **Security Baseline for Windows 10 and later** baselines.
- Settings catalog: The settings from endpoint security account protection profiles are available in the Intune settings catalog.

- **Certificate-based authentication** is also a part of a password-less strategy. You can use certificates to authenticate your users to applications and organization resources through a VPN, a Wi-Fi connection, or email profiles. With certificates, users don't need to enter usernames and passwords, and certificates can make access to these resources easier.

  For more information, go to Use certificates for authentication in Microsoft Intune.

- **Multifactor authentication (MFA)** is a feature available with Microsoft Entra ID. For users to successfully authenticate, at least two different verification methods are required. When MFA is deployed to your environment, you can also require MFA when devices are enrolling into Intune.

  For more information, go to:

  - Plan a Microsoft Entra multifactor authentication deployment
  - Require multifactor authentication for Intune device enrollments

- **Zero Trust** verifies all endpoints, including devices and apps. The idea is to help keep organization data in the organization, and prevent data leaks from accidental or malicious intent. It includes different feature areas, including Windows Hello for

Business, using MFA, and more.

For more information, see Zero Trust with Microsoft Intune.

Related articles

- Learn about managing devices in Intune
- Learn about managing apps in Intune

Last updated on 03/04/2025